DATA PROTECTION GUIDE TO PROTECT CONSUMERS
WITH A FOCUS ON SMALL BUSINESS

Special thanks to the California and Illinois Attorneys General and to the Federal Trade Commission for their preceding materials and contributions to improving cybersecurity.

Disclaimer

This guide is meant to provide guidance only. It does not provide legal advice or legal opinions nor replace the benefit of legal consultation with a private attorney. The suggestions provide the absolute minimum of necessary steps. They provide an overview of the cybersecurity threats facing small businesses, a brief and incomplete summary of several practices that help manage the risks posed by these threats, and a response plan in the event of a cyber-incident.

It is important to recognize that, due to the ever-changing nature of information security and technology, more may be required of businesses and governmental agencies than is explained in this guide. Furthermore, appropriate steps depend on the type of entity and upon each business.
Table of Contents

INTRODUCTION ................................................................................................. 3

IMPORTANT RESOURCES ............................................................................... 4

CYBERSECURITY THREATS ........................................................................... 5

DEVELOPING AN INFORMATION MANAGEMENT PROGRAM .................... 8

   I. Discover ................................................................................................. 8
   II. Scale Down .......................................................................................... 10
   III. Protect ................................................................................................ 12
   IV. Communicate ....................................................................................... 19
   V. Evolve ................................................................................................... 20

RESPONDING TO SECURITY BREACHES .................................................... 21

MISSISSIPPI LAW ON DATA BREACHES - MISS. CODE ANN. § 75-24-29 .... 23

FINALLY, WHAT NOT TO DO ...................................................................... 25

APPENDIX A – Outline of Children’s Online Privacy Protection Act

APPENDIX B – Outline of Family Educational Rights and Privacy Act

APPENDIX C – Federal Trade Commission Orders relating to Referenced Cases
INTRODUCTION

This Guide was created with small businesses in mind but may be helpful to larger companies and government agencies as well.

Relatively small investments in cybersecurity preparedness can yield significant risk reductions. Every business should follow the steps summarized below in order to reduce the chance they will be a victim of cybercrime.\(^1\) Anyone who maintains a computer network or data in any way needs to build a fortress and keep it updated. Cybersecurity is not just for the computer guy. Successful cybersecurity measures require leadership and dedication on all levels. Business owners and all employees must be aware and invest the time and resources necessary to ensure the safety and security of information assets. Small business owners are uniquely positioned to ensure that they and their employees are following good cybersecurity practices. They are also in the best position to understand their company’s network and all the devices that connect to it.\(^2\)

Small size and relative anonymity no longer ensure that a person will be left alone. Any entity, whether big or small, can be the victim of cybercrime. Just as it has become second nature for most of us to lock our front doors when we leave the house, assume the entity is a potential target and take basic precautions to protect it.

Customers and employees expect businesses and agencies to provide adequate and appropriate protection for their personal information, and they have legal rights to have their personal information protected. Additionally, current and potential business partners want assurance that their information, systems, and networks will not be put at risk when they do business. While some may assume they have nothing of value to a cybercriminal, they forget that they retain customer information, create intellectual property, and keep money in the bank.

In addition to implementing adequate cybersecurity measures, entities should clearly explain to consumers and other data-providers how the information they provide will be used and generally how it will be protected.

**It is highly important to train employees and not assume that they know computer security basics.**

---


\(^2\) Id.
These measures, however, cannot guarantee that entities will avoid cybersecurity incidents, and the Guide therefore contains recommendations for how to prepare an effective cybersecurity incident response plan.3

Please note federal law imposes special requirements on certain industries.

Financial institutions and creditors must follow the Gramm-Leach-Bliley (GLB) Act and the Fair Credit Reporting Act (FCRA.)

Health care providers, health plans, and related entities must follow HIPAA, the Health Insurance Portability and Accountability Act.

Websites and internet-based services likely interacting with children must follow COPPA, the Children’s Online Privacy Protection Act, and educational institutions receiving federal funds must follow FERPA, the Family Educational Rights and Privacy Act to protect student records in addition to basic data protection. There are also special rules regarding student surveys under Protection of Pupil Rights Amendment (PPRA.)

IMPORTANT RESOURCES

For more detailed information, entities are encouraged to review and monitor the following:


2. International Org. for Standardization (ISO) (especially for businesses interacting with the federal government) www.iso.org/iso/home.html


3 Id.


CYBERSECURITY THREATS

Advances in online technology have made many day-to-day tasks substantially easier through low cost, Internet enabled point of sale (POS) systems or cloud-based payroll and inventory services for instance that process and store sensitive data. As a result, an increasing number of entities are moving away from paper transactions. Data is more accessible and replicable than ever before and this, in turn, has made data more vulnerable to unauthorized access and distribution.\(^4\)

General Categories of Security Threats:

*Email Scams*

Entities may find themselves the victims of phishing attacks by criminals seeking access to their customer database or bank accounts. Some of the largest breaches are the result of an employee opening a link in an email which appears to be from someone they know.

Social networks give phishers access to a treasure trove of personal information they can use to customize their attacks and increase their likelihood of success. It only takes one employee to fall for a targeted attack and compromise their sensitive corporate credentials for an entire company or agency to suffer.\(^5\)

*Malware*

Malware, which is short for “malicious software,” is any type of program designed or used for unauthorized access to a computer system. According to the cybersecurity company FireEye, malware continues to be the cyber weapon of choice. Malware activity

\(^4\) *Id.*  
\(^5\) *Id.*
has become so pervasive that once every three minutes, an organization will experience a malicious email file attachment, web link, or other malware communication.⁶

Phishing scams may use email, text messages, Facebook or Twitter to distribute links to malicious webpages designed to trick a person into providing information like passwords or account numbers. Often these messages and sites are very different to distinguish from those of a bank or other legitimate sources.⁷ Drive-By Downloads can automatically download an application when a person visits a web page. The attacker can first access the data stored on the target device and then use that device to access other computers, tablets, and cell phones in the target’s network.⁸ An entire organization can be compromised from a single unsecured device. Terms often used in security news stories like viruses, worms, Trojans and spyware describe specific types of malware.⁹

Mobile Devices

Mobile devices are constantly connected to the Internet and can access web-based services, exposing the devices to additional threats.

- Browser exploits take advantage of vulnerabilities in a mobile web browser or software launched by the browser such as a Flash player, PDF reader, or image viewer. Simply by visiting an unsafe web page, one can trigger a browser exploit that can install malware or perform other actions on a device.¹⁰

- “Malicious apps” may look fine on the surface, but they are specifically designed to commit fraud or cause disruption to devices. Even perfectly legitimate apps can pose a threat if exploited for fraudulent purposes.¹¹

Unsecured Internet Connections and Network Access

---

¹⁰ id.
¹¹ id.
Many employees work from home, hotels, airports, and coffee shops on their laptops, tablets, or smart phones. Thus, they are likely using a variety of wireless internet connections and Bluetooth to respond to email and access sensitive accounts and data. Entities do not have direct control over these wireless access points like they do in the workplace, and these unsecured connections risk exposing data when security measures are not taken to protect the transmission of it.\(^\text{12}\)

Remote access services, such as remotely controlled thermostats or security systems can give a perpetrator access to the device used to access the service and to any network to which the device is connected. This weak link must be prevented via “endpoint security” software directed at the remote access portal.

**Physical Breaches**

Laptops, tablets, and smartphones can store a massive amount of data. For many small businesses, a single smartphone may store multiple years’ worth of the company’s financial and inventory records.

As laptops, smartphones, and tablets become ubiquitous in the workplace, the risk of theft or loss of workplace devices rises. If Employees use their devices at home or on the road to conduct work and if they accidentally leave them in a cab, or suffer a break-in, the devices and the data on them could end up in the wrong hands.\(^\text{13}\)

**Point-of-sale Systems**

Hackers can access consumer payment card information through vulnerable devices and software, including the magnetic stripe data and PIN. In response, the credit card payment industry is requiring chip technology as of October 2015 in the United States which is already in place in many other countries; however, hackers are already developing a new manner of attack in response. Point-of-sale systems must be protected via endpoint security software. Retail associations and the payment card industry standards may offer additional updates and suggested protections.

**Foreign Contact**

Internet communications may be closely monitored and recorded in some foreign countries, so entities should be aware that their business communications in another country may be subject to foreign corporate espionage and/or government surveillance.\(^\text{14}\)

\(^\text{12}\) Id. \\
\(^\text{13}\) Id. \\
\(^\text{14}\) Id.
DEVELOPING AN INFORMATION MANAGEMENT PROGRAM

In order to successfully manage private information, entities should take five distinct steps.15

I. Discover
II. Scale Down
III. Protect
IV. Communicate
V. Evolve

I. Discover

Before drafting a privacy or cybersecurity policy, entities should consider their environment, information goals and corporate culture. Additionally, they should look to the state, federal, and international laws that regulate the collection, use, and disclosure of personal information when drafting a privacy policy.

Next, for an entity to draft a successful information policy, it must first understand its actual data practices, as well as its intended data use. To get an accurate assessment of current practices, participation from a wide range of departments, including legal compliance, customer service, marketing, IT, human resources, and sales is necessary.

This team should have the knowledge base and influence in the organization to determine and articulate current practices and future goals.16

Data Inventory

An entity should inventory its data. This inventory should include both customer and employee data records. It should document data location and flow as well as evaluate how, when and with whom the organization shares such information—and the means for data transfer used.17

---

15 Peter P. Swire & Kenesa Ahmad, U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals ch. 3 (International Association of Privacy Professionals 2012).
16 Id.
17 Ill. Atty Gen., Information Security and Security Breach Notification Guidance
Comprehensively review the data stored on IT systems, both on site and off, and with third parties.

When conducting the information assessment, follow these steps:
• Review human resources and personnel records and files and determine what personal employee information is collected, used, maintained, and stored.
• Review internal forms and computer systems that are used by employees for expense reports, trainings, reimbursement requests, and other administrative functions.
• Review all requests for personal information from clients, customers, vendors, and the general public.¹⁸

Data Classification

After completing data inventory, the next step is to classify data according to its level of sensitivity and who needs access to it in order to perform their jobs. Classifying data allows a company to determine the amount of clearance an individual can access or handle, as well as the baseline level of protection that is appropriate for the data.¹⁹

Personal information must be protected. The definition of personal information depends on state and federal law.

It is generally information that identifies a person combined with sensitive information such as their social security number, account number, or medical information, but one should review the law where the entity operates and does business to be sure.

Data Flows

Once data has been inventoried and classified, data flow should be examined and documented to identify areas needing attention.²⁰ Understanding how personal information moves into, through, and out of an entity and who has—or could have—access to this information is essential to assessing security vulnerabilities. Entities should conduct a thorough information assessment of all departments and divisions within the business or governmental agency.

---

¹⁸ Id.
¹⁹ Swire & Ahmad, U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals ch. 3.
²⁰ Id.
Data Accountability

When drafting a privacy policy, one should consider the following questions to assure accountability and compliance:

- Where, how and for what length of time is the data stored?
- How sensitive is the information?
- Will the information be transferred to or from other countries, and if so, how will it be transferred?
- Who determines the rules that apply to the information?
- How is the information to be processed, and how will these processes be maintained?
- Is the use of such data dependent upon other systems?\(^{21}\)

II. Scale Down

Keep only what is necessary.

If the entity does not have a legitimate need for sensitive personally identifiable information, do not keep or request it. Maintaining Social Security numbers (SSNs) on personnel records is required for tax purposes and may be required for other purposes. Other uses may not be required and can be phased out as appropriate.\(^{22}\)

For example, the FTC’s complaint in *RockYou* charged that the company collected email passwords – something the business did not need – and then storing them in clear text. The FTC said the company created an unnecessary risk to people’s email accounts.\(^{23}\)

Sometimes it’s necessary to collect personal data as part of a transaction; although once the deal is done, it may be unwise to keep it. In the FTC’s *BJ’s Wholesale Club* case, the company collected customers’ credit and debit card information to process transactions in its retail stores. According to the complaint, it continued to store that data for up to 30 days – long after the sale was complete. Not only did that violate bank rules, but, by holding on to the information without a legitimate business need, the FTC said BJ’s Wholesale Club created an unreasonable risk. By exploiting other weaknesses in the company’s security practices, hackers stole the account data and used it to make counterfeit credit and debit cards.\(^{24}\) Likewise, in the *Accretive* case, the FTC alleged that the company used people’s personal information in employee training sessions, and then

\(^{21}\) Id.
\(^{22}\) Id.
\(^{23}\) Ill. Atty Gen., Information Security and Security Breach Notification Guidance
failed to remove the information from employees’ computers after the sessions were over. Similarly, in *Foru International*, the FTC charged that the company gave access to sensitive consumer data to service providers who were developing applications for the company. In both cases, the risk could have been avoided by using fictitious information for training or development purposes.25

*Dispose of customer information in a secure way.*

Consider designating or hiring a records retention manager to supervise the disposal of records containing customer information. If an entity hires an outside disposal company, it should conduct due diligence beforehand by checking references or requiring that the company be certified by a recognized industry group.

Burn or shred papers containing customer information so that the information cannot be read or reconstructed. Tearing paper into pieces by hand is insufficient.

Destroy or erase data when disposing of computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones, or any other electronic media or hardware containing customer information.26

Rite Aid and CVS Caremark were prosecuted by the FTC for tossing sensitive personal information in dumpsters. In *Goal Financial*, the FTC alleged that an employee sold surplus hard drives that contained the sensitive personal information of approximately 34,000 customers in clear text.27

*Limit access.*

Do not provide any *one* employee access to *all* systems (financial, personnel, inventory, manufacturing, etc.). For all employees, provide access only to those systems and the specific information that are necessary to do their jobs. Also, limit administrator privileges to a few employees to lessen attempts by employees or hackers to install unauthorized software.28

25 Id.
26 Ill. Atty Gen., Information Security and Security Breach Notification Guidance
Similarly, machines that handle sensitive information like payroll or point of sale (POS) functions should be separate from machines that do routine services. In addition, user accounts should be disabled at the time of an employee’s departure.\(^{29}\)

### III. Protect

Protect the information that the entity keeps. While this Guide predominantly focuses on cyber and electronic security, physical security is still important. Know where sensitive customer information is stored and make sure it is locked with limited access. Also, maintain a careful inventory of computers and any other equipment on which customer information may be stored. In addition, machines that handle sensitive information like payroll or point of sale (POS) functions should ideally be on networks or systems separate from machines involved with routine services, like updating Facebook and checking email.\(^{30}\)

---

**Cybersecurity Checklist:**

1. Ensure that computers are accessible only with a *strong* password.
2. Develop policies for employees who travel or work from home often. Ideally, allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
3. Require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
4. Encrypt all data, at minimum data on mobile devices and that which is transmitted via public networks. (See more on encryption below.)
5. Use a “time-out” function which requires users to re-authenticate after periods of inactivity.
6. Log all computer-readable data extracts or log-ins from databases holding sensitive information and verify each extract. Logs should be reviewed, and inappropriate data extracts or unusual log-ins should be further investigated.\(^{31}\)
7. Maintain current updates to all software including firewalls, anti-virus, and anti-spyware protections. (See more on software below.)
8. Do not allow employees to download and utilize peer-to-peer (P2P) software.\(^{32}\)

---

\(^{29}\) *Id.*


\(^{31}\) See FTC cases *Dave & Buster’s and Cardsystem Solutions.*
9. Develop policies for appropriate use and protection of mobile devices and social media.  
10. Train employees and have them sign a document confirming their cybersecurity responsibilities.  
11. Perform background checks on key employees including anyone with administrator access.  
12. Ensure corporate wireless networks are properly secured.  
13. Do not use public wireless connections to conduct any business.  
14. Back up important data on each computer.  
15. Ideally, use technologies which have the ability to remotely locate and/or wipe clean a device that has gone missing and the ability to analyze behavior so that it can identify and block new methods of attack.  
16. Test and verify protections.

### A. Details on Data Protection

*Protect against authentication bypass.*

“Locking the front door doesn’t offer much protection if the back door is left open.” In *Lookout Services*, the FTC charged that the company failed to adequately test its web application for widely-known security flaws, including one called “predictable resource location.” As a result, a hacker could easily predict patterns and manipulate URLs to bypass the web app’s authentication screen and gain unauthorized access to the company’s databases. The company could have improved the security of its authentication mechanism by testing for common vulnerabilities.  

*Ensure endpoint security.*

Just as a chain is only as strong as its weakest link, network security is only as strong as the weakest security on a computer with remote access to it. That’s the message of FTC cases in which companies failed to ensure that computers with remote access to their networks had appropriate endpoint security. For example, in *Premier Capital Lending*, the company allegedly activated a remote login account for a business client to obtain consumer reports, without first assessing the business’s security. When hackers accessed the client’s system, they stole its remote login credentials and used them to grab consumers’ personal information.

---

35 *Id.*
According to the FTC complaint in *Settlement One*, the business allowed clients that did not have basic security measures, like firewalls and updated antivirus software, to access consumer reports through its online portal.\(^{36}\)

**Encrypt Data**

In basic terms, encrypting data – whether it’s email, photographs, memos or any other type of electronically-stored information – encodes the data so that those without the encryption keys cannot read the information. Strong encryption technology is now commonly available for free, and it is easy to use. Encrypting data can dramatically reduce exposure to a data breach and the theft of proprietary information.\(^{37}\)

Applications such as Symantec PGP, TrueCrypt, Microsoft’s BitLocker and Apple’s FileVault 2 provide full disk encryption for both laptops and desktops that can be used to protect data. The current recommended encryption is Wi-Fi Protected Access 2 (WPA-2) using the Advanced Encryption Standard (AES) for secure encryption.\(^{38}\)

The FTC’s *CBR Systems* case concerned alleged unencrypted backup tapes, a laptop, and an external hard drive containing sensitive information which were stolen from an employee’s car. In each case, the business could have reduced the risk to consumers’ personal information by implementing reasonable security policies when data is en route. For example, when sending files, drives, disks, etc., use a mailing method that lets the company track the location of the package. Limit the instances when employees need to be out and about with sensitive data in their possession. However, when there’s a legitimate business need to travel with confidential information, employees should keep it out of sight and under lock and key whenever possible.\(^{39}\)

**Use industry-tested and accepted methods.**

When considering what technical standards to follow, keep in mind that experts already may have developed effective applicable standards. Savvy entities do not start from scratch when it is not necessary. Instead, they take advantage of that collected wisdom. The FTC’s *ValueClick* case illustrates that principle.

Similarly, the actions against *HTC America*, *Fandango*, and *Credit Karma*, the FTC alleged that the companies failed to follow explicit platform guidelines about secure development practices. For example, Fandango and Credit Karma turned off a critical process known as SSL certificate validation in their mobile apps, leaving the sensitive

\(^{36}\) Id.


\(^{38}\) Id.

information consumers transmitted through those apps open to interception through man-in-the-middle attacks. The companies could have prevented this vulnerability by following the iOS and Android guidelines for software developers, which explicitly warn against turning off SSL certificate validation.\textsuperscript{40}

\textit{Avoid Weak Passwords}

In many instances, passwords are the only things protecting our financial data, trade secrets, and identifying information. Do not use vendor-supplied default passwords and make sure to change passwords often. Hackers can use special software to “guess” passwords, or they can trick unsuspecting employees into turning over their login credentials by directing them to seemingly legitimate login pages.\textsuperscript{41}

\textbf{Strong passwords are a minimum of eight characters in length, and contain numeric characters, symbols, and a mixture of upper- and lower-case alphabetic characters. An employee’s username and password should never be the same.}

\textit{Provide individual accounts.}

Each employee should have an individual account with a unique username and password. Without individual accounts for each user, it may be difficult to hold anyone accountable for data loss or unauthorized data manipulation.\textsuperscript{42}

\textit{Store passwords securely.}

Don’t make it easy for interlopers to access passwords. In \textit{Guidance Software}, the FTC alleged that the company stored network user credentials in clear, readable text that helped a hacker access customer credit card information on the network. Similarly, in \textit{Reed Elsevier}, the FTC charged that the business allowed customers to store user credentials in a vulnerable format in cookies on their computers. In \textit{Twitter}, too, the FTC said the company failed to establish policies that prohibited employees from storing administrative passwords in plain text in personal email accounts.

\textbf{Again, businesses may want to consider other protections such as two-factor authentication that can help protect against password compromises.}\textsuperscript{43}

\begin{flushright}
\textsuperscript{40} \textit{Id.} \\
\textsuperscript{42} \textit{Id.}
\end{flushright}
In the *Lookout Services*, *Twitter*, and *Reed Elsevier* cases, the FTC alleged that the businesses didn’t suspend or disable user credentials after a certain number of unsuccessful login attempts. By not adequately restricting the number of tries, the companies placed their networks at risk.

Implementing a policy to suspend or disable accounts after repeated login attempts would help eliminate the risk.

B. Defend

*Layer protections so that cybersecurity will not fail completely due to one weakness.*

This should include all digital devices, from desktop computers to smartphones, connected to the network, especially devices with broadband (high speed) access to the Internet which is always “on.”

*Secure them with multiple layers of defensive technologies that include, but are not limited to, antivirus, anti-spyware, anti-phishing, and firewall technology.*

Vendors now offer subscriptions to “security service” applications which provide multiple layers of protection of security protection.

*Once installed, keep all operating systems and software up to date. Otherwise, the protective software installed is no protection to the business.*

- This is especially true with a newly purchased computer.
- Out of date operating systems and office software such as Microsoft Office or Adobe can cause a weak link in data security as well and also must be patched and updated on a regular basis.
- Remember to remove or uninstall software the entity is no longer using.

In *Lifelock*, the FTC charged that the company failed to install antivirus programs on the computers that employees used to remotely access its network.

In the *TJX Companies* case, for example, the FTC alleged that the company did not update its anti-virus software, increasing the risk that hackers could exploit known vulnerabilities or overcome the business’s defenses. Depending on the complexity of the

---

45 *Id.*
46 *Id.*
network or software, the entity may need to prioritize patches by severity; nonetheless, having a reasonable process in place to update and patch third party software is an important step to reducing the risk of a compromise.\(^{48}\)

**Don’t install software from untrusted or unknown sources and be leery of suggestions to update software which was recently updated.**\(^{49}\)

**When privacy and data protections are in place, make sure they work!**

In *TRENDnet*, for example, the FTC charged that the company failed to test that an option to make a consumer’s camera feed private would, in fact, restrict access to that feed. As a result, hundreds of “private” camera feeds were publicly available. Similarly, in *Snapchat*, the company advertised that messages would “disappear forever,” but the FTC said the company failed to ensure the accuracy of that claim.\(^{50}\)

In more than a dozen FTC cases, businesses failed to adequately assess their applications for well-known vulnerabilities. For example, in the *Guess?* case, the FTC alleged that the business failed to assess whether its web application was vulnerable to Structured Query Language (SQL) attacks. As a result, hackers were able to gain access to databases with consumers’ credit card information. That’s a risk that could have been avoided by testing for commonly-known vulnerabilities, like those identified by the Open Web Application Security Project (OWASP).\(^{51}\)

**C. Manage Vendors**

**Entities may choose to outsource portions of their operation which receive or manage sensitive data and personal information. Delegating data management or data protection to a third party does not lessen responsibility.**

Entities are responsible for the actions of vendors with whom they contract to collect, analyze, catalog or otherwise provide data management services on the company’s behalf, but the vendors are also responsible.

Likewise, the claims in a privacy policy also apply to third parties when they are working with an organization’s data.

---

\(^{48}\) *Id.*  
\(^{51}\) *Id.*
Be careful choosing vendors. The following clauses may be helpful in ensuring contractors and vendors are complying with privacy policy and data protection practices:

1. Confidentiality
2. No further use of shared information beyond the terms of the contract
3. Subcontractors must comply with the company's privacy and applicable cybersecurity policies.
4. Requirement to notify and to disclose breach
5. Ownership of data
6. Potential liability

D. Bank Securely

It is essential that small business owners put security first when they engage in online banking. This means that online banking should only be performed using a secure browser connection (indicated by “https” and/or a lock visible in the address bar or in the lower right corner of the web browser window). Online banking sessions should be conducted in the private mode of the web browser, and a person should erase the web browser cache, temporary Internet files, cookies, and history afterwards so that if the system is compromised that information will not be accessible to cybercriminals. In addition, take advantage of the security options offered by financial institutions. Examples include using two–factor authentication to access the account, requiring two authorized individuals to sign off on every transfer of funds, and setting up account notifications by email or text message when certain higher–risk activities occur on the account.

Also, set limits on wire transfers. Sophisticated transnational criminal organizations are now routinely hacking businesses’ computers and wiring large sums overseas where they cannot be recovered. To prevent this, set limits on the amount that can be wired from accounts, and (depending on business needs) consider asking the bank to require two executive team signatures before sending wire transfers overseas.

---

52 Swire & Ahmad, U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals ch. 3.
54 Id.
Most banks offer customers the ability to set up text or email notifications to alert them to certain activities on their account.\textsuperscript{55} Lastly, do not allow a single individual to both initiate and approve financial transactions. The unfortunate truth is that insiders, intentionally or not, are the source of most security incidents in the business.\textsuperscript{56}

IV. Communicate

Entities must assure effective communication to internal and external audiences. Internal audiences must be trained on policies and procedures, with individual accountability for compliance. Employees interacting with consumers must know, implement, and be able to explain the policies.

Privacy policies must be up to date and accessible in the place of business and online if the entity has an online presence. It is important that the written policy reflects the actual practices.\textsuperscript{57}

\textit{Educate Employees}

\textbf{Good policies and practices do not exist if employees do not understand and implement them.} Likewise, encryption and defensive software may offer no protection whatsoever if an employee responds to or activates a link on a phishing email.

Educate employees as to why it is important to never click on a hyperlink, or open a file, from an unknown or untrusted source.

\textbf{Employees need to understand that even if they do not have access to data they would consider valuable, they can still be targeted as an avenue to access another computer that does have valuable data.}\textsuperscript{58}

Raise employees’ awareness about the risks of cyber threats, mechanisms for mitigating the risk, and the value of the businesses’ intellectual property and data so that they can alert administration promptly if they notice anything out of the ordinary or if data is compromised. Also, advise employees to refer requests for customer information to designated individuals.\textsuperscript{59}

\textsuperscript{55} Id.
\textsuperscript{56} Id.
\textsuperscript{57} Swire & Ahmad, \textit{U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals} ch. 3.
Employees are the first line of defense, and good security training and procedures can reduce the risk of accidental data loss and other insider risks.\textsuperscript{60} Furthermore, they need to understand that data protection is the law.

Every employee must take information security seriously. After their training, employees should be requested to sign a statement that they understand the policies, that they will follow them, and that they understand the penalties for not following those policies.\textsuperscript{61} In addition, post reminders about employee responsibilities.

Training employees in the fundamentals of cybersecurity is one of the most effective investments one can make toward better cybersecurity.\textsuperscript{62}

Lastly, it is important to keep information out of the hands of rogue or spiteful employees who may steal or sell information by performing background checks of varying degrees depending on their access to customer information and by immediately deactivating their passwords and user names upon employee termination.\textsuperscript{63}

\textbf{V. Evolve}

The technology and nature of cyber-attacks are rapidly evolving, and attacks are unfortunately on the rise. Attackers are steadily inventing ways to infiltrate software, networks, and devices. Therefore, data protection must also evolve, and no guide or advice is ever complete as a result. Regularly monitoring cybersecurity updates on the resources listed at the beginning of this Guide may help entities stay up to date.

Practices that might have kept data reasonably secure one year may not be adequate the next. Information uses evolve in response to the change in technology, laws, conditions and other factors. Thus, it is important to establish a process to review and update the current information management program.\textsuperscript{64}

When updating and revising a privacy policy, make sure the update occurs systematically and is reposted physically and electronically. Additionally, privacy policies should reflect the policy revision date along with a version number, if used.

\textsuperscript{61} \textit{Id}.
\textsuperscript{62} \textit{Id}.
\textsuperscript{63} Ill. Atty Gen., Information Security and Security Breach Notification Guidance.
\textsuperscript{64} Swire & Ahmad, \textit{U.S. Private-sector Privacy: Law and Practice for Information Privacy Professionals} ch. 3.
RESPONDING TO SECURITY BREACHES

*Create a plan in advance to respond to data breaches.*

Identify a core response group that can be convened in the event of a breach to evaluate the situation and help guide further response.

Before a breach occurs, talk to private companies that offer credit monitoring to discuss options. Credit monitoring may not be appropriate in all breach situations depending on the type of data compromised and manner of breach, but consumers have come to expect free credit monitoring which helps them identify if their identities have been stolen.

Plan in advance how to notify the public and how to respond to inquiries.

- Impacted consumers should be notified pursuant to state and federal law. *Adequately notify them as soon as feasible so that consumers can take steps to protect themselves.*
  
  o Under Mississippi law, if a business experiences a breach and the breach appears to be for fraudulent purposes or could cause harm to those affected, then the business must give notice to those whose personal information was disclosed.
  
  o If personal information is in the hands of an unauthorized party or is accessible to them, then harm is possible.

- Depending on the size of the breach, a call center staffed with individuals prepared to answer the most frequently asked questions may be necessary since many businesses and agencies do not have the capability to respond to thousands of inquiries.

- Include Attorney General or other law enforcement identity theft resources and contacts.

Responding to a data breach can be costly. Data breach insurance may be an option to assist the entity in a potential breach.

*Upon discovery of a breach, take the following steps.*

1. Notify the internal response team of the nature of the breach.
2. Assess what happened and begin to implement a pre-set plan to notify and assist consumers.

3. Immediately secure the data and isolate the compromised area.

4. Involve law enforcement, such as local police, the FBI, the U.S. Secret Service, and the state Attorney General.
   - It might be prudent to notify law enforcement first, if an intruder has hacked into the computer network and the entity suspects that the intruder is still present in the system. Although one does not want additional information to be compromised, entities also want to give law enforcement an opportunity to learn more about the thief while he is actively stealing data.
   - *Cooperate in any law enforcement investigation.*

5. Consider hiring an outside forensic analyst to determine the extent of the breach and the individuals affected.

6. If handling the data for another entity, immediately contact them and any other entities from which data was obtained.
MISSISSIPPI LAW ON DATA BREACHES - MISS. CODE ANN. § 75-24-29

(1) This section applies to any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state.

(2) For purposes of this section, the following terms shall have the meanings ascribed unless the context clearly requires otherwise:

(a) “Breach of security” means unauthorized acquisition of electronic files, media, databases or computerized data containing personal information of any resident of this state when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable;

(b) “Personal information” means an individual's first name or first initial and last name in combination with any one or more of the following data elements:

(i) Social security number;

(ii) Driver's license number or state identification card number; or

(iii) An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; “personal information” does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media;

(iv) “Affected individual” means any individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.

(3) A person who conducts business in this state shall disclose any breach of security to all affected individuals. The disclosure shall be made without unreasonable delay, subject to the provisions of subsections (4) and (5) of this section and the completion of an investigation by the person to determine the nature and scope of the incident, to identify the affected individuals, or to restore the reasonable integrity of the data system. Notification shall not be required if, after an appropriate investigation, the person reasonably determines that the breach will not likely result in harm to the affected individuals.

(4) Any person who conducts business in this state that maintains computerized data which includes personal information that the person does not own or license shall notify the owner or licensee of the information of any breach of the security
of the data as soon as practicable following its discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person for fraudulent purposes.

(5) Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation or national security and the law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after the law enforcement agency determines that notification will not compromise the criminal investigation or national security and so notifies the person of that determination.

(6) Any notice required by the provisions of this section may be provided by one of the following methods: (a) written notice; (b) telephone notice; (c) electronic notice, if the person's primary means of communication with the affected individuals is by electronic means or if the notice is consistent with the provisions regarding electronic records and signatures set forth in 15 USCS 7001; or (d) substitute notice, provided the person demonstrates that the cost of providing notice in accordance with paragraph (a), (b) or (c) of this subsection would exceed Five Thousand Dollars ($5,000.00), that the affected class of subject persons to be notified exceeds five thousand (5,000) individuals or the person does not have sufficient contact information. Substitute notice shall consist of the following: electronic mail notice when the person has an electronic mail address for the affected individuals; conspicuous posting of the notice on the Web site of the person if the person maintains one; and notification to major statewide media, including newspapers, radio and television.

(7) Any person who conducts business in this state that maintains its own security breach procedures as part of an information security policy for the treatment of personal information, and otherwise complies with the timing requirements of this section, shall be deemed to be in compliance with the security breach notification requirements of this section if the person notifies affected individuals in accordance with the person's policies in the event of a breach of security. Any person that maintains such a security breach procedure pursuant to the rules, regulations, procedures or guidelines established by the primary or federal functional regulator, as defined in 15 USCS 6809(2), shall be deemed to be in compliance with the security breach notification requirements of this section, provided the person notifies affected individuals in accordance with the policies or the rules, regulations, procedures or guidelines established by the primary or federal functional regulator in the event of a breach of security of the system.
(8) Failure to comply with the requirements of this section shall constitute an unfair trade practice and shall be enforced by the Attorney General; however, nothing in this section may be construed to create a private right of action.

FINALLY, WHAT NOT TO DO...

- Don't install software from untrusted or unknown sources.
- Don't delay in updating software, especially defensive software.
- Don't open links in emails unless they are positively trustworthy.
- Don't respond to suspicious or unknown soliciting emails.
- Don't leave sensitive data and personal information unencrypted.
- Don't assume employees already know all of this.
- Don’t assume a breach will not happen!
APPENDIX A

Children’s Online Privacy Protection Act (COPPA)

The Children’s Online Privacy Protection Act (COPPA) spells out what operators of websites and online services must do to protect children’s privacy and safety online and is enforced by the Federal Trade Commission (FTC.)

Effective July 1, 2013, the FTC updated the COPPA Rule to reflect changes in technology. Violations can result in law enforcement actions.

The following is a step-by-step guide for determining if a company is covered by COPPA and how to comply with the Rule.

OUTLINE:

- Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Children under 13.
- Step 2: Post a Privacy Policy that Complies with COPPA.
- Step 3: Notify Parents Directly Before Collecting Personal Information from Their Children.
- Step 4: Get Parents' Verifiable Consent before Collecting Information from Their Children.
- Step 5: Honor Parents’ Ongoing Rights with Respect to Information Collected from Their Children.
- Step 6: Implement Reasonable Procedures to Protect the Security of Children’s Personal Information.

STEP 1: DETERMINE IF YOUR COMPANY IS A WEBSITE OR ONLINE SERVICE THAT COLLECTS PERSONAL INFORMATION FROM CHILDREN UNDER 13.

COPPA applies to operators of websites and online services that collect personal information from children under 13. Here’s a more specific way of determining if COPPA applies to you. You must comply with COPPA if:

Your website or online service is directed to children under 13 and you or a third party collects personal information from them. A website or online service must comply if it is directed to a general audience, but the operator has actual knowledge that personal information is collected from children under 13.

---

“Website or online service” is defined broadly and includes the following:

- mobile apps that send or receive information online,
- internet-enabled gaming platforms,
- advertising networks,
- internet-enabled location-based services, and
- voice-over internet protocol services.

The FTC looks at a variety of factors to see if a site or service is directed to children under 13, including the content, the use of animated characters or other child-oriented activities, the age of models, the presence of child celebrities, ads on the site or service that are directed to children, and other reliable evidence about the age of the actual or intended audience.

“Personal information” under COPPA is broader than Personal Information under other laws. Each of these is considered personal information under COPPA:

- full name;
- home or other physical address, including street name and city or town,
- online contact information like an email address or other identifier that permits someone to contact a person directly
- screen name or user name where it functions as online contact information;
- telephone number;
- Social Security number;
- a persistent identifier that can be used to recognize a user over time and across different sites, including a cookie number, an IP address, a processor or device serial number, or a unique device identifier;
- a photo, video, or audio file containing a child’s image or voice;
- geolocation information sufficient to identify a street name and city or town; or
- other information about the child or parent that is collected from the child and is combined with one of these identifiers.

Under COPPA, an entity is collecting information if they:

- request, prompt, or encourage the submission of information, even if it’s optional;
• let information be made publicly available (for example, with an open chat or posting function) unless you take reasonable measures to delete all or virtually all personal information before postings are public and delete all information from its records; or
• passively track a child online.

The FTC states:

if another company collects personal information through your child-directed site or service — through an ad network or plug-in, for example — you’re responsible for complying with COPPA. If you have actual knowledge that you’re collecting personal information directly from users of a child-directed site or service, you’re responsible for complying with COPPA, too.

STEP 2: POST A PRIVACY POLICY THAT COMPLIES WITH COPPA.

If a website or internet-based service is covered by COPPA, the next step is to post a privacy policy. It must clearly and comprehensively describe how personal information collected online from children under 13 is handled. The notice must include the practices of any others collecting personal information from the site or service — for example, plug-ins or ad networks.

Include a link to the privacy policy on the homepage and anywhere personal information is collected from children. If there is a separate section for children, post a link to the privacy policy on the homepage of the children’ part of the site or service.

Make those links clear and prominent.

To comply with COPPA, the privacy policy should be clear and easy to read.

Privacy Policy Requirements:

• A list of all operators collecting personal information
• A description of the personal information collected and how it’s used.
• A description of parental rights, including:
  o that the site will not require a child to disclose more information than is reasonably necessary to participate in an activity;
  o that they can review their child’s personal information, direct the site to delete it, and refuse to allow any further collection or use of the child’s information;
that they can agree to the collection and use of their child’s information, but still not allow disclosure to third parties unless that’s part of the service (for example, social networking); and

- the procedures to follow to exercise their rights.

**STEP 3: NOTIFY PARENTS DIRECTLY BEFORE COLLECTING PERSONAL INFORMATION FROM THEIR CHILDREN.**

COPPA requires that the site give parents “direct notice” before collecting information from their children. In addition, if the operator makes a material change to the practices parents previously agreed to, they have to send an updated direct notice.

The notice should be clear and easy to read. Don’t include any unrelated or confusing information. The notice must tell parents:

- that the site collected their online contact information for the purpose of getting their consent;
- that the site wants to collect personal information from their child;
- that their consent is required for the collection, use, and disclosure of the information;
- the specific personal information and how it might be disclosed to others;
- a link to the online privacy policy;
- how the parent can give their consent; and
- that if the parent doesn’t consent within a reasonable time, the parent’s online contact information will be deleted.

In certain circumstances, it’s okay under COPPA to collect a narrow class of personal information without getting parental consent although direct notice is still required.

**STEP 4: GET PARENTS’ VERIFIABLE CONSENT BEFORE COLLECTING INFORMATION FROM THEIR CHILDREN.**

Before collecting, using or disclosing personal information from a child, the site must get their parent’s verifiable consent.

Acceptable methods provided by the FTC include:

- sign a consent form and send it back via fax, mail, or electronic scan;
use a credit card, debit card, or other online payment system that provides notification of each separate transaction to the account holder;

• call a toll-free number staffed by trained personnel;

• connect to trained personnel via a video conference; or

• provide a copy of a form of government issued ID to check against a database, as long as it is deleted from the site's records when the verification process is complete.

If the site uses a child’s personal information only for internal purposes and won’t disclose it, the operator may use a method known as “email plus” where the operator sends an email to the parent and have them respond with their consent followed by confirmation to the parent via email, letter, or phone call. If email plus is used, the operator must let the parent know they can revoke their consent anytime.

Parents must have the option of allowing the collection and use of their child's personal information without agreeing to disclosing that information to third parties. If changes are made to the collection, use, or disclosure practices the parent already agreed to, the parent must receive a new notice and give consent again.


**STEP 5: HONOR PARENTS’ ONGOING RIGHTS WITH RESPECT TO INFORMATION COLLECTED FROM THEIR CHILDREN.**

Even if parents have agreed to information collected from their children, they still have ongoing rights.

If a parent asks, the operator must:

• give them a way to review the personal information collected from their child;

• give them a way to revoke their consent and refuse the further use or collection of personal information from their child; and

• delete their child’s personal information.

Any time you’re communicating with a parent about personal information already collected from their child, take reasonable steps to ensure the person is actually the parent or guardian. At the same time, make sure the method isn’t unduly burdensome on the parent. Under COPPA, it may be okay to terminate a service to a child if the
parent revokes consent, but only if the information at issue is reasonably necessary for the child’s participation in that activity.

STEP 6: IMPLEMENT REASONABLE PROCEDURES TO PROTECT THE SECURITY OF CHILDREN’ PERSONAL INFORMATION.

COPPA requires a site or internet-based service to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

- Minimize what is collected in the first place.
- Take reasonable steps to release personal information only to service providers and third parties capable of maintaining its confidentiality, security, and integrity and get assurances they’ll live up to those responsibilities.
- Hold on to personal information only as long as is reasonably necessary for the purpose for which it was collected. Securely dispose of it once there is no longer a legitimate reason for retaining it.

For more information about the Children’s Online Privacy Protection Rule, visit the Children’s Privacy page of the FTC’s Business Center or their Complying with COPPA: Frequently Asked Questions. See also OnGuard Online.gov for general information about protecting children’ privacy online.
APPENDIX B

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education.\(^1\)

FERPA gives parents the following rights with respect to their children's education records:

- Parents or eligible students have the right to inspect and review the student's education records maintained by the school.
  - Schools are not required to provide copies of records unless, for reasons such as great distance, it is impossible for parents or eligible students to review the records. Schools may charge a fee for copies.

- Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading.
  - If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible student has the right to place a statement with the record setting forth his or her view about the contested information.

- Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record.
  - However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):
    a) School officials with legitimate educational interest;
    b) Other schools to which a student is transferring;
    c) Specified officials for audit or evaluation purposes;
    d) Appropriate parties in connection with financial aid to a student;

e) Organizations conducting certain studies for or on behalf of the school;
f) Accrediting organizations;
g) To comply with a judicial order or lawfully issued subpoena;
h) Appropriate officials in cases of health and safety Emergencies, and
i) State and local authorities, within a juvenile justice system, pursuant to specific State law.

These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.

**Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance.**

Please note they must still tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose it.

**Schools must notify parents and eligible students annually of their rights under FERPA.**
The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Decision and Order (“Order”):
1. Respondent Accretive Health, Inc. (“Accretive Health” or “Respondent”) is a Delaware corporation with its principal executive office located at 401 North Michigan Avenue, Suite 2700, Chicago, Illinois.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

I.

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Accretive Health, and its successors and assigns.

2. “Personal Information” means individually identifiable information from or about an individual consumer, including but not limited to: (a) a first and last name; (b) a home or other physical address; (c) an email address or other online contact information, such as instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) an insurance account number or other insurance information; (i) credit or debit card information; (j) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, or a processor serial number; or (k) any information that is combined with any of (a) through (j) above.


II.

IT IS ORDERED that respondent shall, no later than the date of entry of this Order, establish and implement, and thereafter maintain, or continue to maintain a comprehensive information security program reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:
1. The designation of an employee or employees to coordinate and be accountable for the information security program;

2. The identification of material internal and external risks to the security, confidentiality and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and the assessment of the sufficiency of any safeguards in place to control the risks. At a minimum, this risk assessment should include consideration of the risks in each relevant area of operations, including but not limited to: (a) employee training and management; (b) information systems, including network and software design, information processing, storage, transmission, and disposal; and (c) prevention, detection, and response to attacks, intrusions, and other system failures;

3. The design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing and monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

4. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

5. The evaluation and adjustment of the information security program in light of the results of the testing and monitoring required by Paragraph 3 of this Section, any material changes to operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have material impact on the effectiveness of the information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance of Section II of the Order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) of respondent from a qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: (a) a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); (b) a person holding Global Information Assurance Certification (GIAC) from the System Administrator, Audit, Network, Security (SANS) Institute; or (c) a similarly qualified person or organization approved by the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. The reporting period for the Assessments shall cover (i) the first one hundred and eighty (180) days after service of the Order for the Initial Assessment and (ii) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:
1. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

2. Explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

3. Explain how the safeguards that have been implemented meet or exceed the protections required by Section II of the Order; and

4. Certify that Respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director of Enforcement, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the Order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, initial and biennial Assessments shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580, with the subject line FTC v. Accretive Health, Inc., FTC File Number 1223077. Provided, however, that in lieu of overnight courier, an Assessment may be sent by first class mail, but only if an electronic version of such Assessment is contemporaneously sent to the Commission at DEBrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that Respondent shall maintain and, upon request, make available to the Commission for inspection and copying:

1. For a period of three (3) years after the date of preparation of each Assessment required under Section III of the Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Respondent’s compliance with Section II of this order, for the compliance period covered by such Assessment;

2. Unless covered by IV.1, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this Order, including but not limited to documents, whether prepared by or on behalf of Respondent, that contradict, qualify, or call into question compliance with the Order.
V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Accretive Health, Inc., FTC File No. 1223077. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that Respondent, within sixty (60) days after the date of service of this Order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this Order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on February 5, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:
1. Any part in this Order that terminates in less than twenty (20) years; and

2. this order’s application to any respondent that is not named as a defendant in such complaint; and

3. This order if such complaint is filed after the order has terminated pursuant to this part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: February 5, 2014
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

In the Matter of                             ) FILE NO. 0423160
) AGREEMENT CONTAINING
BJ'S WHOLESALE CLUB, INC., a corporation.     ) CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of BJ’s Wholesale Club, Inc., a Delaware corporation (“proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between BJ’s Wholesale Club, Inc., by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent BJ’s Wholesale Club, Inc. is a Delaware corporation with its principal office or place of business at One Mercer Road, Natick, Massachusetts 01760.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:
   
   A. any further procedural steps;

   B. the requirement that the Commission’s decision contain a statement of findings of fact and conclusions of law; and

   C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter
may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission’s Rules, the Commission may, without further notice to proposed respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent’s address as stated in this agreement by any means specified in Section 4.4(a) of the Commission’s Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and data stored on the magnetic stripe of a credit or debit card; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with
other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, “respondent” shall mean BJ’s Wholesale Club, Inc. and its successors and assigns, officers, agents, representatives, and employees.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent’s operations or business
arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that respondent obtain an assessment and report (an “Assessment”) from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one hundred and eighty (180) days after service of the order, and biennially thereafter for twenty (20) years after service of the order that:

A. sets forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explains how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and

D. certifies that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the first Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.
III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent’s compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.
VI.

**IT IS FURTHER ORDERED** that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

*Provided, further*, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Signed this seventeenth day of May, 2005

BJ’s WHOLESALE CLUB, INC.

By: ______________________

BJ’s WHOLESALE CLUB, INC.

______________________

DAVID MEDINE

JAMES W. PRENDERGAST

Wilmer Cutler Pickering Hale and Dorr LLP

Counsel for respondent BJ’s Wholesale Club, Inc.
FEDERAL TRADE COMMISSION

By: ______________________
    ALAIN SHEER
    Counsel for the Federal Trade Commission

APPROVED:

______________________________
JOEL WINSTON
Associate Director
Division of Financial Practices

______________________________
LYDIA B. PARNES
Director
Bureau of Consumer Protection
The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent and its successor corporation, Solidus Networks, Inc., doing business as Pay By Touch Solutions, having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, its successor corporation, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent and its successor corporation of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent or its successor corporation that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and
The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Respondent CardSystems Solutions, Inc. is a Delaware corporation with its principal office or place of business at 6390 East Broadway, Tucson, Arizona 85710.

Solidus Networks, Inc, doing business as Pay By Touch Solutions, is a Delaware corporation with its principal office or place of business at 101 2nd St Ste 1500, San Francisco, California 94105.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent and Solidus Networks, Inc., and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and data stored on a card’s magnetic stripe; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, “respondent” shall mean CardSystems Solutions, Inc. and its successors and assigns, including Solidus Networks, Inc., officers, agents, representatives, and employees.
I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order.
for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after
service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that
respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity,
the nature and scope of respondent’s activities, and the sensitivity of the personal
information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the
protections required by Paragraph I of this order; and

D. certify that respondent’s security program is operating with sufficient
effectiveness to provide reasonable assurance that the security, confidentiality, and
integrity of personal information is protected and has so operated throughout the reporting
period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the
reporting period to which the Assessment applies by a person qualified as a Certified Information
System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a
person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit,
Network, Security (SANS) Institute; or a similarly qualified person or organization approved by
the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews,
audits, audit trails, policies, training materials, and assessments, whether prepared by or on
behalf of respondent, relied upon to prepare such Assessment to the Associate Director for
20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial
Assessments shall be retained by respondent until the order is terminated and provided to the
Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make
available to the Federal Trade Commission for inspection and copying, a print or electronic copy
of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of
respondent, that contradict, qualify, or call into question respondent’s compliance with
this order; and
B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph II of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent’s compliance with Paragraphs I and II of this order for the compliance period covered by such biennial Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on September 5, 2026, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order,
whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Harbour recused.

Donald S. Clark
Secretary

SEAL:
ISSUED: September 5, 2006
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Edith Ramirez, Chairwoman
Julie Brill
Maureen K. Ohlhausen
Joshua D. Wright

In the Matter of

CBR SYSTEMS, INC.

DOCKET NO. C-4400

DECISION AND ORDER

The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft of complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by respondent that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment filed by an interested person, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:
1. Respondent Cbr Systems, Inc. is a California corporation with its principal office or place of business at 1200 Bayhill Drive, Suite 301, San Bruno, California 94066.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER
DEFINITIONS

For purposes of this order, the following definitions shall apply:


3. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) a bank account, debit card, or credit card account number; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number; (i) clinical laboratory testing information, including test results; or (j) the fact and circumstances of a child’s adoption, such as whether the birth mother was a surrogate. For the purpose of this provision, a “consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which it uses, maintains, and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.
II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers by respondent or by any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent. This section may be satisfied through the review and maintenance of an existing program so long as that program fulfills the requirements set forth herein. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of the information security program in light of the results of the testing and monitoring required by subpart C, any material changes to any operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the information security program.
III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SANS Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that the security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Cbr Systems, Inc., FTC File No.1123120. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.
IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment;

B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this order, including but not limited to:

1. all advertisements and promotional materials containing any representations covered by this order, with all materials used or relied upon in making or disseminating the representation; and

2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver copies of the order as directed below:

A. Respondent shall deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

B. Respondent shall secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.
VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Cbr Systems, Inc., FTC File No.1123120. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on April 29, 2033, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: April 29, 2013
The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:
1. Respondent Credit Karma, Inc. (“Credit Karma”) is a Delaware corporation with its principal office or place of business at 115 Sansome Street, Suite 400, San Francisco, CA 94104.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Credit Karma, Inc. and its successors and assigns.


3. “Covered information” shall mean information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) credit report information; (j) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (k) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (l) an authentication credential, such as a username or password; or (m) any communications or content that is input into, stored on, captured with, or accessed through a computer, including but not limited to contacts, emails, SMS messages, photos, videos, and audio recordings.

4. “Computer” shall mean any desktop, laptop computer, tablet, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

5. “Client software” shall mean any program or application developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent, that is installed locally on a consumer’s computer and that communicates with a server.
I.

**IT IS ORDERED** that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information.

II.

**IT IS FURTHER ORDERED** that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity, and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent’s products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, or accessed through a computer using respondent’s products or services, and assessment of the sufficiency of any safeguards in place to control these risks.

C. at a minimum, the risk assessment required by Subpart B should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, including in secure engineering and defensive programming; (2) product design, development and research; (3) secure software design, development, and testing; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

D. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures, including through reasonable and appropriate software security testing techniques;
E. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards;

F. the evaluation and adjustment of respondent’s security program in light of the results of the testing and monitoring required by subpart B, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, for any product or service offered through client software, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of covered information is protected and has so operated throughout the reporting period.
Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Credit Karma, Inc.*, FTC File No. 1323091. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

**IT IS FURTHER ORDERED** that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment;

B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:

   i. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and

   ii. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order.
V.

**IT IS FURTHER ORDERED** that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line *In the matter of Credit Karma, Inc.*, FTC File No. 1323091. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

**IT IS FURTHER ORDERED** that respondent, within one hundred twenty (120) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

VIII.

This order will terminate on August 13, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:
A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner McSweeny not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: August 13, 2014
The Federal Trade Commission (“Commission”) has conducted an investigation of certain acts and practices of CVS Caremark Corporation (“proposed respondent”). Proposed respondent, having been represented by counsel, is willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

**IT IS HEREBY AGREED** by and between CVS Caremark Corporation, by its duly authorized officers, and counsel for the Federal Trade Commission that:

1. Proposed respondent CVS Caremark Corporation is a Delaware corporation with its principal office or place of business at One CVS Drive, Woonsocket, Rhode Island, 02895.

2. Proposed respondent admits all the jurisdictional facts set forth in the draft complaint.

3. Proposed respondent waives:
   
   (a) Any further procedural steps;
   
   (b) The requirement that the Commission’s decision contain a statement of findings of fact and conclusions of law; and

   (c) All rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

4. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of
thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

5. This agreement is for settlement purposes only and does not constitute an admission by proposed respondent that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true. Proposed respondent expressly denies the allegations set forth in the draft complaint, except for the jurisdictional facts, and expressly denies that the law has been violated.

6. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission’s Rules, the Commission may, without further notice to proposed respondent: (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondent’s address as stated in this agreement by any means specified in Section 4.4(a) of the Commission’s Rules shall constitute service. Proposed respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

7. Proposed respondent has read the draft complaint and consent order. It understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “store” shall mean each pharmacy entity or store location that sells prescription medicines, drugs, devices, supplies, or services and/or non-prescription products and services.

2. Unless otherwise specified, “LLC” shall mean a limited liability company: (a) that owns, controls, or operates one or more stores (including, but not limited to, the companies identified in attached Exhibit A), and (b) in which CVS Caremark Corporation is a
member, directly or indirectly.

3. Unless otherwise specified, “respondent” shall mean CVS Caremark Corporation, its subsidiaries, divisions, affiliates, and LLCs, and its successors and assigns.

4. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above. For the purpose of this provision, a “consumer” shall include an “employee,” and an individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, and other person directly or indirectly under the control of respondent.


I.

IT IS ORDERED that respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and
complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with their compliance with Part II of this order, respondent, and its officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first year after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and
complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent CVS Caremark Corporation shall deliver a copy of this order to all its current and future subsidiaries (including LLCs and each store that is
owned, controlled, or operated by respondent or an LLC), current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within sixty (60) days after service of this order, and to such future subsidiaries and personnel within sixty (60) days after the respondent acquires the subsidiary or the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary (including an LLC), parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in respondent’s name or address. Provided, however, that, with respect to any proposed change in respondent about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent shall, within ninety (90) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VIII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

CVS CAREMARK CORPORATION

Dated: _______ By:__________________________________
DIANE NOBLES
Senior Vice President and Chief Compliance Officer
CVS Caremark Corporation

Dated: _______ By:__________________________________
ANTHONY E. DIRESTA
Reed Smith L.L.P.
Counsel for respondent CVS Caremark Corporation

FEDERAL TRADE COMMISSION

Dated: _______ By:__________________________________
LORETTA H. GARRISON

__________________________
KRISTIN K. COHEN

__________________________
ALAIN SHEER

Counsel for the Federal Trade Commission

APPROVED:

__________________________
JESSICA RICH
Assistant Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection

-7-
JOEL WINSTON
Associate Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection

EILEEN HARRINGTON
(Acting) Director
Bureau of Consumer Protection
The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:
1. Respondent is a Missouri corporation with its principal office or place of business at 2481 Manana Drive, Dallas, Texas 75220.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent and this proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number; (g) a credit card or debit card account number; (h) a persistent identifier, such as a customer number held in “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (i) any information that is combined with any of (a) through (h) above.

2. Unless otherwise specified, “respondent” shall mean Dave & Buster’s, Inc., and its subsidiaries, divisions, and affiliates owned or controlled by Dave & Buster’s, Inc. and the successors and assigns of Dave & Buster’s, Inc.


I.

IT IS ORDERED that respondent, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in
the unauthorized disclosure, misuse, loss, alteration, destruction, or other
compromise of such information, and assessment of the sufficiency of any
safeguards in place to control these risks. At a minimum, this risk
assessment should include consideration of risks in each area of relevant
operation, including, but not limited to: (1) employee training and
management; (2) information systems, including network and software
design, information processing, storage, transmission, and disposal; and
(3) prevention, detection, and response to attacks, intrusions, or other
systems failures;

C. the design and implementation of reasonable safeguards to control the
risks identified through risk assessment and regular testing or monitoring
of the effectiveness of the safeguards’ key controls, systems, and
procedures;

D. the development and use of reasonable steps to select and retain service
providers capable of appropriately safeguarding personal information they
receive from respondent, and requiring service providers by contract to
implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondent’s information security program in
light of the results of the testing and monitoring required by sub-Part C, any
material changes to respondent’s operations or business arrangements, or any
other circumstances that respondent knows or has reason to know may have a
material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this
order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from
a qualified, objective, independent third-party professional, who uses procedures and standards
generally accepted in the profession. The reporting period for the Assessments shall cover: (1)
the first one hundred and eighty (180) days after service of the order for the initial Assessment,
and (2) each two (2) year period thereafter for ten (10) years after service of the order for the
biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that
respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity,
the nature and scope of respondent’s activities, and the sensitivity of the personal
information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the
protections required by the Part I of this order; and
D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers at corporate headquarters, regional offices, and at each store having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.
V.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

**IT IS FURTHER ORDERED** that respondent shall, within ninety (90) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on May 20, 2030, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Ramirez not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: May 20, 2010
The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comment received from an interested person pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:
1. Respondent Fandango, LLC (“Fandango”) is a Delaware limited liability company with its principal office or place of business at 12200 W. Olympic Boulevard, Suite 400, Los Angeles, CA 90064.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Fandango, LLC and its successors and assigns.


3. “Covered information” shall mean information from or about an individual consumer, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (j) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; or (k) an authentication credential, such as a username or password.

4. “Computer” shall mean any desktop, laptop computer, tablet, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

5. “Client software” shall mean any program or application developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent, that is installed locally on a consumer’s computer and that communicates with a server.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent or its products or services maintain and protect the privacy, security, confidentiality, or integrity of any covered information.
II.

**IT IS FURTHER ORDERED** that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing products and services for consumers, and (2) protect the security, integrity and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent’s products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, or accessed through a computer using respondent’s products or services, and assessment of the sufficiency of any safeguards in place to control these risks.

C. at a minimum, this risk assessment required by Subpart B should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, including in secure engineering and defensive programming; (2) product design and development; (3) secure software design, development, and testing; (4) review, assessment, and response to third-party security vulnerability reports, and (5) prevention, detection, and response to attacks, intrusions, or systems failures;

D. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures, including through reasonable and appropriate software security testing techniques;

E. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards; and
F. the evaluation and adjustment of respondent’s security program in light of the results of the testing and monitoring required by subpart B, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, for any product or service offered through client software, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific controls and procedures that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of covered information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of
request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Fandango, LLC., FTC File No. 1323089. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment;

B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this order, including but not limited to:

   i. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and

   ii. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part
VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Fandango, LLC, FTC File No. 1323089. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

VIII.

This order will terminate on August 13, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner McSweeny not participating.

Donald S. Clark
Secretary

SEAL
ISSUED: August 13, 2014
The Federal Trade Commission (“Commission”) having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq.; and

The respondent, its attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order (“consent agreement”), which includes: a statement by the respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the consent agreement, and only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such consent agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:
1. Respondent foru™ International Corporation (“foru”), formerly known as GeneWize Life Sciences, Inc., is a Delaware corporation with its principal office or place of business at 1231 Greenway Drive, Suite 200, Irving, Texas 75038.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and this proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:


3. “Covered Product” means any drug, food, or cosmetic that is: (a) customized or personalized for a consumer based on that consumer’s DNA or SNP (single nucleotide polymorphism) assessment, including, but not limited to, LifeMap ME DNA Customized Nutritional Supplements, GeneWize Nutritional Supplements, LifeMap ME DNA Customized Skin Repair Serum, foru™ Core Plus, GeneWize Customized Skin Repair Serum, and foru™ Skin Repair Serum; or (b) promoted to modulate the effect of genes.

4. “Covered Assessment” means any genetic test or assessment, including, but not limited to, the Healthy Aging Assessment and LifeMap Healthy Aging Assessment.

5. “Essentially Equivalent Product” means a product that contains the identical ingredients, except for inactive ingredients (e.g., binders, colors, fillers, excipients), in the same form and dosage, and with the same route of administration (e.g., orally, sublingually), as the Covered Product; provided that the Covered Product may contain additional ingredients if reliable scientific evidence generally accepted by experts in the field demonstrates that the amount and combination of additional ingredients is unlikely to impede or inhibit the effectiveness of the ingredients in the Essentially Equivalent Product.


9. “Adequate and well-controlled human clinical study” means a human clinical study that: is randomized and adequately controlled; utilizes valid end points generally recognized by
experts in the relevant disease field; yields statistically significant between-group results; and is conducted by persons qualified by training and experience to conduct such a study. Such study shall be double-blind and placebo-controlled; provided, however, that any study of a conventional food need not be placebo-controlled or double-blind if placebo control or blinding cannot be effectively implemented given the nature of the intervention. For the purposes of this proviso, “conventional food” does not include any dietary supplement, any customized or personalized product based on a consumer’s DNA or SNP assessment, or any product promoted to modulate the effect of genes. Respondent shall have the burden of proving that placebo-control or blinding cannot be effectively implemented.

10. “Endorsement” means as defined in the Commission’s Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255.0.

11. “Affiliate” means any person or entity who participates in an Affiliate Program.

12. “Affiliate Program” means any arrangement whereby any person or entity: (a) provides respondent with, or refers to respondent, potential or actual customers; or (b) otherwise markets, advertises, or offers for sale any product or service on behalf of respondent.

13. “Personal Information” shall mean individually identifiable information from or about an individual consumer, including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a bank account, debit card, or credit card account number; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number; or (h) clinical laboratory testing information, including test results. For the purpose of this provision, a “consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

14. The term “including” in this order means “without limitation.”

15. The terms “and” and “or” in this order shall be construed conjunctively or disjunctively as necessary, to make the applicable phrase or sentence inclusive rather than exclusive.

I.

IT IS ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, licensee, affiliate, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any Covered Product, in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, including through the use of a product name, endorsement, depiction, illustration, trademark, or trade name, that such product is effective in the diagnosis, cure, mitigation, treatment, or prevention of any disease, including, but not limited to, any representation that the product will treat, prevent, mitigate, or reduce the risk of diabetes, heart
disease, arthritis, or insomnia, unless the representation is non-misleading and, at the time the representation is made, respondent possesses and relies upon competent and reliable scientific evidence that substantiates that the representation is true. For purposes of this Part I, “competent and reliable scientific evidence” shall consist of at least two adequate and well-controlled human clinical studies of the Covered Product, or of an Essentially Equivalent Product, conducted by different researchers, independently of each other, that conform to acceptable designs and protocols and whose results, when considered in light of the entire body of relevant and reliable scientific evidence, are sufficient to substantiate that the representation is true; provided that, if the respondent represents that such product is effective in the diagnosis, cure, mitigation, treatment, prevention, or the reduction of risk of disease for persons with a particular genetic variation or single nucleotide polymorphism (“SNP”), then studies required under this Part I shall be conducted on human subjects with such genetic variation or SNP. Respondent shall have the burden of proving that a product satisfies the definition of an Essentially Equivalent Product.

II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, licensee, affiliate, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any Covered Product or any Covered Assessment, in or affecting commerce, shall not make any representation, in any manner, expressly or by implication, including through the use of a product name, endorsement, depiction, or illustration, other than representations covered under Part I of this order, about the health benefits, performance, or efficacy of any Covered Product or any Covered Assessment, unless the representation is non-misleading, and, at the time of making such representation, respondent possesses and relies upon competent and reliable scientific evidence that is sufficient in quality and quantity based on standards generally accepted in the relevant scientific fields, when considered in light of the entire body of relevant and reliable scientific evidence, to substantiate that the representation is true. For purposes of this Part II, competent and reliable scientific evidence means tests, analyses, research, or studies that have been conducted and evaluated in an objective manner by qualified persons and are generally accepted in the profession to yield accurate and reliable results.

III.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, licensee, affiliate, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any Covered Product or any Covered Assessment, in or affecting commerce, shall not misrepresent, in any manner, directly or indirectly, expressly or by implication, including through the use of endorsements:

A. The existence, contents, validity, results, or conclusions of any test, study, or research; or
B. That the benefits of any Covered Product or Covered Assessment are scientifically proven.

IV.

IT IS FURTHER ORDERED that:

A. Nothing in Parts I through III of this order shall prohibit respondent from making any representation for any product that is specifically permitted in labeling for such product by regulations promulgated by the Food and Drug Administration pursuant to the Nutrition Labeling and Education Act of 1990 or permitted under Sections 303-304 of the Food and Drug Administration Modernization Act of 1997; and

B. Nothing in Parts I through III of this order shall prohibit respondent from making any representation for any drug that is permitted in labeling for such drug under any tentative final or final standard promulgated by the Food and Drug Administration, or any new drug application approved by the Food and Drug Administration.

V.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, licensee, affiliate, trade name, or other device, in connection with the manufacturing, labeling, advertising, promotion, offering for sale, sale, or distribution of any Covered Product or any Covered Assessment, in or affecting commerce, shall not provide to any person or entity the means and instrumentalities with which to make, directly or by implication, any representations prohibited by Parts I through III of this order. For purposes of this Part, “means and instrumentalities” shall mean any information, document, or article referring or relating to any Covered Product or any Covered Assessment, including, but not limited to, any advertising, labeling, promotional, or purported substantiation materials, for use by affiliates in their marketing of any Covered Product or any Covered Assessment in or affecting commerce.

VI.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, in connection with the manufacturing, advertising, labeling, promotion, offering for sale, sale, or distribution of any product or service, in or affecting commerce, shall take steps sufficient to ensure compliance with Parts I through III of this order. Such steps shall include, at a minimum:

A. Establishing, implementing, and thereafter maintaining a system to monitor and review its affiliates’ representations and disclosures to ensure compliance with Parts I through III of this order. The system shall be implemented as follows:
1. No later than thirty (30) days after the date of service of this order, and, on a semi-annual basis thereafter, respondent shall determine those affiliates that generate the most sales for respondent. For respondent’s top fifty (50) revenue-generating affiliates, respondent shall:

   (a) Monitor and review each affiliate’s web sites on at least a monthly basis at times not disclosed in advance to its affiliates and in a manner reasonably calculated not to disclose the source of the monitoring activity at the time it is being conducted; and

   (b) Conduct online monitoring and review of the Internet on at least a monthly basis, including, but not limited to, social networks such as Facebook, microsites such as Twitter, and video sites such as YouTube, for any representations by such affiliates.

2. For the remainder of respondent’s affiliates, no later than thirty (30) days after the date of service of this order, and, on a semi-annual basis thereafter, respondent shall select a random sample of fifty (50) affiliates. Respondent shall:

   (a) Monitor and review each of these randomly selected affiliates’ web sites on at least a monthly basis at times not disclosed in advance to its affiliates and in a manner reasonably calculated not to disclose the source of the monitoring activity at the time it is being conducted; and

   (b) Conduct online monitoring and review of the Internet on at least a monthly basis, including, but not limited to, social networks such as Facebook, microsites such as Twitter, and video sites such as YouTube, for any representations by such affiliates.

B. Within seven (7) days of reasonably concluding that an affiliate has made representations that the affiliate knew or should have known violated Parts I, II, or III of this order, respondent shall terminate the affiliate from any affiliate program and cease payment to the affiliate; provided, however, that nothing in this subpart shall prevent respondent from honoring respondent’s payment obligation to an affiliate pursuant to a contract executed by the affiliate and respondent prior to the date of service of the order; and

C. Creating, and thereafter, maintaining, and within fourteen (14) days of receipt of a written request from a representative of the Federal Trade Commission, making available for inspection and copying, reports sufficient to show compliance with this Part of the order.
VII.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, licensee, affiliate, trade name, or other device, in connection with the manufacturing, advertising, labeling, promotion, offering for sale, sale, or distribution of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of Personal Information collected from or about consumers.

VIII.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, partnership, subsidiary, division, trade name, or other device, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of Personal Information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the Personal Information respondent collects from or about consumers, including:

A. The designation of an employee or employees to coordinate and be accountable for the information security program;

B. The identification of material internal and external risks to the security, confidentiality, and integrity of Personal Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. The design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

D. The development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding Personal Information received from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. The evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subpart C, any
material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

IX.

IT IS FURTHER ORDERED that, in connection with its compliance with Part VIII of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of its activities, and the sensitivity of the Personal Information collected from or about consumers;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part VIII of this order; and

D. Certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of Personal Information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. The respondent shall provide its initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission in writing, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: In the Matter of foru™ International Corporation, FTC File No. 112 3095. Provided, however, that in lieu of overnight courier, notices may be sent by
first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

X.

IT IS FURTHER ORDERED that respondent foru™ International Corporation, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, directors, Scientific Advisory Board members, and licensees, and to employees having managerial responsibilities with respect to the subject matter of this order, and shall secure from each such person a signed and dated statement acknowledging receipt of the order. Respondent foru™ International Corporation, and its successors and assigns, shall deliver this order to current personnel within thirty (30) days after the date of service of this order, and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

XI.

IT IS FURTHER ORDERED that respondent foru™ International Corporation, and its successors and assigns, shall maintain and, upon request, make available to a representative to the Commission for inspection and copying:

A. For a period of three (3) years after the date of preparation of each Assessment required under Part IX of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts VIII and IX of this order, for the compliance period covered by such Assessment;

B. Unless covered by Part XI.A, for a period of five (5) years after the last date of dissemination of any representation covered by this order, maintain and upon reasonable notice make available to the Commission for inspection and copying:

1. All advertisements and promotional materials containing the representation, including, but not limited to, all marketing and training materials distributed to licensees and affiliates;

2. All materials that were relied upon in disseminating the representation; and

3. All tests, reports, studies, surveys, demonstrations, or other evidence in respondent’s possession or control that contradict, qualify, or call into question the representation, or the basis relied upon for the representation, including complaints and other communications with consumers or with governmental or consumer protection organizations.
XII.

IT IS FURTHER ORDERED that respondent foru™ International Corporation, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent foru™ International Corporation, and its successors and assigns, learns less than thirty (30) days prior to the date such action is to take place, respondent foru™ International Corporation, and its successors and assigns, shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission in writing, all notices required by this Part shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The subject line must begin: In the Matter of foru™ International Corporation, FTC File No. 112 3095.

XIII.

IT IS FURTHER ORDERED that respondent foru™ International Corporation, and its successors and assigns, within sixty (60) days after service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its own compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

XIV.

This order will terminate on May 8, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Ohlhausen dissenting, and Commissioner McSweeny not participating.

Donald S. Clark
Secretary

SEAL:

ISSUED: May 8, 2014

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Acts, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:
1. Respondent Goal Financial, LLC, (“Goal Financial”) is a California limited liability company with its principal office or place of business at 9477 Waples Street, Suite 100, San Diego, California, 92121.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) a bank, loan, or credit card account number; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any information that is combined with any of (a) through (g) above.


3. All other terms are synonymous in meaning and equal in scope to the usage of such terms in the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq, attached hereto as Appendix A or as may hereafter be amended.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the collection of personal information from or about consumers, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, or integrity of any personal information collected from or about consumers.
II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondent, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information.

E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.
III.

**IT IS FURTHER ORDERED** that respondent shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of:

A. the Standards for Safeguarding Customer Information Rule, 16 C.F.R. Part 314, as attached or as may be amended; or

B. the Privacy of Customer Financial Information Rule, 16 C.F.R. Part 313, as attached or as may be amended.

In the event that any of these Rules is hereafter amended or modified, respondent’s compliance with that Rule as so amended or modified shall not be a violation of this order.

IV.

**IT IS FURTHER ORDERED** that, in connection with its compliance with Parts II, and III.A. of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Parts II and III A. of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the
Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

V.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III.A. of this order, for the compliance period covered by such Assessment. Respondent shall provide such documents to the Associate Director of Enforcement within ten (10) days of request.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent and its successors and assigns shall notify the Commission at least thirty (30) days prior to any change in the limited liability company that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change
in the company name or address. Provided, however, that, with respect to any proposed change in the company about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

IT IS FURTHER ORDERED that respondent and its successors and assigns shall, within sixty (60) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

IX.

This order will terminate on April 9, 2028, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: April 9, 2008

Page 6 of 6
UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS: Timothy J. Muris, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle
Thomas B. Leary

In the Matter of

GUESS?, INC., a corporation,

and

GUESS.COM, INC., a corporation.

DOCKET NO. C-4091

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondents named in the caption hereof, and the Respondents having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondents with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq; and

The Respondents, their attorney, and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondents of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of said agreement is for settlement purposes only and does not constitute an admission by Respondents that the law has been violated as alleged in such complaint, or that the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules.

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondents have violated the said Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days, now in further conformity with the procedure described
in § 2.34 of its Rules, the Commission hereby issues its complaint, makes the following jurisdictional findings and enters the following order:

1. Respondent Guess?, Inc. is a Delaware corporation with its principal office or place of business at 1444 S. Alameda Street, Los Angeles, California 90021. Respondent Guess.com, inc. is a Delaware corporation and a wholly-owned subsidiary of Respondent Guess?, Inc. Its principal office or place of business is at 1444 S. Alameda Street, Los Angeles, California 90021.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual’s email address; (d) a telephone number; (e) a social security number; (f) credit and/or debit card information, including credit and/or debit card number and expiration date; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with (a) through (g) above.

2. Unless otherwise specified, “Respondents” shall mean Guess?, Inc. and its successors and assigns, officers, agents, representatives, and employees, Guess.com, inc. and its successors and assigns, officers, agents, representatives, and employees, and both of them and their successors and assigns, officers, agents, representatives, and employees.


I.

IT IS ORDERED that Respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the online advertising, marketing, promotion, offering for sale, or sale of
any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which Respondents maintain and protect the security, confidentiality, or integrity of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that Respondents, directly or through any corporation, subsidiary, division, or other device, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall establish and maintain a comprehensive information security program in writing that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program shall contain administrative, technical, and physical safeguards appropriate to Respondents’ size and complexity, the nature and scope of Respondents’ activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the evaluation and adjustment of Respondents’ information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to Respondents’ operations or business arrangements, or any other circumstances that Respondents know or have reason to know may have a material impact on the effectiveness of their information security program.
III.

IT IS FURTHER ORDERED that Respondents obtain an assessment and report from a qualified, objective, independent third-party professional, using procedures and standards generally accepted in the profession, within one (1) year after service of the order, and biannually thereafter, that:

A. sets forth the specific administrative, technical, and physical safeguards that Respondents have implemented and maintained during the reporting period;

B. explains how such safeguards are appropriate to Respondents’ size and complexity, the nature and scope of Respondents’ activities, and the sensitivity of the personal information collected from or about consumers;

C. explains how the safeguards that have been implemented meet or exceed the protections required by Paragraph II of this order; and

D. certifies that Respondents’ security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biannual reports, has so operated throughout the reporting period.

Each assessment and report required by this Paragraph shall be prepared by a person qualified as a Certified Information System Security Professional (CISSP) or holding Global Information Assurance Certification from the SysAdmin, Audit, Network, Security Institute; or by a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission. Respondents shall provide the first assessment and report to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after it is prepared. All subsequent biannual reports shall be retained in accordance with Paragraph IV. B. of this order and provided to the Associate Director of Enforcement upon request.

IV.

IT IS FURTHER ORDERED that Respondents shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years:

1. a sample copy of each different print, broadcast, cable, or Internet advertisement, promotion, information collection form, Web page, screen, email message, or
other document containing any representation regarding Respondents’ online collection, use, and security of personal information from or about consumers. Each Web page copy shall be dated and contain the full URL of the Web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting the information on the Web. Provided, however, that after creation of any Web page or screen in compliance with this order, Respondents shall not be required to retain a print or electronic copy of any amended Web page or screen to the extent that the amendment does not affect Respondents’ compliance obligations under this order, and

2. any documents, whether prepared by or on behalf of Respondents, that contradict, qualify, or call into question Respondents’ compliance with this order; and

B. for a period of three (3) years after the date of preparation of each previous assessment and report required under Paragraph III of this order, and for the initial assessment and report, from the date the order is entered until two years following preparation of the assessment and report: all reports, studies, reviews, audits, audit trails, security assessments, risk assessments, policies, training materials, logs (from devices that detect or prevent attacks such as firewalls and intrusion detection systems), and plans (including the assessments and reports required under Paragraph III), whether prepared by or on behalf of Respondents, relating to Respondents’ compliance with Paragraphs II and III of this order.

V.

IT IS FURTHER ORDERED that Respondents shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that Respondents shall notify the Commission at least thirty (30) days prior to any change in either corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in either corporation about which either Respondent learns less than thirty (30) days prior to the
date such action is to take place, Respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that Respondents shall, within one hundred and twenty (120) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which they have complied with this order.

VIII.

This order will terminate on July 30, 2023, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order’s application to any Respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondents did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: July 30, 2003
UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

In the Matter of
GUIDANCE SOFTWARE, INC., a corporation.

DOCKET NO. C-4187

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq.:

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission

Page 1 of 6
hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:

1. Proposed respondent Guidance Software, Inc. is a California corporation with its principal office or place of business at 215 N. Marengo Avenue, Pasadena, California, 91101.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about a consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals a consumer’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and numerical security code; (g) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies a consumer; or (h) any other information from or about a consumer that is combined with (a) through (g) above.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the privacy, confidentiality, security, or integrity of any personal information collected from or about consumers.

II.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division,
or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from respondent, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information.

E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, using procedures and standards generally
accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment, as well as all: plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relied upon to prepare such Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this
order; and

B. for a period of three (3) years after the date of preparation of each biennial Assessment required under Paragraph III of this order: all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, whether prepared by or on behalf of respondent, relating to respondent’s compliance with Paragraphs II and III of this order for the compliance period covered by such biennial Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

IT IS FURTHER ORDERED that respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission an initial report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VIII.

This order will terminate on March 30th, 2027, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes
later; *provided, however*, that the filing of such a complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Paragraph.

*Provided, further*, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Paragraph as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark  
Secretary

SEAL:  
ISSUED: March 30th, 2007
The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to section 2.34 of its Rules, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent HTC America, Inc. (“HTC”) is a Washington corporation with its principal office or place of business at 13920 SE Eastgate Way, Suite #400, Bellevue, WA 98005.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean HTC America, Inc., and its successors and assigns.


3. “Covered device” shall mean any desktop computer, laptop computer, tablet, handheld or mobile device, telephone, or other electronic product or device developed by respondent or any corporation, subsidiary, division, or affiliate owned or controlled by respondent that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

4. “Covered information” shall mean individually-identifiable information from or about an individual consumer collected by respondent through a covered device or input into, stored on, captured with, or transmitted through a covered device, including but not limited to (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (j) precise geo-location data of an individual or mobile device, including GPS-based, WiFi-based, or cell-based location information; (k) an authentication credential, such as a username and password; or (l) any other communications or content that is input into, stored on, captured with, accessed or transmitted through a covered device, including but not limited to contacts, emails, text messages, photos, videos, and audio recordings.

5. “Covered device functionality” shall mean any capability of a covered device to capture, access, or transmit covered information.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device or affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in
any manner, expressly or by implication, the extent to which respondent or its products or services, including any covered devices, use, maintain and protect the security of covered device functionality or the security, privacy, confidentiality, or integrity of any covered information from or about consumers.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks related to the development and management of new and existing covered devices, and (2) protect the security, confidentiality, and integrity of covered information, whether collected by respondent or input into, stored on, captured with, accessed or transmitted through a covered device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered device functionality or covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the security program;

B. the identification of material internal and external risks to the security of covered devices that could result in unauthorized access to or use of covered device functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. the identification of material internal and external risks to the security, confidentiality, and integrity of covered information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, accessed or transmitted through a covered device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. at a minimum, the risk assessments required by subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development and research; (3) secure software design and testing, including secure engineering and defensive programming; and (4) review, assessment, and response to third-party security vulnerability reports;

E. the design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including through reasonable and appropriate software security testing techniques, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;
F. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards; and

G. the evaluation and adjustment of the security program in light of the results of the testing and monitoring required by subpart E, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

Provided, however, that this Part does not obligate respondent to identify and correct security vulnerabilities in third parties’ software on covered devices to the extent the vulnerabilities are not the result of respondent’s integration, modification, or customization of the third party software.

III.

IT IS FURTHER ORDERED that respondent shall develop security patches to fix the security vulnerabilities described in Attachment A for each affected covered device having an operating system version released on or after December 2010. Within thirty (30) days of service of this order, respondent shall release the applicable security patch(es) either directly to affected covered devices or to the applicable network operator for deployment of the security patch(es) to the affected covered devices. Respondent shall provide users of the affected covered devices with clear and prominent notice regarding the availability of the applicable security patch(es) and instructions for installing the applicable security patch(es).

IV.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience in secure mobile programming; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and secure mobile programming; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;
B. explain how such safeguards are appropriate to respondent’s size and complexity, the
nature and scope of respondent’s activities, and the sensitivity of the covered device
functionality or covered information;

C. explain how the safeguards that have been implemented meet or exceed the
protections required by Part II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to
provide reasonable assurance that the security of covered device functionality and the
security, confidentiality, and integrity of covered information is protected and has so
operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the
reporting period to which the Assessment applies. Respondent shall provide the initial
Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal
Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been
prepared. All subsequent biennial Assessments shall be retained by respondent until the order is
terminated and provided to the Associate Director of Enforcement within ten (10) days of
request. Unless otherwise directed by a representative of the Commission, the initial
Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not
the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer
Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C.
20580, with the subject line In the matter of HTC America, Inc., FTC File No. 1223049.
Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but
only if an electronic version of any such notice is contemporaneously sent to the Commission at
Debrief@ftc.gov.

V.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make
available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years after the date of preparation of each Assessment
required under Part IV of this order, all materials relied upon to prepare the
Assessment, whether prepared by or on behalf of the respondent, including but not
limited to all plans, reports, studies, reviews, audits, audit trails, policies, training
materials, and assessments, and any other materials relating to respondent’s
compliance with Parts II and III of this order, for the compliance period covered by
such Assessment;

B. unless covered by V.A, for a period of three (3) years from the date of preparation or
dissemination, whichever is later, all other documents relating to compliance with this
order, including but not limited to:
1. all advertisements and promotional materials containing any representations covered by this order, as well as all materials used or relied upon in making or disseminating the representation; and

2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of HTC America, Inc., FTC File No. 1223049. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.
IV.

This order will terminate on June 25, 2033, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission, Commissioner Ohlhausen recused.

Donald S. Clark
Secretary

SEAL
ISSUED: June 25, 2013
ATTACHMENT A

PERMISSION RE-DELEGATION

1. Permission re-delegation occurs when one application that has permission to access covered information or covered device functionality provides another application that has not been given the same level of permission with access to that information or functionality. Because HTC failed in numerous instances to include “permission check” code in its custom, pre-installed applications on its Android-based devices, any third-party application exploiting these vulnerabilities could command those HTC applications to access various covered information and covered device functionality on its behalf -- including enabling the device’s microphone; accessing the user’s GPS-based, cell-based, and WiFi-based location information; and sending text messages -- all without requesting the user’s permission.

APPLICATION INSTALLATION VULNERABILITY

2. HTC pre-installed a custom application on its Android-based devices that could download and install applications outside of the normal Android installation process. HTC failed to include appropriate permission check code to protect this pre-installed application from exploitation. As a result, any third-party application exploiting the vulnerability could command this pre-installed application to download and install any additional applications from any server onto the device without the user’s knowledge or consent.

INSECURE COMMUNICATIONS MECHANISMS

3. HTC failed to use readily-available and documented secure communications mechanisms in implementing logging applications on its devices, placing covered information at risk. Communications with logging applications should be secure to ensure that only designated applications can access the information. HTC implemented insecure communication mechanisms, as described below.

   a. HTC Loggers. HTC installed its customer support and trouble-shooting tool HTC Loggers on Android-based mobile devices. Because HTC Loggers could collect sensitive information from various device logs, it was supposed to have been accessible only to HTC and network operators. Because HTC used an insecure communications mechanism, however, any third-party application on the user’s device that could connect to the internet could exploit this vulnerability to communicate with HTC Loggers without authorization and command it to collect and transmit covered information from the device logs.
b. Carrier IQ. HTC embedded Carrier IQ diagnostics software on Android-based mobile devices and Windows Mobile-based mobile devices at the direction of network operators who used Carrier IQ to collect a variety of covered information from user devices to analyze network and device problems. In order to embed the Carrier IQ software on its mobile devices, HTC developed a “CIQ Interface” that would pass the necessary information to the Carrier IQ software. Because HTC used an insecure communications mechanism, any third-party application on the user’s device that could connect to the internet could exploit this vulnerability to communicate with the CIQ Interface, allowing it to:

i. Intercept the covered information being collected by the Carrier IQ software; and

ii. In the case of HTC’s Android-based devices, perform potentially malicious actions, including, but not limited to, sending text messages without permission.

DEBUG CODE

4. During the development of its CIQ Interface for its Android-based devices, HTC activated “debug code” in order to help test whether the CIQ Interface was functioning as intended, but then failed to deactivate the code before its devices shipped for sale to consumers. As a result of the active debug code, covered information was written to the Android system log, and was accessible to any third-party application with permission to read the system log, and in many instances, was also sent to HTC.
Federal Trade Commission, 

Plaintiff,

v.

LifeLock, Inc.
a corporation; Robert J. Maynard, Jr., individually and as an officer of LifeLock,

Defendants.

Civil No.

STIPULATED FINAL JUDGMENT AND ORDER FOR PERMANENT INJUNCTION AND OTHER EQUITABLE RELIEF AS TO DEFENDANTS LIFELOCK AND DAVIS

Plaintiff, the Federal Trade Commission ("FTC" or "Commission"), has concurrently filed its Complaint, which alleges that Defendants LifeLock, Inc. ("LifeLock"), Robert J. Maynard, Jr. ("Maynard"), and Richard Todd Davis ("Davis") have engaged in violations of Section 5 of the FTC Act, 15 U.S.C. § 45. The Commission and Defendants LifeLock and Davis ("Settling Defendants") have agreed to the entry of this Stipulated Final Judgment and Order for Permanent Injunction and Other Equitable Relief ("Order") to resolve all matters in dispute in this action without trial or adjudication of any issue of law or fact herein and without Settling Defendants admitting the truth of, or liability for, any of the matters alleged in the Complaint. Settling Defendants have waived service of the Summons and Complaint.
THEREFORE, IT IS HEREBY ORDERED, ADJUDGED, AND DECREED as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter of this case and over Settling Defendants LifeLock and Davis.

2. Venue in this district is proper under 28 U.S.C. § 1391(b) and (c), and 15 U.S.C. § 53(b).

3. The acts and practices of Settling Defendants are in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

4. The Complaint states claims upon which relief may be granted against Settling Defendants under Sections 5 and 13(b) of the FTC Act, 15 U.S.C. §§ 45 and 53(b).

5. Settling Defendants make no admission to the allegations in the Complaint, other than the jurisdictional facts.

6. Settling Defendants waive: (a) all rights to seek appellate review or otherwise challenge or contest the validity of this Order; (b) any claim they may have against the Commission, its employees, representatives, or agents that relate to the matter stated herein; (c) all claims under the Equal Justice Act, 28 U.S.C. § 2412, as amended by Pub. L. 104-121, 110 Stat. 847, 863-64 (1996); and (d) any rights to attorneys’ fees that may arise under said provision of law.

7. Settling Defendants have entered into this Order freely and without coercion, and they acknowledge that they have read the provisions of this Order and are prepared to abide by them.

8. Entry of this Order is in the public interest.
9. LifeLock is concurrently agreeing to orders resolving related complaints brought by the Attorneys General of the States of Alaska, Arizona, California, Delaware, Florida, Hawaii, Idaho, Illinois, Indiana, Iowa, Kentucky, Maine, Maryland, Massachusetts, Michigan, Missouri, Mississippi, Montana, Nebraska, Nevada, New Mexico, New York, North Carolina, North Dakota, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Vermont, Virginia, Washington, and West Virginia (the “Participating States”). These state orders will require LifeLock to pay $1 million to the Office of the Attorney General of Illinois for distribution among the Participating States.

DEFINITIONS

1. “Individual Defendant” shall mean Davis.

2. “Corporate Defendant” shall mean LifeLock, Inc. and its successors and assigns.

3. “Settling Defendants” shall mean Individual Defendant and Corporate Defendant, individually, collectively, or in any combination.

4. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and/or data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and/or check number; (h) a driver’s license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an
individual consumer; or (j) any information that is combined with any of (a) through (i) above.

5. “Subscribing Consumer” shall mean any person or entity that paid for Corporate Defendant’s service at any time between April 1, 2005 and March 31, 2009.

ORDER

I. PROHIBITED BUSINESS ACTIVITIES

IT IS ORDERED that Settling Defendants and their officers, agents, servants, and employees and all persons in active concert or participation with any of them, who receive actual notice of this Order by personal service or otherwise, whether acting directly or through any sole proprietorship, partnership, limited liability company, corporation, subsidiary, branch, division, or other entity, are hereby permanently restrained and enjoined from:

A. in connection with the advertising, distributing, promoting, offering for sale, or sale of any product, service, or program designed for the purpose of preventing, mitigating, or recovering from any form of identity theft as defined in 18 U.S.C. § 1028, misrepresenting in any manner, expressly or by implication:

1. that such product, service, or program provides complete protection against all forms of identity theft by making customers’ personal information useless to identity thieves;

2. that such product, service, or program prevents unauthorized changes to customers’ address information;

3. that such product, service, or program constantly monitors activity on each of its customers’ consumer reports;

4. that such product, service, or program ensures that a customer will always receive a phone call from a potential creditor before a new credit account
is opened in the customer’s name;

5. the means, methods, procedures, effects, effectiveness, coverage, or scope of such product, service, or program;

6. the risk of identity theft to consumers;

7. whether a particular consumer has become or is likely to become a victim of identity theft; and/or

8. the opinions, beliefs, findings, or experiences of an individual or group of consumers related in any way to any such product, service, or program.

Such products, services, or programs include, but are not limited to, the placement of fraud alerts on behalf of consumers, searching the internet for consumers’ personal data, monitoring commercial transactions for consumers’ personal data, identity theft protection for minors, and guarantees of any such products, services, or programs.

B. misrepresenting in any manner, expressly or by implication, the manner or extent to which they maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

II. INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that Corporate Defendant and any business entity that Individual Defendant controls, directly or indirectly, which collects, maintains, or stores personal information from or about consumers, shall, upon operation of this business, establish and implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards.

Page 5 of 22
appropriate to the entity’s size and complexity, the nature and scope of the entity’s activities, and
the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for
the information security program;

B. the identification of material internal and external risks to the security,
confidentiality, and integrity of personal information that could result in the unauthorized
disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and
assessment of the sufficiency of any safeguards in place to control these risks. At a minimum,
this risk assessment should include consideration of risks in each area of relevant operation,
including, but not limited to, (1) employee training and management, (2) information systems,
including network and software design, information processing, storage, transmission, and
disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems
failure;

C. the design and implementation of reasonable safeguards to control the risks
identified through risk assessment, and regular testing or monitoring of the effectiveness of the
safeguards’ key controls, system, and procedures;

D. the development and use of reasonable steps to retain service providers capable of
appropriately safeguarding personal information received from Settling Defendants and
requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of Settling Defendants’ information security
program in light of the results of the testing and monitoring required by Subsection C of this
Section, any material changes to Settling Defendants’ operations or business arrangements, or
any other circumstances that Settling Defendants know or have reason to know may have a
material impact on the effectiveness of their information security program.

III. BIENNIAL ASSESSMENT REQUIREMENTS

A. IT IS FURTHER ORDERED that Corporate Defendant and any business entity that Individual Defendant controls, directly or indirectly, which collects, maintains, or stores personal information from our about consumers, shall, in connection with their compliance with Section II of this Order, obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred eighty days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

1. set forth the specific administrative, technical, and physical safeguards implemented and maintained during the reporting period;

2. explain how such safeguards are appropriate to Settling Defendants’ size and complexity, the nature and scope of Settling Defendants’ activities, and the sensitivity of the personal information collected from or about consumers;

3. explain how the safeguards that have been implemented meet or exceed the protections required by Section II of this Order; and

4. certify that Settling Defendants’ security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

B. Each Assessment shall be prepared and completed within sixty (60) days after the
end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

C. Settling Defendants shall provide the initial Assessment within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Settling Defendants until the Order is terminated and provided to the Commission within ten (10) days of request.

IV. CONSUMER REDRESS

IT IS FURTHER ORDERED that:

A. Judgment in the amount of $35,000,000.00 is hereby entered jointly and severally against Settling Defendants. Full payment for the foregoing judgment is suspended, subject to the following conditions:

1. Corporate Defendant shall pay eleven million dollars ($11,000,000), which Corporate Defendant represents their undersigned counsel holds in escrow for no purpose other than payment to the Commission. Such payment shall be made within seven days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of the Commission.

2. Individual Defendant shall pay ten thousand dollars ($10,000), which Individual Defendant represents their undersigned counsel holds in escrow.
for no purpose other than payment to the Commission. Such payment shall be made within seven days of entry of this Order by electronic fund transfer in accordance with instructions previously provided by a representative of the Commission.

B. In the event of any default in payment, which default continues for ten (10) days beyond the due date of payment, the entire unpaid amount, together with interest, as computed pursuant to 28 U.S.C. § 1961 from the date of default to the date of payment, shall immediately become due and payable.

C. All funds paid to the FTC pursuant to the Order shall be deposited into an account administered by the Commission or its agent to be used for equitable relief which will include, but not be limited to, consumer redress, and any attendant expenses for the administration of such equitable relief. Acceptance of redress from the FTC shall constitute an acknowledgment by the consumer that, to the extent that the consumer makes a subsequent claim, the defendant is entitled to deduct the amount of the redress received from the FTC from any other or additional redress ordered. Upon completion of consumer redress, Commission shall supply to Defendants the names of consumers that received redress and the amount received. In the event that funds remain after redress is attempted, the Commission may apply any remaining funds for such other equitable relief (including consumer information remedies) as it determines to be reasonably related to Settling Defendants’ practices alleged in the Complaint. Any funds not used for such equitable relief shall be deposited to the United States Treasury as disgorgement. Settling Defendants shall have no right to challenge the Commission’s choice of remedies under this Section. Settling Defendants shall have no right to contest the manner of distribution chosen by the Commission.
D. Settling Defendants relinquish all dominion, control, and title to the funds paid to the fullest extent permitted by law. Settling Defendants shall make no claim to or demand return of the funds, directly or indirectly, through counsel or otherwise.

E. Settling Defendants agree that the facts as alleged in the Complaint filed in this action shall be taken as true without further proof in any bankruptcy case or subsequent civil litigation pursued by the Commission to enforce its rights to any payment or money judgment pursuant to this Order, including but not limited to a nondischargeability complaint in any bankruptcy case. Settling Defendants further stipulate and agree that the facts alleged in the Complaint establish all elements necessary to sustain an action pursuant to, and that this Order shall have collateral estoppel effect for purposes of, Section 523(a)(2)(A) of the Bankruptcy Code, 11 U.S.C. § 523(a)(2)(A).

F. Settling Defendants shall, within ten (10) days of the date of entry of this Order, provide to the Commission, an encrypted file containing, in Access database format, for each Subscribing Consumer: (1) the consumer’s name; (2) most recent known mailing address, e-mail address, and telephone number; (3) the beginning and end date for the consumer’s subscription to the service; and (4) the monthly rate paid by the consumer. The database shall be formatted with a separate field for each piece of information requested, and, for the mailing address, separate fields for street number, building/apartment number, city, state, and zip code. Settling Defendants shall cooperate in good faith with the Commission or its representative to obtain and provide any additional information required to administer consumer redress and take all reasonable steps to ensure that all data provided is accurate, up-to-date, and in a secure and useable format. In the event the Defendants fail to provide data that is accurate, up-to-date, and in a secure and useable format, the Commission may apply any remaining funds for such other
equitable relief (including consumer information remedies) as it determines to be reasonably related to Settling Defendants’ practices alleged in the Complaint. Any funds not used for such equitable relief shall be deposited to the United States Treasury as disgorgement.

**V. RIGHT TO REOPEN AS TO MONETARY JUDGMENT**

**IT IS FURTHER ORDERED** that the Commission’s agreement to this Order is expressly premised upon the truthfulness, accuracy and completeness of Settling Defendants’ sworn financial statements and supporting documents submitted to the Commission, which include material information upon which the Commission relied in negotiating and agreeing to this Order. If, upon motion by the Commission, this Court finds that any Settling Defendant has failed to disclose any material asset, or materially misstated the value of any asset in the financial statements and information submitted to the Commission, or has made any other material misstatement or omission in the financial statements and related documents described above, then this Order shall be reopened and suspension of the judgment against that particular Settling Defendant shall be lifted for the purpose of requiring payment in the full amount of the judgment ($35,000,000). Provided, however, that in all other respects this Order shall remain in full force and effect, unless otherwise ordered by the Court.

**VI. COMPLIANCE MONITORING**

**IT IS FURTHER ORDERED** that, for the purpose of (i) monitoring and investigating compliance with any provision of this Order, and (ii) investigating the accuracy of any Settling Defendant’s financial statements upon which the Commission’s agreement to this Order is expressly premised:

A. Within ten (10) days of receipt of written notice from a representative of the Commission, Settling Defendants each shall submit additional written reports, which are true
and accurate and sworn to under penalty of perjury; produce documents for inspection and
copying; appear for deposition; and provide entry during normal business hours to any business
location in each Settling Defendant’s possession or direct or indirect control to inspect the
business operation;

B. In addition, the Commission is authorized to use all other lawful means, including
but not limited to:

1. obtaining discovery from any person, without further leave of court, using
the procedures prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, 45 and 69;

2. posing as consumers and suppliers to Settling Defendants, their
employees, or any other entity managed or controlled in whole or in part by any Settling
Defendant, without the necessity of identification of prior notice; and

C. Settling Defendants each shall permit representatives of the Commission to
interview any employer, consultant, independent contractor, representative, agent, or employee
who has agreed to such an interview, relating in any way to any conduct subject to this Order.
The person interviewed may have counsel present.

Provided however, that nothing in this Order shall limit the Commission’s lawful use of
compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. § 49, 57b-1, to
obtain any documentary material, tangible things, testimony, or information relevant to unfair or
deceptive acts or practices in or affecting commerce (within the meaning of 15 U.S.C.
§ 45(a)(1)).

VII. COMPLIANCE REPORTING

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this
Order may be monitored:

Page 12 of 22
A. For a period of five (5) years from the date of entry of this Order for Corporate Defendant and a period of three (3) years from the date of entry of this Order for Individual Defendant,

1. Individual Defendant shall notify the Commission of the following:
   a. Any changes in Individual Defendant’s residence, mailing addresses, and telephone numbers, within ten (10) days of the date of the change;
   b. Any changes in Individual Defendant’s employment status (including self-employment), and any change in Individual Defendant’s ownership in any business entity, within ten (10) days of the date of such change. Such notice shall include the name and address of each business that Individual Defendant is affiliated with, employed by, creates or forms, or performs services for; a detailed description of the nature of the business; and a detailed description of Individual Defendant’s duties and responsibilities in connection with the business or employment; and
   c. Any changes in Individual Defendant’s name or use of any aliases or fictitious names.

2. Settling Defendants shall notify the Commission of any changes in structure of Corporate Defendant or any business entity that any Defendant directly or indirectly controls, or has ownership interest in, that may affect compliance obligations under this Order, including but not limited to: incorporation or other organization; a dissolution, assignment, sale, merger, or other action; the creation or dissolution of a subsidiary, parent, or affiliate that
engages in any acts or practices subject to this Order; or a change in the business name or address, at least thirty (30) days prior to such change, provided that, with respect to any proposed change in the business entity which a Defendant learns less than thirty (30) days prior to the date such action is to take place, such Defendant shall notify the Commission as soon as practicable after obtaining such knowledge.

B. One hundred eighty (180) days after the date of entry of this Order and annually thereafter for a period of five (5) years for Corporate Defendant and three (3) years for Individual Defendant, Settling Defendants each shall provide a written report to the FTC, which is true and accurate and sworn to under penalty of perjury, setting forth in detail the manner and form in which they have complied and are complying with this Order. This report shall include, but not be limited to:

1. For Individual Defendant:
   a. Individual Defendant’s then-current residence address, mailing address, and telephone numbers;
   b. Individual Defendant’s then-current employment status (including self-employment), including the name, addresses, and telephone numbers of each business that Individual Defendant is affiliated with, employed by, or performs services for; a detailed description of the nature of the business; and a detailed description of Individual Defendant’s duties and responsibilities in connection with the business or employment; and
   c. Any other changes required to be reported under Subsection A of this Section.
2. For all Settling Defendants:
   a. A copy of each acknowledgment of receipt of this Order, obtained pursuant to the Section titled “Distribution of Order;”
   b. Any other changes required to be reported under Subsection A of this Section.

C. Each Defendant shall notify the Commission of the filing of a bankruptcy petition by such Defendant within fifteen (15) days of filing.

D. For the purposes of this Order, Settling Defendants shall, unless otherwise directed by the Commission’s authorized representatives, send by overnight courier all reports and notifications required by this Order to the Commission, to the following address:

   Associate Director for Enforcement
   Federal Trade Commission
   600 Pennsylvania Avenue, N.W., Room NJ-2122
   Washington, D.C. 20580
   RE: FTC v. LifeLock, Inc.

Provided that, in lieu of overnight courier, Settling Defendants may send such reports or notifications by first-class mail, but only if Settling Defendants contemporaneously send an electronic version of such report or notification to the Commission at: DEBrief@ftc.gov.

E. For purposes of the compliance reporting and monitoring required by this Order, the Commission is authorized to communicate directly with each Defendant.

VIII. RECORD KEEPING PROVISIONS

IT IS FURTHER ORDERED that Settling Defendants and their agents, employees, officers, corporations, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, in connection with, are hereby restrained and enjoined from failing to create and retain the following records for the following
periods:

A. For a period of eight (8) years from the date of entry of this Order for Corporate Defendant and six (6) years from the date of entry of this Order for Individual Defendant, the following records in connection with the sale or provision of products or services related to identity theft:

1. Accounting records that reflect the cost of goods or services sold, revenues generated, and the disbursement of such revenues;

2. Personnel records accurately reflecting: the name, address, and telephone number of each person employed in any capacity by such business, including as an independent contractor; that person's job title or position; the date upon which the person commenced work; and the date and reason for the person's termination, if applicable;

3. Customer files containing the names, addresses, phone numbers, dollar amounts paid, quantity of items or services purchased, and description of items or services purchased, to the extent such information is obtained in the ordinary course of business;

4. Complaints and refund requests (whether received directly, indirectly, or through any third party) and any responses to those complaints or requests;

5. Copies of all sales scripts, training materials, advertisements, or other marketing materials;

6. Any documents, whether prepared by or on behalf of Settling Defendants, that contradict, qualify, or call into question Settling Defendants’
compliance with Sections I, II, and III of this Order; and

7. All records and documents necessary to demonstrate full compliance with each provision of this Order, including but not limited to, copies of acknowledgments of receipt of this Order required by the Sections titled “Distribution of Order” and “Acknowledgment of Receipt of Order” and all reports submitted to the FTC pursuant to the Section titled “Compliance Reporting;”

B. For a period of three (3) years after the date of preparation of each Assessment required under the Section titled “Biennial Assessment Requirements”: All materials relied upon to prepare the Assessment, whether prepared by or on behalf of any Settling Defendant, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Settling Defendants’ compliance with the Section titled “Biennial Assessment Requirements.”

IX. DISTRIBUTION OF ORDER

IT IS FURTHER ORDERED that for a period of five (5) years from the date of entry of this Order for Corporate Defendant and three (3) years from the date of entry of this Order for Individual Defendant, Settling Defendants shall deliver copies of the Order as directed below:

A. Corporate Defendant: Corporate Defendant must deliver a copy of this Order to (1) all of its principals, officers, directors, and managers; (2) all of its employees, agents, and representatives who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled “Compliance Reporting.” For current personnel, delivery shall be within five (5) days of service of this Order upon such Defendant. For new personnel, delivery shall occur prior to
them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled “Compliance Reporting,” delivery shall be at least ten (10) days prior to the change in structure.

B. Individual Defendant as Control Person: For any business that Individual Defendant controls, directly or indirectly, or in which Individual Defendant has a majority ownership interest, Individual Defendant must deliver a copy of this Order to (1) all principals, officers, directors, and managers of that business; (2) all employees, agents, and representatives of that business who engage in conduct related to the subject matter of the Order; and (3) any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled “Compliance Reporting.” For current personnel, delivery shall be within five (5) days of service of this Order upon such Defendant. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Subsection A.2 of the Section titled “Compliance Reporting,” delivery shall be at least ten (10) days prior to the change in structure.

C. Individual Defendant as employee or non-control person: For any business where Individual Defendant is not a controlling person of a business but otherwise engages in conduct related to the subject matter of this Order, such Individual Defendant must deliver a copy of this Order to all principals and managers of such business before engaging in such conduct.

D. Settling Defendants must secure a signed and dated statement acknowledging receipt of the Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this Section.

X. ACKNOWLEDGMENT OF RECEIPT OF THIS ORDER

IT IS FURTHER ORDERED that each Defendant, within five (5) business days of
receipt of this Order as entered by the Court, must submit to the Commission a truthful sworn statement acknowledging receipt of this Order.

XI. COOPERATION WITH COMMISSION COUNSEL

IT IS FURTHER ORDERED that the Settling Defendants shall, in connection with this action or any subsequent investigation related to or associated with the transaction or the occurrences that are the subject of the Complaint, cooperate in good faith with the Commission and appear at such places and times as the Commission shall reasonably request, after written notice, for interviews, conferences, pretrial discovery, review of documents, and for such other matters as may be reasonably requested by the Commission. If requested in writing by the Commission, the Settling Defendants shall appear or cause their officers, employees, representatives or agents to appear, and provide truthful testimony in any trial, deposition, or other proceeding related to or associated with the transactions or the occurrences that are the subject of the Complaint, without the service of a subpoena.

XII. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

XIII. COSTS AND ATTORNEYS’ FEES

IT IS FURTHER ORDERED that each party shall bear its own costs and attorneys’ fees incurred in connection with this action.
XIV. NOTICE OF ENTRY OF ORDER

IT IS FURTHER ORDERED that entry in the docket of this Order by the Clerk of Court shall constitute notice to Settling Defendants of the terms and conditions of this Order, and that Settling Defendants waive all rights to contest in any future proceeding whether Settling Defendants were properly served with this Order.

The parties hereby stipulate to the entry of the foregoing Order, which shall constitute a final Order in this action.

IT IS SO ORDERED:
STIPULATED AND AGREED TO BY:

FOR DEFENDANT LIFELOCK:

Richard Todd Davis  
Chief Executive Officer  
LifeLock, Inc.

Andrew Berg  
Greenberg Traurig, LLP  
Counsel for LifeLock, Inc.
2101 L Street, N.W.  
Suite 1000  
Washington, D.C. 20037  
(202) 331-3181  
berga@gtlaw.com

FOR DEFENDANT RICHARD TODD DAVIS:

Richard Todd Davis  

Andrew Berg  
Greenberg Traurig, LLP  
Counsel for Richard Todd Davis  
2101 L Street, N.W.  
Suite 1000  
Washington, D.C. 20037  
(202) 331-3181  
berga@gtlaw.com
FOR PLAINTIFF FEDERAL TRADE COMMISSION

Willard K. Tom
General Counsel

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection

David Lincicum
Burke Kappler
Federal Trade Commission
600 Pennsylvania Avenue, NW
Mail Stop NJ-8122
Washington, DC 20580
(202) 326-3224 (general)
(202) 326-2773 (Lincicum)
(202) 326-3768 (facsimile)
dlincicum@ftc.gov
UNITED STATES OF AMERICA  
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman  
William E. Kovacic  
J. Thomas Rosch  
Edith Ramirez  
Julie Brill

In the Matter of )  
LOOKOUT SERVICES, INC., ) DOCKET NO. C-4326  
a corporation. )  
DECISION AND ORDER)

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:
1. Respondent is a Texas corporation with its principal office or place of business at 5909 West Loop South, Suite 300, Bellaire, Texas 77401.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Lookout Services, Inc., its subsidiaries, divisions, affiliates, successors and assigns.

2. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) a bank account, debit card, or credit card account number; (h) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; (i) a biometric record; or (j) any information that is combined with any of (a) through (i) above. For the purpose of this provision, a “consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.
II.

**IT IS FURTHER ORDERED** that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of the information security program.
III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been completed. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Lookout Services, Inc., FTC File No.1023076. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

-4-
IV.

**IT IS FURTHER ORDERED** that respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent, including but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment;

B. unless covered by IV.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, a print or electronic copy of each document relating to compliance with this order, including but not limited to:

1. all advertisements and promotional materials containing any representations covered by this order, with all materials used or relied upon in making or disseminating the representation; and

2. any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question compliance with this order.

V.

**IT IS FURTHER ORDERED** that respondent shall deliver copies of the order as directed below:

A. Respondent must deliver a copy of this order to (1) all current and future principals, officers, directors, and managers, (2) all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order, and (3) any business entity resulting from any change in structure set forth in Part VI. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure.

B. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.
VI.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the matter of Lookout Services, Inc., FTC File No.1023076. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

VII.

IT IS FURTHER ORDERED that respondent, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on June 15, 2031, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.
Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: June 15, 2011
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

Commissioners: William E. Kovacic, Chairman
             Pamela Jones Harbour
             Jon Leibowitz
             J. Thomas Rosch

In the Matter of

PREMIER CAPITAL LENDING, INC., a corporation,
and

DEBRA STILES, individually and as an officer of the corporation.

DOCKET NO. C-4241

DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the respondents named in the caption hereof, and the respondents having been furnished thereafter with a copy of a draft Complaint, which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the respondents with violation of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq., and the Federal Trade Commission Act, 15 U.S.C. § 45 et seq.; and

The respondents and counsel for the Commission, having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), including an admission by the respondents of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of the Agreement is for settlement purposes only and does not constitute an admission by the respondents that the law has been violated as alleged in such Complaint, or that any of the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondents have violated the said Acts, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30)
days for the receipt and consideration of public comment, now in further conformity with the
procedure prescribed in Section 2.34 of its Rules, the Commission hereby issues its Complaint,
makes the following jurisdictional findings, and enters the following Order:

1. Respondent Premier Capital Lending, Inc. (“PCL”) is a Texas Corporation with its
   principal place of business at 901 W. Bardin Road, Suite 200, Arlington, Texas 76017.

2. Respondent Debra Stiles (“Stiles”) is a co-owner of PCL, Secretary of the company, and
   Manager of its headquarters office in Arlington, Texas. Individually or in concert with
   others, she formulates, directs, or controls the policies, acts, or practices of respondent
   PCL. Her principal place of business is the same as PCL’s.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personally identifiable information” or “personal information” shall mean individually
   identifiable information from or about an individual consumer including, but not limited
   to: (a) a first and last name; (b) a home or other physical address, including street name
   and name of city or town; (c) an email address or other online contact information, such
   as an instant messaging user identifier or a screen name that reveals an individual’s email
   address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card
   information, including card number, expiration date, and security code; (g) a persistent
   identifier, such as a customer number held in a “cookie” or processor serial number, that
   is combined with other available data that identifies an individual consumer; or (h) any
   information that is combined with any of (a) through (g) above.

2. “Gramm-Leach-Bliley Act” or “GLB Act” refers to 15 U.S.C. §§ 6801-6809, as
   amended, the “Safeguards Rule” or the “Standards for Safeguarding Customer
   Information Rule” refers to 16 C.F.R. Part 314, issued pursuant to Title V, Subtitle A of
   the GLB Act, 15 U.S.C. §§ 6801-6809, and the “Privacy Rule” or the “Commission’s
   Privacy of Consumer Financial Information Rule” refers to 16 C.F.R. Part 313, issued
   pursuant to the GLB Act.

3. “Financial institution” shall mean as defined in Section 509(3)(A) of the GLB Act, 15

4. Unless otherwise specified, “respondents” shall mean Premier Capital Lending, Inc. and
   its subsidiaries, divisions, affiliates, successors and assigns (“PCL”), and Debra Stiles.

5. “Commerce” shall mean as defined in Section 4 of the Federal Trade Commission Act,
I.

IT IS ORDERED that respondents, and their officers, agents, representatives, and employees, shall not directly or through any corporation, subsidiary, division, website, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, misrepresent in any manner, expressly or by implication, the extent to which respondents maintain and protect the privacy, confidentiality, or security of any personal information collected from or about consumers.

II.

IT IS FURTHER ORDERED that respondents, and their officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, or other device, no later than the date of service of this order, shall establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumers’ personal information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent PCL’s size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to, (1) employee training and management, (2) information systems, including network and software design, information processing, storage, transmission, and disposal, and (3) prevention, detection, and response to attacks, intrusions, or other systems failure;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondents and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of respondents’ information security program in
light of the results of the testing and monitoring required by subpart C, any material changes to respondents’ operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

III.

IT IS FURTHER ORDERED that respondents, and their officers, agents, representatives, and employees, shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of:

A. the Safeguards Rule, 16 C.F.R. Part 314; or
B. the Privacy Rule, 16 C.F.R. Part 313.

In the event that either of these Rules is hereafter amended or modified, respondents’ compliance with that Rule as so amended or modified shall not be a violation of this order.

IV.

IT IS FURTHER ORDERED that, in connection with their compliance with Parts II and III.A. of this order, respondents, and their officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional using procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (A) the first one hundred and eighty (180) days after service of the order for the initial Assessment; and (B) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent PCL has implemented and maintained during the reporting period;
B. explain how such safeguards are appropriate to respondent PCL’s size and complexity, the nature and scope of respondent PCL’s activities, and the sensitivity of the personal information collected from or about consumers;
C. explain how the safeguards that have been implemented meet or exceed the protections required by the Safeguards Rule; and
D. certify that respondent PCL’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and, for biennial reports, has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the
reporting period to which the Assessment applies by: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission.

Respondents shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) business days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondents until three years after completion of the final Assessment and provided to the Associate Director of Enforcement upon request within ten (10) business days after respondents receives such request.

V.

IT IS FURTHER ORDERED that respondents shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including by not limited to:

A. for a period of five (5) years:

1. any documents, whether prepared by or on behalf of either respondent, that contradict, qualify, or call into question respondents’ compliance with this order;

2. consumer complaints (whether received in written or electronic form, directly, indirectly or through any third party), and any responses to those complaints, whether in written or electronic form, that relate to respondents’ activities as alleged in the draft Complaint and respondents’ compliance with the provisions of this order;

3. copies of all subpoenas and other communications with law enforcement entities or personnel, whether in written or electronic form, if such documents bear in any respect on respondents’ collection, maintenance, or furnishing of consumer reports or other personal information of consumers; and

4. all records and documents necessary to demonstrate full compliance with each provision of this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of either respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to
respondents’ compliance with Parts II and III.A. of this order, for the compliance period covered by such Assessment. Respondents shall provide such documents to the Associate Director of Enforcement within ten (10) days of request.

VI.

**IT IS FURTHER ORDERED** that respondents shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondents shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

**IT IS FURTHER ORDERED** that respondent Stiles, for a period of ten (10) years after the date of issuance of the order, shall notify the Commission of the discontinuance of her current business or employment or of her affiliation with any new business or employment that provides financial products or services. The notice shall include respondent Stiles’ new business address and telephone number and a description of the nature of the business or employment and her duties or responsibilities. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VIII.

**IT IS FURTHER ORDERED** that respondents shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondents learn fewer than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

IX.

**IT IS FURTHER ORDERED** that respondents shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which they have complied with this order.
This order will terminate on December 10, 2028, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent(s) did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent(s) will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL:
ISSUED: December 10, 2008
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Deborah Platt Majoras, Chairman
Pamela Jones Harbour
Jon Leibowitz
William E. Kovacic
J. Thomas Rosch

In the Matter of ) FILE NO. 0523094
) AGREEMENT CONTAINING
) CONSENT ORDER

The Federal Trade Commission has conducted an investigation of certain acts and practices of Reed Elsevier Inc. and Seisint, Inc. ("proposed respondents"). Proposed respondents, having been represented by counsel, are willing to enter into an agreement containing a consent order resolving the allegations contained in the attached draft complaint. Therefore,

IT IS HEREBY AGREED by and between Reed Elsevier Inc., by its duly authorized officers; Seisint, Inc., by its duly authorized officers; and counsel for the Federal Trade Commission that:

1. Proposed respondent Reed Elsevier Inc. is a Massachusetts corporation with its principal office or place of business at 125 Park Avenue, Suite 2300, New York, New York 10017.

2. Proposed respondent Seisint, Inc. is a Florida corporation with its principal office or place of business at 6601 Park of Commerce Boulevard, Boca Raton, Florida 33487.

3. Proposed respondents admit all the jurisdictional facts set forth in the draft complaint.

4. Proposed respondents waive:
   A. any further procedural steps;
   B. the requirement that the Commission’s decision contain a statement of
findings of fact and conclusions of law; and

C. all rights to seek judicial review or otherwise to challenge or contest the validity of the order entered pursuant to this agreement.

5. This agreement shall not become part of the public record of the proceeding unless and until it is accepted by the Commission. If this agreement is accepted by the Commission, it, together with the draft complaint, will be placed on the public record for a period of thirty (30) days and information about it publicly released. The Commission thereafter may either withdraw its acceptance of this agreement and so notify proposed respondents, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

6. This agreement is for settlement purposes only and does not constitute an admission by proposed respondents that the law has been violated as alleged in the draft complaint, or that the facts as alleged in the draft complaint, other than the jurisdictional facts, are true.

7. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission’s Rules, the Commission may, without further notice to proposed respondents, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to proposed respondents’ addresses as stated in this agreement by any means specified in Section 4.4(a) of the Commission’s Rules shall constitute service. Proposed respondents waive any right they may have to any other manner of service. The complaint may be used in construing the terms of the order. No agreement, understanding, representation, or interpretation not contained in the order or in the agreement may be used to vary or contradict the terms of the order.

8. Proposed respondents have read the draft complaint and consent order. They understand that they may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondents” shall mean Reed Elsevier Inc., its
successors and assigns, officers, agents, representatives, and employees, and Seisint, Inc., and its successors and assigns, officers, agents, representatives, and employees.

2. “Personal information” shall mean individually identifiable information from or about a consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals a consumer’s email address; (d) a telephone number; (e) a Social Security number; (f) a date of birth; (g) a driver’s license number; (h) credit and/or debit card information, including but not limited to card number and expiration date and transaction detail data; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies a consumer; or (j) any other information from or about a consumer that is combined with (a) through (i) above.

3. “Information product or service” shall mean each product, service, or other means by which respondents individually or collectively provide direct or indirect access to personal information from or about consumers that is comprised in whole or part of nonpublic information; provided, however, that this term shall not include information products or services that: (a) provide access solely to personal information that is publicly available information, or (b) permit customers to upload or otherwise supply, organize, manage, or retrieve information that is under the customer’s control.

4. “Publicly available information” shall mean information that respondents have a reasonable basis to believe is lawfully made available to the general public from: (a) Federal, State, or local government records, (b) widely distributed media, or (c) disclosures to the general public that are required to be made by Federal, State, or local law. Respondents shall have a reasonable basis to believe information is lawfully made available to the general public if respondents have taken reasonable steps to determine: (a) that the information is of the type that is available to the general public, and (b) whether an individual can direct that the information not be made available to the general public and, if so, that the individual has not done so.

5. “LexisNexis” shall mean Seisint, Inc., and its successors and assigns, officers, agents, representatives, and employees, and the LexisNexis division of respondent Reed Elsevier Inc., and its successors and assigns, officers, agents, representatives, and employees; provided, however, that, for the purposes of this order, LexisNexis shall:

   (a) be treated as a corporation under the control of respondent Reed Elsevier Inc. for the purpose of determining whether any other entity is a successor or assign of LexisNexis; and

   (b) include any other corporation, subsidiary, division, or other device under the control of respondent Reed Elsevier Inc. (collectively, “entity”) to the extent that such entity advertises, markets, promotes, offers for sale, or sells any information product or service that includes a Social Security number; driver’s license number; date of birth; or bank, credit card, or other financial account number (collectively, “designated information”), including, but not limited to, any information product or service that can be used to access, view, or retrieve designated
information from databases under the entity’s possession or control.


I.

IT IS ORDERED that each respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of personal information collected from or about consumers made available through any information product or service of LexisNexis (“the information”), in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of the information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to each respondent’s size and complexity, the nature and scope of each respondent’s activities, and the sensitivity of the information, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of the information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of the information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards; provided, however, that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve, and supply to respondent, additional personal information about the consumer.
E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph I of this order, each respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph I of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.
III.

IT IS FURTHER ORDERED that each respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question its compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Paragraph II of this order: all materials relied upon to prepare the Assessment, whether prepared by or behalf of respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments and any other materials relating to its compliance with Paragraphs I and II of this order, for the compliance period covered by such Assessment.

IV.

IT IS FURTHER ORDERED that each respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having managerial responsibilities relating to the subject matter of this order. Each respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that each respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that each respondent shall, within one hundred and eighty (180) days after service of this order, and at such other times as the Commission may require,
file with the Commission an initial report, in writing, setting forth in detail the manner and form
in which it has complied with this order.

VII.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20)
years from the most recent date that the United States or the Federal Trade Commission files a
complaint (with or without an accompanying consent decree) in federal court alleging any
violation of the order, whichever comes later; provided, however, that the filing of such a
complaint will not affect the duration of:

A. any Paragraph in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such
complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this
Paragraph.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did
not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld
on appeal, then the order will terminate according to this Paragraph as though the complaint had
never been filed, except that the order will not terminate between the date such complaint is filed
and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or
ruling is upheld on appeal.

REED ELSEVIER INC.

Dated: ____________

By: ______________________

HENRY Z. HORBACZEWSKI
Senior Vice President and General Counsel
Reed Elsevier Inc.

SEISINT, INC.

Dated: ____________

By: ______________________

JAMES M. PECK
President
Seisint, Inc.
Dated: ____________

By: ________________

EMILIO W. CIVIDANES
LISA JOSE FALES
Venable, LLP
Counsel for respondents Reed Elsevier Inc., and Seisint, Inc.

FEDERAL TRADE COMMISSION

Dated: ____________

By: ________________

ALAIN SHEER
KATRINA A. BLODGETT
KATHRYN D. RATTE’
Counsel for the Federal Trade Commission

APPROVED:

______________________________
JESSICA RICH
Assistant Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection

______________________________
JOEL WINSTON LYDIA B. PARNES
Associate Director  Director
Division of Privacy and Identity Protection  Bureau of Consumer Protection
Bureau of Consumer Protection
In the Matter of

RITE AID CORPORATION,
a corporation.

DOCKET NO. C-4308

DECISION AND ORDER

The Federal Trade Commission having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge the Respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq;

The Respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondent has violated the said Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days, and having duly considered the comments filed thereafter by interested persons pursuant to Section 2.34 of its Rules, now in further conformity with the procedure described in Section 2.34 of its Rules, the Commission hereby issues its Complaint, makes the following jurisdictional findings and enters the following Order:
1. Respondent Rite Aid Corporation is a Delaware corporation with its principal office or place of business at 30 Hunter Lane, Camp Hill, Pennsylvania 17011.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “store” shall mean each pharmacy entity or store location that sells prescription medicines, drugs, devices, supplies, or services and/or non-prescription products and services.

2. Unless otherwise specified, “LLC” shall mean a limited liability company: (a) that owns, controls, or operates one or more stores (including, but not limited to, the companies identified in attached Exhibit A), and (b) in which Rite Aid Corporation is a member, directly or indirectly.

3. Unless otherwise specified, “Respondent” shall mean Rite Aid Corporation, its subsidiaries, divisions, affiliates, and LLCs, and its successors and assigns.

4. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license number or other government-issued identification number; (g) prescription information, such as medication and dosage, and prescribing physician name, address, and telephone number, health insurer name, insurance account number, or insurance policy number; (h) a bank account, debit card, or credit card account number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; (j) a biometric record; or (k) any information that is combined with any of (a) through (j) above. For the purpose of this provision, a “consumer” shall include an “employee,” and an individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, and other person directly or indirectly under the control of Respondent.

I.  

IT IS ORDERED that Respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which it maintains and protects the privacy, confidentiality, security, or integrity of personal information collected from or about consumers.

II.  

IT IS FURTHER ORDERED that Respondent, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they
receive from Respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of Respondent’s information security program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent’s operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with their compliance with Part II of this order, Respondent, and its officers, agents, representatives, and employees, shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first year after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that Respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to Respondent’s size and complexity, the nature and scope of Respondent’s activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part II of this order; and

D. certify that Respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten
(10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Respondent until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

IV.

IT IS FURTHER ORDERED that Respondent shall maintain and, upon request, make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including, but not limited to, documents, prepared by or on behalf of Respondent, that contradict, qualify, or call into question Respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of Respondent, including, but not limited to, all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Respondent’s compliance with Parts II and III of this order, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that Respondent Rite Aid Corporation shall deliver a copy of this order to all its current and future subsidiaries (including LLCs and each store that is owned, controlled, or operated by Respondent or an LLC), current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within sixty (60) days after service of this order, and to such future subsidiaries and personnel within sixty (60) days after the Respondent acquires the subsidiary or the person assumes such position or responsibilities.

VI.

IT IS FURTHER ORDERED that Respondent shall notify the Commission at least thirty (30) days prior to any change in Respondent that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary (including an LLC), parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in Respondent’s name or address. Provided, however, that, with respect to any proposed change in Respondent about which Respondent learns less than thirty (30) days prior to the date such action is to take place, Respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division

VII.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports.

VIII.

This order will terminate on November 12, 2030, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this order that terminates in less than twenty (20) years;

B. This order’s application to any Respondent that is not named as a defendant in such complaint; and

C. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: November 12, 2010
WHEREAS Plaintiff, the United States of America, has commenced this action by filing the complaint herein; Defendant has waived service of the Summons and Complaint; the parties have been represented by the attorneys whose names appear hereafter; and the parties have agreed to Consent Decree
settlement of this action upon the following terms and conditions, without adjudication of any issue
of fact or law, and without Defendant admitting any issue of fact or law other than those related to
jurisdiction and venue;

THEREFORE, on the joint motion of Plaintiff and Defendant, it is hereby ORDERED,
ADJUDGED, and DECREED as follows:

1. This Court has jurisdiction of the subject matter and of the parties pursuant to 28 U.S.C.
   §§ 1331, 1337(a), 1345, and 1355, and 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), and 57b.

2. Venue is proper as to all parties in the Northern District of California under 15 U.S.C.
   § 53(b) and 28 U.S.C. §§ 1391(b)-(c) and 1395(a).

3. The activities of Defendant are in or affecting commerce as defined in Section 4 of the FTC

4. The Complaint states a claim upon which relief may be granted against Defendant under
   Sections 5(a)(1), 5(m)(1)(A), 13(b), and 16(a) of the Federal Trade Commission Act ("FTC
   Act"), 15 U.S.C. §§ 41-58, 45(a)(1), 45(m)(1)(A), 53(b), and 56(a) and under Sections
   1303(c) and 1306(d) of the Children’s Online Privacy Protection Act of 1998 ("COPPA"),
   15 U.S.C. §§ 6501-6506, 6502(c), and 6505(d); the Commission’s Children’s Online Privacy
   Protection Rule, 16 C.F.R. Part 312. Among other things, the Complaint alleges that:

   A. Defendant violated the FTC Act by deceptively representing to consumers that it
      provided reasonable security for the personal information it collected from
      consumers;

   B. Defendant violated COPPA and the FTC Act by failing to provide notice to parents
      of its information practices, and to obtain verifiable parental consent prior to
      collecting, using, and or disclosing personal information from children online;
C. Defendant violated the FTC Act by deceptively representing that it did not collect information from children online; and

D. Defendant violated the FTC Act by deceptively representing that it would delete any personal information collected from children online.

Defendant has entered into this Consent Decree and Order for Civil Penalties, Injunction, and Other Relief ("Order") freely and without coercion. Defendant further acknowledges that it has read the provisions of this Order and is prepared to abide by them.

Plaintiff and Defendant hereby waive all rights to appeal or otherwise challenge the validity of this Order.

Plaintiff and Defendant stipulate and agree that entry of this Order shall constitute a full, complete, and final settlement of this action.

Defendant has agreed that this Order does not entitle it to seek or to obtain attorneys’ fees as a prevailing party under the Equal Access to Justice Act, 28 U.S.C. § 2412, and Defendant further waives any rights to attorneys’ fees that may arise under said provision of law.

Entry of this Order is in the public interest.

DEFINITIONS


The terms “child,” “collects,” “collection,” “Commission,” “delete,” “disclosure,” “Internet,” “online contact information,” “operator,” “parent,” “person,” “personal information,” “third party,” “verifiable consent,” and “website or online service directed to children,” are defined in Section 312.2 of the Rule, 16 C.F.R. § 312.2.
“Consumer personal information” means individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a Social Security number; (f) a driver’s license or other state-issued identification number; (g) a financial institution account number; (h) credit or debit card information; (i) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, or processor serial number; (j) nonpublic communications and content posted on Defendant’s web site or within Defendant’s applications provided on any other web site; or (k) any information that is combined with any of (a) through (i) above.


INJUNCTION REGARDING COLLECTION OF INFORMATION FROM CHILDREN ONLINE

IT IS ORDERED that Defendant, and its officers, agents, representatives, and employees, and all persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, are hereby enjoined, directly or through any corporation, subsidiary, division, website, or other device, in collection with any website or online service directed to children, or on any website or online service through which they, with actual knowledge, collect, use, and/or disclose personal information from children, from:

A. failing to provide sufficient notice of the information Defendant collects online
from children, how it uses such information, its disclosure practices, and all other content, as required by Section 312.4(b) of the Rule, 16 C.F.R. § 312.4(b);

B. failing to provide direct notice to parents of what information Defendant collects online from children, how it uses such information, its disclosure practices, and all other required content, as required by Section 312.4(c) of the Rule, 16 C.F.R. § 312.4(c);

C. failing to obtain verifiable parental consent before any collection, use, and/or disclosure of personal information from children, as required by Section 312.5 of the Rule, 16 C.F.R. § 312.5(a)(1);

D. failing to establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children, as required by Section 312.8 of the Rule, 16 C.F.R. § 312.8; or

E. violating any other provision of the Rule, 16 C.F.R. Part 312, and as the Rule may hereafter be amended. A copy of the Rule is attached hereto as “Appendix A” and incorporated herein as if fully set forth verbatim.

IT IS FURTHER ORDERED that Defendant, and its officers, agents, representatives, and employees, and all persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise, are hereby enjoined, directly or through any corporation, subsidiary, division, website, or other device, in connection with the operation of any website or online service, from making any misrepresentation concerning the collection, use, disclosure, or deletion of children’s personal information.
DELETION OF CHILDREN’S PERSONAL INFORMATION

16. IT IS FURTHER ORDERED that Defendant, within 10 days from the date of receipt of notice of the entry of this Order shall delete all personal information collected and maintained within its possession, custody, or control in violation of the Rule at any time from April 21, 2000 through the date of entry of this Order.

CONSUMER EDUCATION REMEDY

17. IT IS FURTHER ORDERED that, for a period of 5 years from the date of entry of this Order, Defendant, in connection with its operation of any website or online service directed to children, and any website or online service through which Defendant, with actual knowledge, collects, uses, and/or discloses personal information from children, shall place a clear and conspicuous notice, that will unavoidably be seen by users prior to the collection of personal information from the users, which states as follows in bold typeface:

NOTICE: Visit www.OnGuardOnline.gov for tips from the Federal Trade Commission on protecting kids’ privacy online

[“www.OnguardOnline.gov” must contain a hyperlink to http://www.onguardonline.gov/topics/kids-privacy.aspx]

Defendant shall be required to change the hyperlinks/URLs within 15 days after receipt of notice from the Federal Trade Commission of a change to such hyperlinks/URLs.

CIVIL PENALTY

18. IT IS FURTHER ORDERED that Defendant shall pay to Plaintiff a civil penalty, pursuant to Section 5(m)(1)(A) of the FTC Act, 15 U.S.C. § 45(m)(1)(A), in the amount of two hundred and fifty thousand dollars ($250,000), due and payable within five (5) days of receipt of notice of the entry of this Order. Unless otherwise directed, payment
shall be made by electronic fund transfer in accordance with procedures specified by the
Consumer Protection Branch, Civil Division, U.S. Department of Justice, Washington,
DC 20530.

19. Defendant relinquishes all dominion, control, and title to the funds paid to the fullest
extent permitted by law. Defendant shall make no claim to or demand return of the
funds, directly or indirectly, through counsel or otherwise.

20. Defendant agrees that the facts as alleged in the Complaint filed in this action shall be
taken as true, without further proof, in any subsequent civil litigation filed by or on
behalf of the Commission to enforce its rights to any payment or money judgment
pursuant to this Order.

21. In the event of any default in payment, which default continues for ten (10) days beyond
the due date of payment, the entire unpaid penalty, together with interest, as computed
pursuant to 28 U.S.C. § 1961 (accrued from the date of default to the date of payment)
shall immediately become due and payable.

INJUNCTION REGARDING SECURITY OF CONSUMER PERSONAL
INFORMATION

22. **IT IS ORDERED** that Defendant, and its officers, agents, representatives, and
employees, directly or through any corporation, subsidiary, limited liability company,
division, or other device, in connection with the advertising, marketing, promotion,
offering for sale, or sale of any product or service, in or affecting commerce, shall not
misrepresent in any manner, expressly or by implication, the extent to which they
maintain and protect the privacy, confidentiality, security, or integrity of consumer
personal information collected from or about consumers.

Consent Decree Page 7 of 20
23. IT IS FURTHER ORDERED that Defendant, and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, limited liability company, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of consumer personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to Defendant's size and complexity, the nature and scope of Defendant's activities, and the sensitivity of the consumer personal information collected from or about consumers, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of consumer personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks,
intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding consumer personal information they receive from Defendant, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of Defendant’s information security program in light of the results of the testing and monitoring required by subpart C, any material changes to Defendant’s operations or business arrangements, or any other circumstances that Defendant knows or has reason to know may have a material impact on the effectiveness of its information security program.

24. **IT IS FURTHER ORDERED** that, in connection with its compliance with Paragraph 23 of this order, Defendant shall obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first year after service of the Order for the initial Assessment, and (2) each 2 year period thereafter for 20 years after service of the Order for the biennial Assessments.
A. Each Assessment shall:

1. set forth the specific administrative, technical, and physical safeguards that Defendant has implemented and maintained during the reporting period;

2. explain how such safeguards are appropriate to Defendant’s size and complexity, the nature and scope of Defendant’s activities, and the sensitivity of the consumer personal information collected from or about consumers;

3. explain how the safeguards that have been implemented meet or exceed the protections required by the Paragraph 23 of this Order; and

4. certify that Defendant’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of consumer personal information is protected and has so operated throughout the reporting period.

B. Each Assessment shall be prepared and completed within 60 days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.
C. Defendant shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within 10 days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by Defendant until the order is terminated and provided to the Associate Director for Enforcement within 10 days of request.

ORDER ACKNOWLEDGMENTS

IT IS FURTHER ORDERED that Defendant obtain acknowledgments of receipt of this Order:

A. Defendant, within 7 days of entry of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

B. For 8 years after entry of this Order, Defendant must deliver a copy of this Order to: (1) all principals, officers, directors, and managers; (2) all employees, agents, and representatives having supervisory responsibilities relating to the collection, retention, storage, or security of consumer personal information and all employees, agents, and representatives having supervisory responsibilities related to the operation of any website or online service subject to this Order; and (3) any business entity resulting from any change in structure as set forth in the Section titled “Compliance Reporting.” Delivery must occur within 7 days of entry of this Order for current personnel. To all others, delivery must occur before they assume their responsibilities.

C. From each individual or entity to which a Defendant delivered a copy of this Order, that Defendant must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.
COMPLIANCE REPORTING

26. **IT IS FURTHER ORDERED** that Defendant make timely submissions to the Commission:

   A. One hundred eighty (180) days after the date of entry of this Order, Defendant must submit a compliance report, sworn under penalty of perjury. This report must:

   1. Designate at least one telephone number and an email, physical, and postal address as points of contact, which representatives of the Commission may use to communicate with Defendant;

   2. Identify all of Defendant's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses;

   3. Describe the activities of each business, including the products and services offered and the means of advertising, marketing, and sales;

   4. Describe in detail whether and how Defendant is in compliance with each Section of this Order;

   5. Provide a statement setting forth in detail the criteria and process through which Defendant's websites or online services register visitors online for any activity requiring the submission of personal information, and a copy of each different version of screen or page providing or collecting registration information;

   6. Provide a copy of each different version of any privacy notice posted on each website or online service operated by Defendant;

   7. Provide a statement setting forth in detail each place where the privacy Consent Decree
notice on any such website or online service is located and a copy of each
different version of screen or page on which such website or online
service collects personal information;

8. Provide a copy of each different version of any privacy notice sent to
parents of children that register on each website or online service;

9. Provide a statement setting forth in detail when and how each such notice
to parents is provided;

10. Provide a statement setting forth in detail the methods used to obtain
verifiable parental consent prior to any collection, use, and/or disclosure
of personal information from children;

11. Provide a statement setting forth in detail the means provided for parents
to review the personal information collected from their children and to
refuse to permit its further use or maintenance;

12. Provide a statement setting forth in detail why each type of information
collected from a child is reasonably necessary for the provision of the
particular related activity;

13. Provide a statement setting forth in detail the procedures used to protect
the confidentiality, security, and integrity of personal information
collected from children; and

14. Provide a copy of each Order Acknowledgement obtained pursuant to this
Order, unless previously submitted to the Commission.

B. For 20 years following entry of this Order, Defendant must submit a compliance
notice, sworn under penalty of perjury, within 14 days of any change in the
following: (a) any designated point of contact; or (b) the structure of Defendant or any entity that Defendant has any ownership interest in or directly or indirectly controls that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.

C. Defendant must submit to the Commission notice of the filing of any bankruptcy petition, insolvency proceeding, or any similar proceeding by or against Defendant within 14 days of its filing.

D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 18 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.

E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: FTC v. RockYou, Inc.

RECORDKEEPING

27. IT IS FURTHER ORDERED that Defendant must create certain records for 20 years after entry of the Order, and to retain each such record for 5 years. Specifically,
Defendant, in connection with personal information collected from consumers, including children under the age of 13, must maintain the following records:

A. Accounting records showing the revenues from all goods or services sold, all costs incurred in generating those revenues, and the resulting net profit or loss;

B. Personnel records showing, for each person providing services, whether as an employee or otherwise, that person's: name, addresses, and telephone numbers; job title or position; dates of service; and, if applicable, the reason for termination;

C. A copy of all complaints submitted by consumers to Defendant regarding its information security practices or its practices relating to the collection or retention of consumer personal information, including from children;

D. All records necessary to demonstrate full compliance with each provision of this Order, including all submissions to the Commission; and

E. A sample copy of every materially different form, page, or screen created, maintained, or otherwise provided by Defendant through which Defendant collects personal information, and a sample copy of each materially different document containing any representation regarding Defendant's collection, use, and disclosure practices pertaining to personal information of a child. Each web page copy shall be accompanied by the URL of the web page where the material was posted online. Electronic copies shall include all text and graphics files, audio scripts, and other computer files used in presenting information on the Internet. Provided, however, that Defendant shall not be required to retain any document for longer than two (2) years after the document was created, or to
retain a print or electronic copy of any amended web page or screen to the extent that the amendment does not affect Defendant’s compliance obligations under this Order.

COMPLIANCE MONITORING

IT IS FURTHER ORDERED that for the purpose of monitoring compliance with this Order:

A. Within 14 days of receipt of a written request from a representative of the Commission, Defendant must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury; appear for depositions; and produce documents, for inspection and copying. The Commission is also authorized to obtain discovery, without further leave of court, using any of the procedures prescribed by Federal Rules of Civil Procedure 29, 30 (including telephonic depositions), 31, 33, 34, 36, 45, and 69.

B. For matters concerning this Order, the Commission is authorized to communicate directly with Defendant. Defendant must permit representatives of the Commission to interview any employee or other person affiliated with any Defendant who has agreed to such an interview. The person interviewed may have counsel present.

C. The Commission may use all other lawful means, including posing, through its representatives, as consumers, suppliers, or other individuals or entities, to Defendant or any individual or entity affiliated with Defendant, without the necessity of identification or prior notice. Nothing in this Order limits the Commission’s lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.
RETENTION OF JURISDICTION

29. IT IS FURTHER ORDERED that this Court retains jurisdiction of this matter for the purposes of construction, modification, and enforcement of this Order.

JUDGMENT IS THEREFORE ENTERED in favor of Plaintiff and against Defendant, pursuant to all the terms and conditions recited above.

Dated this 27 day of March, 2012.

______________________________
Susan Illston
UNITED STATES DISTRICT JUDGE
The parties, by their counsel, hereby consent to the terms and conditions of the Order as set forth above and consent to the entry thereof.

FOR THE UNITED STATES OF AMERICA:

STUART F. DELEERY
Acting Assistant Attorney General
Civil Division
U.S. Department of Justice

MAAME EWUSI-MENSAH FRIMPONG
Acting Deputy Assistant Attorney General
Civil Division

MICHAEL S. BLUME
Director
Consumer Protection Branch

KENNETH L. JOST
Deputy Director
Consumer Protection Branch

ALAN PHELPS
Trial Attorney
Consumer Protection Branch
U.S. Department of Justice
P.O. Box 386
Washington, DC 20044
Telephone: 202-307-6154
Fax: 202-514-8742
Email: alan.phelps@usdoj.gov
FOR THE FEDERAL TRADE COMMISSION:

KATRINA ANE BLODGETT
Attorney
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
202-326-3158 (voice)
202-326-3062 (fax)

MAMIE KRESSES
Attorney
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
202-326-2070 (voice)
202-326-3259 (fax)

CHRISTOPHER OLESEN
Attorney
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, D.C. 20580
202-326-3621 (voice)
202-326-3259 (fax)
FOR THE DEFENDANT:

RockYou, Inc.

LISA MARINO
Chief Executive Officer
RockYou, Inc.

GARRET RASMUSSEN
Orrick, Herrington & Sutcliffe LLP
Columbia Center
1152 15th Street, N.W.
Washington, D.C. 20005-1706
202-339-8481
Attorney for Defendant RockYou, Inc.
§ 311.5 Labeling.
A manufacturer or other seller may represent, on a label or a container of processed used oil, that such oil is substantially equivalent to new oil for use as engine oil only if the manufacturer has determined that the oil is substantially equivalent to new oil for use as engine oil in accordance with the NIST test procedures prescribed under § 311.4 of this part, and has based the representation on that determination.

§ 311.6 Prohibited acts.
It is unlawful for any manufacturer or other seller to represent, on a label or a container of processed used oil, that such oil is substantially equivalent to new oil for use as engine oil unless the manufacturer or other seller has based such representation on the manufacturer's determination that the processed, used oil is substantially equivalent to new oil for use as engine oil in accordance with the NIST test procedures prescribed under § 311.4 of this part. Violations will be subject to enforcement through civil penalties (as adjusted for inflation pursuant to § 1.98 of this chapter), imprisonment, and/or injunctive relief in accordance with the enforcement provisions of Section 525 of the Energy Policy and Conservation Act (42 U.S.C. 6295).


PART 312—CHILDREN’S ONLINE PRIVACY PROTECTION RULE

Sec.
312.1 Scope of regulations in this part.
312.2 Definitions.
312.3 Regulation of unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.
312.4 Notices.
312.5 Parental consent.
312.6 Right of parent to review personal information provided by a child.
312.7 Prohibition against conditioning a child’s participation on collection of personal information.
312.8 Confidentiality, security, and integrity of personal information collected from children.
312.9 Enforcement.
312.10 Safe harbors.

§ 312.1 Scope of regulations in this part.
This part implements the Children's Online Privacy Protection Act of 1998, (15 U.S.C. 6501, et seq.) which prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet. The effective date of this part is April 21, 2000.

§ 312.2 Definitions.
Child means an individual under the age of 13.
Collects or collection means the gathering of any personal information from a child by any means, including but not limited to:
(a) Requesting that children submit personal information online;
(b) Enabling children to make personal information publicly available through a chat room, message board, or other means, except where the operator deletes all individually identifiable information from postings by children before they are made public, and also deletes such information from the operator's records; or
(c) The passive tracking or use of any identifying code linked to an individual, such as a cookie.
Commission means the Federal Trade Commission.
Delete means to remove personal information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.
Disclosure means, with respect to personal information:
(a) The release of personal information collected from a child in identifiable form by an operator for any purpose, except where an operator provides such information to a person who provides support for the internal operations of the website or online service and who does not disclose or use that information for any other purpose. For purposes of this definition:

373
§ 312.2

(1) Release of personal information means the sharing, selling, renting, or any other means of providing personal information to any third party, and

(2) Support for the internal operations of the website or online service means those activities necessary to maintain the technical functioning of the website or online service, or to fulfill a request of a child as permitted by §312.5(c)(2) and (3); or

(b) Making personal information collected from a child by an operator publicly available in identifiable form, by any means, including by a public posting through the Internet, or through a personal home page posted on a website or online service; a pen pal service; an electronic mail service; a message board; or a chat room.

Federal agency means an agency, as that term is defined in Section 551(1) of title 5, United States Code.

Internet means collectively the myriad of computer and telecommunications facilities, including equipment and operating software, which comprise the interconnected world-wide network of networks that employ the Transmission Control Protocol/Internet Protocol, or any predecessor or successor protocols to such protocol, to communicate information of all kinds by wire, radio, or other methods of transmission.

Online contact information means an e-mail address or any other substantially similar identifier that permits direct contact with a person online.

Operator means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce:

(a) Among the several States or with 1 or more foreign nations;

(b) In any territory of the United States or in the District of Columbia, or between any such territory and

(1) Another such territory, or

(2) Any State or foreign nation; or

(c) Between the District of Columbia and any State, territory, or foreign nation. This definition does not include any nonprofit entity that would otherwise be exempt from coverage under Section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

Parent includes a legal guardian.

Person means any individual, partnership, corporation, trust, estate, cooperative, association, or other entity.

Personal information means individually identifiable information about an individual collected online, including:

(a) A first and last name;

(b) A home or other physical address including street name and name of a city or town;

(c) An e-mail address or other online contact information, including but not limited to an instant messaging user identifier, or a screen name that reveals an individual's e-mail address;

(d) A telephone number;

(e) A Social Security number;

(f) A persistent identifier, such as a customer number held in a cookie or a processor serial number, where such identifier is associated with individually identifiable information; or a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or

(g) Information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition.

Third party means any person who is not:

(a) An operator with respect to the collection or maintenance of personal information on the website or online service; or

(b) A person who provides support for the internal operations of the website or online service and who does not use or disclose information protected under this part for any other purpose.

Obtaining verifiable consent means making any reasonable effort (taking into consideration available technology) to ensure that before personal information is collected from a child, a parent of the child:

374
§312.4 Notice.

(a) General principles of notice. All notices under §§312.3(a) and 312.5 must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.

(b) Notice on the website or online service. Under §312.3(a), an operator of a website or online service directed to children must post a link to a notice of its information practices with regard to children on the home page of its website or online service and at each area on the website or online service where personal information is collected from children. An operator of a general audience website or online service that has a separate children’s area or site must post a link to a notice of its information practices with regard to children on the home page of the children’s area.

(1) Placement of the notice. (i) The link to the notice must be clearly labeled as a notice of the website or online service’s information practices with regard to children;

(ii) The link to the notice must be placed in a clear and prominent place and manner on the home page of the website or online service; and

(iii) The link to the notice must be placed in a clear and prominent place and manner at each area on the website or online service where children directly provide, or are asked to provide, personal information, and in close proximity to the requests for information in each such area.
§ 312.4 16 CFR Ch. I (1-1-10 Edition)

(2) Content of the notice. To be complete, the notice of the website or online service's information practices must state the following:

(i) The name, address, telephone number, and e-mail address of all operators collecting or maintaining personal information from children through the website or online service. Provided that: the operators of a website or online service may list the name, address, phone number, and e-mail address of one operator who will respond to all inquiries from parents concerning the operators' privacy policies and use of children's information, as long as the names of all the operators collecting or maintaining personal information from children through the website or online service are also listed in the notice;

(ii) The types of personal information collected from children and whether the personal information is collected directly or passively;

(iii) How such personal information is or may be used by the operator(s), including but not limited to fulfillment of a requested transaction, recordkeeping, marketing back to the child, or making it publicly available through a chat room or by other means;

(iv) Whether personal information is disclosed to third parties, and if so, the types of business in which such third parties are engaged, and the general purposes for which such information is used; whether those third parties have agreed to maintain the confidentiality, security, and integrity of the personal information they obtain from the operator; and that the parent has the option to consent to the collection and use of their child's personal information without consenting to the disclosure of that information to third parties;

(v) That the operator is prohibited from conditioning a child's participation in an activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity; and

(vi) That the parent can review and have deleted the child's personal information, and refuse to permit further collection or use of the child's information, and state the procedures for doing so.

(c) Notice to a parent. Under §312.5, an operator must make reasonable efforts, taking into account available technology, to ensure that a parent of a child receives notice of the operator's practices with regard to the collection, use, and/or disclosure of the child's personal information, including notice of any material change in the collection, use, and/or disclosure practices to which the parent has previously consented.

(1) Content of the notice to the parent.

(i) All notices must state the following:

(A) That the operator wishes to collect personal information from the child;

(B) The information set forth in paragraph (b) of this section.

(ii) In the case of a notice to obtain verifiable parental consent under §312.5(a), the notice must also state that the parent's consent is required for the collection, use, and/or disclosure of such information, and state the means by which the parent can provide verifiable consent to the collection of information;

(iii) In the case of a notice under the exception in §312.5(c)(3), the notice must also state the following:

(A) That the operator has collected the child's e-mail address or other online contact information to respond to the child's request for information and that the requested information will require more than one contact with the child;

(B) That the parent may refuse to permit further contact with the child and require the deletion of the information, and how the parent can do so; and

(C) That if the parent fails to respond to the notice, the operator may use the information for the purpose(s) stated in the notice.

(iv) In the case of a notice under the exception in §312.5(c)(4), the notice must also state the following:

(A) That the operator has collected the child's name and e-mail address or other online contact information to protect the safety of the child participating on the website or online service;

(B) That the parent may refuse to permit the use of the information and
require the deletion of the information, and how the parent can do so; and
(0) That if the parent fails to respond to the notice, the operator may use the
information for the purpose stated in the notice.

§ 312.5 Parental consent.
(a) General requirements. (1) An operator is required to obtain verifiable pa-
rental consent before any collection, use, and/or disclosure of personal informa-
tion from children, including consent to any material change in the col-
lection, use, and/or disclosure practices to which the parent has previously con-

sent.
(2) An operator must give the parent the option to consent to the collection
and use of the child's personal information without consenting to disclosure of
his or her personal information to third parties.
(b) Mechanisms for verifiable parental consent. (1) An operator must make
reasonable efforts to obtain verifiable parental consent, taking into consider-
ation available technology. Any method to obtain verifiable parental consent
must be reasonably calculated, in light of available technology, to ensure that
the person providing consent is the child's parent.
(2) Methods to obtain verifiable pa-
rental consent that satisfy the require-
ments of this paragraph include; pro-
viding a consent form to be signed by
the parent and returned to the opera-
tor by postal mail or facsimile; re-
quiring a parent to use a credit card in
connection with a transaction; having
a parent call a toll-free telephone num-
ber staffed by trained personnel; using
a digital certificate that uses public
key technology; and using e-mail ac-
companied by a PIN or password ob-
tained through one of the verification
methods listed in this paragraph. Pro-
vided that: Until the Commission oth-

erwise determines, methods to obtain
verifiable parental consent for uses of
information other than the "disclo-
sures" defined by § 312.2 may also in-
clude use of e-mail coupled with ad-

ditional steps to provide assurances that
the person providing the consent is the
parent. Such additional steps include:
(3) Where the operator collects on-
line contact information from a child to
be used to respond directly more than
once to a specific request from the
child, and where such information is
not used for any other purpose. In such
cases, the operator must make reason-
able efforts, taking into consideration
available technology, to ensure that a
parent receives notice and has the op-
portunity to request that the operator
make no further use of the informa-
tion, as described in § 312.4(c), imme-
diately after the initial response and
before making any additional response
to the child. Mechanisms to provide
such notice include, but are not limited
to, sending the notice by postal mail or
sending the notice to the parent's e-
mail address, but do not include asking
a child to print a notice form or send-
ing an e-mail to the child.
(4) Where the operator collects a
child's name and online contact infor-
mation to the extent reasonably nec-
necessary to protect the safety of a child
participant on the website or online

377
§ 312.6 Right of parent to review personal information provided by a child.

(a) Upon request of a parent whose child has provided personal information to a website or online service, the operator of that website or online service is required to provide to that parent the following:

(1) A description of the specific types or categories of personal information collected from children by the operator, such as name, address, telephone number, e-mail address, hobbies, and extracurricular activities;

(2) The opportunity at any time to refuse to permit the operator's further use or future online collection of personal information from that child, and to direct the operator to delete the child's personal information; and

(3) Notwithstanding any other provision of law, a means of reviewing any personal information collected from the child. The means employed by the operator to carry out this provision must:

(i) Ensure that the requestor is a parent of that child, taking into account available technology; and

(ii) Not be unduly burdensome to the parent.

(b) Neither an operator nor the operator's agent shall be held liable under any Federal or State law for any disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information under this section.

(c) Subject to the limitations set forth in § 312.7, an operator may terminate any service provided to a child whose parent has refused, under paragraph (a)(2) of this section, to permit the operator's further use or collection of personal information from his or her child or has directed the operator to delete the child's personal information.

§ 312.7 Prohibition against conditioning a child's participation on collection of personal information.

An operator is prohibited from conditioning a child's participation in a game, the offering of a prize, or another activity on the child's disclosing more personal information than is reasonably necessary to participate in such activity.

§ 312.8 Confidentiality, security, and integrity of personal information collected from children.

The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.

§ 312.9 Enforcement.

Subject to sections 5503 and 5505 of the Children's Online Privacy Protection Act of 1998, a violation of a regulation prescribed under section 5502(a) of this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

§ 312.10 Safe harbors.

(a) In general. An operator will be deemed to be in compliance with the requirements of this part if that operator complies with self-regulatory guidelines, issued by representatives of the marketing or online industries, or by other persons, that, after notice and
§ 312.10

Comment, are approved by the Commission.

(b) Criteria for approval of self-regulatory guidelines. To be approved by the Commission, guidelines must include the following:

(1) A requirement that operators subject to the guidelines ("subject operators") implement substantially similar requirements that provide the same or greater protections for children as those contained in §§312.2 through 312.9;

(2) An effective, mandatory mechanism for the independent assessment of subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Periodic reviews of subject operators' information practices conducted on a random basis either by the industry group promulgating the guidelines or by an independent entity;

(ii) Periodic reviews of all subject operators' information practices, conducted either by the industry group promulgating the guidelines or by an independent entity;

(iii) Seeding of subject operators' databases, if accompanied by either paragraphs (b)(2)(i) or (b)(2)(ii) of this section; or

(iv) Any other equally effective independent assessment mechanism;

and

(3) Effective incentives for subject operators' compliance with the guidelines. This performance standard may be satisfied by:

(i) Mandatory, public reporting of disciplinary action taken against subject operators by the industry group promulgating the guidelines;

(ii) Consumer redress;

(iii) Voluntary payments to the United States Treasury in connection with an industry-directed program for violators of the guidelines;

(iv) Referral to the Commission of operators who engage in a pattern or practice of violating the guidelines; or

(v) Any other equally effective incentive.

(4) The assessment mechanism required under paragraph (b)(2) of this section can be provided by an independent enforcement program, such as a seal program. In considering whether to initiate an investigation or to bring an enforcement action for violations of this part, and in considering appropriate remedies for such violations, the Commission will take into account whether an operator has been subject to self-regulatory guidelines approved under this section and whether the operator has taken remedial action pursuant to such guidelines, including but not limited to actions set forth in paragraphs (b)(3)(i) through (iii) of this section.

(c) Request for Commission approval of self-regulatory guidelines. (1) To obtain Commission approval of self-regulatory guidelines, industry groups or other persons must file a request for such approval. A request shall be accompanied by the following:

(i) A copy of the full text of the guidelines for which approval is sought and any accompanying commentary;

(ii) A comparison of each provision of §§312.3 through 312.8 with the corresponding provisions of the guidelines; and

(iii) A statement explaining:

(A) How the guidelines, including the applicable assessment mechanism, meet the requirements of this part; and

(B) How the assessment mechanism and compliance incentives required under paragraphs (b)(2) and (3) of this section provide effective enforcement of the requirements of this part.

(2) The Commission shall act upon a request under this section within 180 days of the filing of such request and shall set forth its conclusions in writing.

(3) Industry groups or other persons whose guidelines have been approved by the Commission must submit proposed changes in those guidelines for review and approval by the Commission in the manner required for initial approval of guidelines under paragraph (c)(1). The statement required under paragraph (c)(1)(iii) must describe how the proposed changes affect existing provisions of the guidelines.

(d) Records. Industry groups or other persons who seek safe harbor treatment by compliance with guidelines that have been approved under this part shall maintain for a period not less than three years and upon request make available to the Commission for inspection and copying:
§ 312.11

(1) Consumer complaints alleging violations of the guidelines by subject operators;

(2) Records of disciplinary actions taken against subject operators; and

(3) Results of the independent assessments of subject operators' compliance required under paragraph (b)(2) of this section.

(e) Revocation of approval. The Commission reserves the right to revoke any approval granted under this section if at any time it determines that the approved self-regulatory guidelines and their implementation do not, in fact, meet the requirements of this part.

§ 312.11 Rulemaking review.

No later than April 21, 2005, the Commission shall initiate a rulemaking review proceeding to evaluate the implementation of this part on practices relating to the collection and disclosure of information relating to children, children's ability to obtain access to information of their choice online, and on the availability of websites directed to children; and report to Congress on the results of this review.

§ 312.12 Severability.

The provisions of this part are separate and severable from one another. If any provision is stayed or determined to be invalid, it is the Commission's intention that the remaining provisions shall continue in effect.

PART 313—PRIVACY OF CONSUMER FINANCIAL INFORMATION

Sec.
313.1 Purpose and scope.
313.2 Model privacy form and examples.
313.3 Definitions.

Subpart A—Privacy and Opt Out Notices

313.4 Initial privacy notice to consumers required.
313.5 Annual privacy notice to customers required.
313.6 Information to be included in privacy notices.
313.7 Form of opt out notice to consumers; opt out methods.
313.8 Revised privacy notices.

16 CFR Ch. I (1-1-10 Edition)

313.9 Delivering privacy and opt out notices.

Subpart B—Limits on Disclosures

313.10 Limitation on disclosure of nonpublic personal information to nonaffiliated third parties.
313.11 Limits on redisclosure and reuse of information.
313.12 Limits on sharing account number information for marketing purposes.

Subpart C—Exceptions

313.13 Exception to opt out requirements for service providers and joint marketing.
313.14 Exceptions to notice and opt out requirements for processing and servicing transactions.
313.15 Other exceptions to notice and opt out requirements.

Subpart D—Relation to Other Laws; Effective Date

313.16 Protection of Fair Credit Reporting Act.
313.17 Relation to State laws.
313.18 Effective date; transition rule.

APPENDIX A TO PART 313—MODEL PRIVACY FORM

APPENDIX B TO PAR T 313—SAMPLE CLAUSES

AUTHORITY: 16 U.S.C. 6801 et seq.

SOURCE: 65 FR 33617, May 24, 2000, unless otherwise noted.

§ 313.1 Purpose and scope.

(a) Purpose. This part governs the treatment of nonpublic personal information about consumers by the financial institutions listed in paragraph (b) of this section. This part:

(1) Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices;

(2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and

(3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to the exceptions in §§313.13, 313.14, and 313.15.

(b) Scope. This part applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family or household purposes from the
UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

___________________________________________

In the Matter of

SETLEMENTONE CREDIT CORPORATION,,
a corporation; and

SACKETT NATIONAL HOLDINGS, INC.,
a corporation.

DOCKET NO. C-4330
DECISION AND ORDER


The Respondents, their attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the Respondents of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by Respondents that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission's Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the Respondents have violated the Federal Trade Commission Act, the Fair Credit Reporting Act, and the Gramm-Leach-Bliley Act’s Safeguards Rule, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a
period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons, now in further conformity with the procedure described in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:

1.a. Respondent SettlementOne is a California corporation with its principal office or place of business at 2605 Camino Del Rio South, Suite 400, San Diego, CA 92108. SettlementOne is a wholly-owned subsidiary of Sackett National Holdings, Inc.

1.b. Respondent Sackett National Holdings, Inc. is a corporation with its principal office or place of business at 2605 Camino Del Rio South, San Diego, CA 92108. SNH conducts business through its ten wholly-owned subsidiaries, including SettlementOne.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondents, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information; (d) a telephone number; (e) a Social Security number; (f) a credit card or debit card account number; (g) checking account information, (h) a driver’s license, military or state identification number; (i) a persistent identifier, such as a customer number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.


6. Unless otherwise specified, “respondents” shall mean Sackett National Holdings and SettlementOne Credit Corporation, and their subsidiaries, divisions, affiliates, successors and assigns.


I.

IT IS ORDERED that respondents shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers, including the security, confidentiality, and integrity of personal information accessible to end users. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to the respondents’ size and complexity, the nature and scope of the respondents’ activities, and the sensitivity of the personal information collected from or about consumers. The information security program must include:

A. the designation of an employee or employees to coordinate and be accountable for the information security program;

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, access, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures;

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they
receive from the respondents, and requiring service providers by contract to implement and maintain appropriate safeguards; and

E. the evaluation and adjustment of the respondents’ information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondents’ operations or business arrangements, or any other circumstances that respondents know or have reason to know may have a material impact on the effectiveness of their information security program.

II.

IT IS FURTHER ORDERED that respondents and their officers, agents, representatives, and employees, shall not, directly or through any corporation, subsidiary, division, website, or other device, violate any provision of the Safeguards Rule, 16 C.F.R. Part 314. In the event that this Rule is hereafter amended or modified, respondents’ compliance with that Rule as so amended or modified shall not be a violation of this order.

III.

IT IS FURTHER ORDERED that respondents, in connection with the compilation, creation, sale, or dissemination of any consumer report shall:

A. Furnish such consumer report only to those persons which it has reason to believe have a permissible purpose as described in Section 604(a)(3) of the Fair Credit Reporting Act, 15 U.S.C. § 1681b(a)(3), or under such other circumstances as set forth in Section 604 of the Fair Credit Reporting Act, 15 U.S.C. § 1681b;

B. Maintain reasonable procedures to limit the furnishing of such consumer report to those with a permissible purpose and ensure that no consumer report is furnished to any person when there are reasonable grounds to believe that the consumer report will not be used for a permissible purpose, as required by Section 607(a) of the Fair Credit Reporting Act, 15 U.S.C. § 1681e(a).

IV.

IT IS FURTHER ORDERED that respondents shall, in connection with their compliance with Part I of this order, obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession, provided however; that except for SettlementOne Credit Corporation for which such Assessments are always required, Sackett National Holdings, Inc. shall not be required to obtain such Assessments for any subsidiary, division, affiliate, successor or assign if the personal information such entities collect, maintain, or store from or about consumers is limited to a first and last name; a home or other physical address, including street name and name of city or town; an email address; a telephone number; or publicly available information regarding property ownership and appraised home value. Each
Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondents have implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondents’ size and complexity, the nature and scope of respondents’ activities, and the sensitivity of the personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by the Safeguards Rule; and

D. certify that respondents’ security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Respondents shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondents until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days after respondents receive such request.

V.

IT IS FURTHER ORDERED that respondents shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying:

A. for a period of five (5) years, a print or electronic copy of each document relating to compliance, including but not limited to documents, prepared by or on behalf of respondents, that contradict, qualify, or call into question respondents’ compliance with this order;

B. for a period of five (5) years, copies of all subpoenas and other communications with law enforcement entities or personnel, whether in written or electronic form,
if such documents bear in any respect on respondents’ collection, maintenance, or furnishing of consumer reports or other personal information of consumers; and

C. for a period of three (3) years after the date of preparation of each Assessment required under Part IV of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondents, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondents’ compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

VI.

IT IS FURTHER ORDERED, that for a period of five (5) years from the date of entry of this Order, respondents shall deliver copies of the Order as directed below:

A. Respondents must deliver a copy of this order to (1) all current and future principals, officers, directors and managers, (2) all employees, agents and representatives who engage in conduct related to the subject matter of the order, and (3) any business entity resulting from any change in structure set forth in Part VII. For current personnel, delivery shall be within five (5) days of service of this Order. For new personnel, delivery shall occur prior to them assuming their responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure.

B. Respondents must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondents shall notify the Commission at least thirty (30) days prior to any change in the corporations that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that with respect to any proposed change in the corporations about which respondents learn less than thirty (30) days prior to the date such action is to take place, respondents shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.
VIII.

IT IS FURTHER ORDERED that respondents and their successors and assigns, within sixty (60) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of their own compliance with this order. Within ten (10) day of receipt of written notice from a representative of the Commission, they shall submit additional true and accurate written reports.

IX.

This order will terminate on August 17, 2031, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;
B. this order’s application to any respondent that is not named as a defendant in such complaint; and
C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondents did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Richard C. Donohue
Acting Secretary

SEAL
ISSUED: August 17, 2011
The Federal Trade Commission (“Commission” or “FTC”), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure prescribed in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Order:

1. Respondent Snapchat, Inc. (“Snapchat”), the successor corporation to Toyopa Group LLC, is a Delaware corporation with its principal office or place of business at 63 Market Street, Venice, California 90291.
2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Snapchat, Inc. and its successors and assigns.


3. “Covered information” shall mean information from or about an individual consumer, including but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a persistent identifier, such as a customer number held in a “cookie,” a static Internet Protocol (“IP”) address, a mobile device ID, or processor serial number; (f) precise geo-location data of an individual or mobile device, including GPS-based, Wi-Fi-based, or cell-based location information; (g) an authentication credential, such as a username or password; or (h) any communications or content that is transmitted or stored through respondent’s products or services.

4. “Computer” shall mean any desktop, laptop computer, tablet, handheld device, telephone, or other electronic product or device that has a platform on which to download, install, or run any software program, code, script, or other content and to play any digital audio, visual, or audiovisual content.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or indirectly, shall not misrepresent in any manner, expressly or by implication, in or affecting commerce, the extent to which respondent or its products or services maintain and protect the privacy, security, or confidentiality of any covered information, including but not limited to: (1) the extent to which a message is deleted after being viewed by the recipient; (2) the extent to which respondent or its products or services are capable of detecting or notifying the sender when a recipient has captured a screenshot of, or otherwise saved, a message; (3) the categories of covered information collected; or (4) the steps taken to protect against misuse or unauthorized disclosure of covered information.
II.

IT IS FURTHER ORDERED that respondent, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive privacy program that is reasonably designed to: (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information, whether collected by respondent or input into, stored on, captured with, or accessed through a computer using respondent’s products or services. Such program, the content and implementation of which must be fully documented in writing, shall contain privacy controls and procedures appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information, including:

A. the designation of an employee or employees to coordinate and be accountable for the privacy program;

B. the identification of reasonably foreseeable, material risks, both internal and external, that could result in the respondent’s unauthorized collection, use, or disclosure of covered information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this privacy risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order; and (2) product design, development and research;

C. the design and implementation of reasonable privacy controls and procedures to address the risks identified through the privacy risk assessment, and regular testing or monitoring of the effectiveness of the privacy controls and procedures;

D. the development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this order, and requiring service providers by contract to implement and maintain appropriate safeguards;

E. the evaluation and adjustment of respondent’s privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows, or has reason to know, may have a material impact on the effectiveness of its privacy program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this order, respondent shall obtain initial and biennial assessments and reports ("Assessments") from
a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. A person qualified to prepare such Assessments shall have a minimum of three (3) years of experience in the field of privacy and data protection. All persons selected to conduct such assessments and prepare such reports shall be approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific privacy controls that respondent has implemented and maintained during the reporting period;

B. explain how such privacy controls are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the covered information;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this order; and

D. certify that the privacy controls are operating with sufficient effectiveness to provide reasonable assurance to protect the privacy of covered information and that the controls have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 with the subject line In the Matter of Snapchat, Inc., FTC File No. 1323078.

IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, unless respondent asserts a valid legal privilege, a print or electronic copy of:

A. for a period of five (5) years from the date of preparation or dissemination, whichever is later, statements disseminated to consumers that describe the extent to which

Snapchat
respondent maintains and protects the privacy, security and confidentiality of any covered information, including, but not limited to, any statement related to a change in any website or service controlled by respondent that relates to the privacy, security, and confidentiality of covered information, with all materials relied upon in making or disseminating such statements;

B. for a period of five (5) years from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to the conduct prohibited by this order and any responses to such complaints;

C. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent that contradict, qualify, or call into question respondent’s compliance with this order; and

D. for a period of five (5) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of respondent including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

V.

**IT IS FURTHER ORDERED** that respondent shall deliver a copy of this order to all current and future subsidiaries, current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current subsidiaries and personnel within thirty (30) days after service of this order, and to such future subsidiaries and personnel within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VI, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this order, within thirty (30) days of delivery, from all persons receiving a copy of the order pursuant to this section.

VI.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part
shall be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580 with the subject line In the Matter of Snapchat, Inc., FTC File No. 1323078.

VII.

IT IS FURTHER ORDERED that respondent within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

VIII.

This order will terminate on December 23, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Janice Podoll Frankle
Acting Secretary

SEAL
ISSUED: December 23, 2014
DECISION AND ORDER

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the Respondent named in the caption hereof, and the Respondent having been furnished thereafter with a copy of a draft of Complaint which the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the Respondent with violation of the Federal Trade Commission Act; and

The Respondent and counsel for the Commission having thereafter executed an agreement containing a consent order, an admission by the Respondent of all the jurisdictional facts set forth in the aforesaid draft complaint, a statement that the signing of the agreement is for settlement purposes only and does not constitute an admission by the Respondent that the law has been violated as alleged in such complaint, or that any of the facts as alleged in such complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the Respondent has violated the Federal Trade Commission Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, now in further conformity with the procedure prescribed in Section 2.34 of its Rules, 16 C.F.R. § 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following order:
1. Respondent The TJX Companies, Inc. is a Delaware corporation with its principal office or place of business at 770 Cochituate Road, Framingham, Massachusetts, 01701.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this Order, the following definitions shall apply:

1. “Personal information” shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual’s email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information, including the ABA routing number, account number, and check number; (h) a driver’s license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a “cookie” or processor serial number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.

2. Unless otherwise specified, “respondent” shall mean The TJX Companies, Inc., and its successors and assigns, officers, agents, representatives, and employees.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, or other device, in connection with the advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce, shall, no later than the date of service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers, including:
A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of material internal and external risks to the security, confidentiality, and integrity of personal information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, and assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding personal information they receive from respondent, and requiring service providers by contract to implement and maintain appropriate safeguards.

E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by sub-Part C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

II.

IT IS FURTHER ORDERED that, in connection with its compliance with Part I of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the personal information collected from or about consumers;
C. explain how the safeguards that have been implemented meet or exceed the protections required by the Part I of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of personal information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.

III.

IT IS FURTHER ORDERED that respondent shall maintain, and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of each document relating to compliance, including but not limited to:

A. for a period of five (5) years: any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

B. for a period of three (3) years after the date of preparation of each Assessment required under Part II of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Parts I and II of this order, for the compliance period covered by such Assessment.

IV.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel
within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.

V.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Part shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VI.

IT IS FURTHER ORDERED that respondent shall, within one hundred eighty (180) days after service of this order, and at such other times as the Federal Trade Commission may require, file with the Commission a report, in writing, setting forth in detail the manner and form in which it has complied with this order.

VII.

This order will terminate on July 29, 2028, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in less than twenty (20) years;

B. this order’s application to any respondent that is not named as a defendant in such complaint; and

C. this order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and
the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: July 29, 2008
The Federal Trade Commission ("Commission" or "FTC"), having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued by the Commission, would charge respondent with violations of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45 et seq.;

The respondent, its attorney, and counsel for the Commission having thereafter executed an Agreement Containing Consent Order ("Consent Agreement"), which includes: a statement by respondent that it neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in the Consent Agreement, and, only for purposes of this action, admits the facts necessary to establish jurisdiction; and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it had reason to believe that the respondent has violated the FTC Act, and that a complaint should issue stating its charges in that respect, and having thereupon accepted the executed consent agreement and placed such agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons pursuant to Commission Rule 2.34, 16 C.F.R. § 2.34, now in further conformity with the procedure prescribed in Commission Rule 2.34, the Commission hereby issues its complaint, makes the following jurisdictional findings, and enters the following Decision and Order ("Order"): 
1. Respondent TRENDnet, Inc. (“TRENDnet”) is a California corporation with its principal office or place of business at 20675 Manhattan Place, Torrance, California 90501.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the respondent, and the proceeding is in the public interest.

**ORDER**

**DEFINITIONS**

For purposes of this Order, the following definitions shall apply:

1. “Affected Consumers” shall mean persons who purchased and installed one of the following Cameras with software last updated prior to February 7, 2012: TV-IP110 (Version A1.xR); TV-IP110W (Version A1.xR); TV-IP110WN (Version A1.xR); TV-IP110WN (Version V2.0R); TV-IP121W (Version A1.xR); TV-IP121WN (Version V1.0R); TV-IP121WN (Version V2.0R); TV-IP212 (Version A1.xR); TV-IP212W (Version V1.xR); TV-IP252P (Version B1.xR); TV-IP312 (Version A1.xR); TV-IP312W (Version V1.xR); TV-IP312WN (Version A1.xR); TV-IP322P (Version V1.0R); TV-IP410 (Version A1.XR); TV-IP410W (Version A1.xR); TV-IP410WN (Version V1.0R); TV-IP422 (Versions A1.xR/A2.xR); TV-IP422W (Versions A1.xR/A2.xR); TV-IP422WN (Version V1.0R); TV-VS1 (Version V1.0R); and TV-VS1P (Version V1.0R).

2. “App” or “Apps” shall mean any software application or related code developed, branded, or provided by respondent for a mobile device, including, but not limited to, any iPhone, iPod touch, iPad, BlackBerry, Android, Amazon Kindle, or Microsoft Windows device.

3. “Cameras” shall mean any Internet Protocol (“IP”) camera, cloud camera, or other Internet-accessible camera advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits, or allows for the transmission of Live Feed Information over the Internet.

4. “Clear(ly) and prominent(ly)” shall mean:
   
   A. In textual communications (e.g., printed publications or words displayed on the screen of a computer or device), the required disclosures are of a type, size, and location sufficiently noticeable for an ordinary consumer to read and comprehend them, in print that contrasts highly with the background on which they appear;

   B. In communications disseminated orally or through audible means (e.g., radio or streaming audio), the required disclosures are delivered in a volume and cadence sufficient for an ordinary consumer to hear and comprehend them;
C. In communications disseminated through video means (e.g., television or streaming video), the required disclosures are in writing in a form consistent with subparagraph (A) of this definition and shall appear on the screen for a duration sufficient for an ordinary consumer to read and comprehend them, and in the same language as the predominant language that is used in the communication; and

D. In all instances, the required disclosures (1) are presented in an understandable language and syntax; and (2) include nothing contrary to, inconsistent with, or in mitigation of any other statements or disclosures provided by respondent.

5. “Commerce” shall mean commerce among the several States or with foreign nations, or in any Territory of the United States or in the District of Columbia, or between any such Territory and another, or between any such Territory and any State or foreign nation, or between the District of Columbia and any State or Territory or foreign nation, as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

6. “Covered Device” shall mean: (1) any Internet-accessible electronic product or device, including but not limited to “Cameras,” advertised, developed, branded, or sold by respondent, or on behalf of respondent, or any corporation, subsidiary, division or affiliate owned or controlled by respondent that transmits or allows for the transmission of Covered Information over the Internet; and (2) any App or software advertised, developed, branded, or provided by respondent or any corporation, subsidiary, division or affiliate owned or controlled by respondent used to operate, manage, access, or view the product or device.

7. “Covered Device Functionality” shall mean any capability of a Covered Device to capture, access, store, or transmit Covered Information.

8. “Covered Information” shall mean individually-identifiable information from or about an individual consumer input into, stored on, captured with, accessed, or transmitted through a Covered Device, including but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as a user identifier or screen name; (d) photos; (e) videos; (f) pre-recorded and live-streaming audio; (g) an IP address, User ID or other persistent identifier; or (h) an authentication credential, such as a username or password.

9. “Live Feed Information” shall mean video, audio, or audiovisual data.

I.

IT IS ORDERED that respondent and its officers, agents, representatives, and employees, directly or through any corporation, subsidiary, division, website, other device, or an affiliate owned or controlled by respondent, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication:

A. The extent to which respondent or its products or services maintain and protect:
   1. The security of Covered Device Functionality;
   2. The security, privacy, confidentiality, or integrity of any Covered Information; and

B. The extent to which a consumer can control the security of any Covered Information input into, stored on, captured with, accessed, or transmitted by a Covered Device.

II.

IT IS FURTHER ORDERED that respondent shall, no later than the date of service of this Order, establish and implement, and thereafter maintain, a comprehensive security program that is reasonably designed to (1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information, whether collected by respondent, or input into, stored on, captured with, accessed, or transmitted through a Covered Device. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the Covered Device Functionality or Covered Information, including:

A. The designation of an employee or employees to coordinate and be accountable for the security program;

B. The identification of material internal and external risks to the security of Covered Devices that could result in unauthorized access to or use of Covered Device Functionality, and assessment of the sufficiency of any safeguards in place to control these risks;

C. The identification of material internal and external risks to the security, confidentiality, and integrity of Covered Information that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of such information, whether such information is in respondent’s possession or is input into, stored on, captured with, accessed, or transmitted through a Covered
Device, and assessment of the sufficiency of any safeguards in place to control these risks;

D. At a minimum, the risk assessments required by Subparts B and C should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-party security vulnerability reports;

E. The design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user’s security settings;

F. Regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures;

G. The development and use of reasonable steps to select and retain service providers capable of maintaining security practices consistent with this Order, and requiring service providers, by contract, to establish and implement, and thereafter maintain, appropriate safeguards consistent with this Order; and

H. The evaluation and adjustment of the security program in light of the results of the testing and monitoring required by Subpart F, any material changes to the respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Part II of this Order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such Assessments shall be: a person qualified as a Certified Secure Software Lifecycle Professional (CSSLP) with experience programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or as a Certified Information System Security Professional (CISSP) with professional experience in the Software Development Security domain and in programming secure Covered Devices or other similar Internet-accessible consumer-grade devices; or a similarly qualified person or organization; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal
Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after service of the Order for the initial Assessment; and (2) each two (2) year period thereafter for twenty (20) years after service of the Order for the biennial Assessments. Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. Explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the Covered Device Functionality or Covered Information;

C. Explain how the safeguards that have been implemented meet or exceed the protections required by Part II of this Order; and

D. Certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance that the security of Covered Device Functionality and the security, confidentiality, and integrity of Covered Information is protected and has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the Order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request. Unless otherwise directed by a representative of the Commission, the initial Assessment, and any subsequent Assessments requested, shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the Matter of TRENDnet, Inc., FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.

IV.

IT IS FURTHER ORDERED that respondent shall:

A. Notify Affected Consumers, clearly and prominently, that their Cameras had a flaw that allowed third parties to access their Live Feed Information without inputting authentication credentials, despite their security setting choices; and provide instructions on how to remove this flaw. Notification shall include, but not be limited to, each of the following means:
1. On or before ten (10) days after the date of service of this Order and for two (2) years after the date of service of this Order, posting of a notice on its website;

2. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who complain or inquire about a Camera; and

3. On or before ten (10) days after the date of service of this Order and for three (3) years after the date of service of this Order, informing Affected Consumers who register, or who have registered, their Camera with respondent; and

B. Provide prompt and free support with clear and prominent contact information to help consumers update and/or uninstall a Camera. For two (2) years after the date of service of this Order, this support shall include toll-free, telephonic and electronic mail support.

V.

**IT IS FURTHER ORDERED** that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. For a period of five (5) years after the date of preparation of each Assessment required under Part III of this Order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to respondent’s compliance with Part III of this Order, for the compliance period covered by such Assessment;

B. Unless covered by V.A, for a period of five (5) years from the date of preparation or dissemination, whichever is later, all other documents relating to compliance with this Order, including but not limited to:

1. All advertisements, promotional materials, installation and user guides, and packaging containing any representations covered by this Order, as well as all materials used or relied upon in making or disseminating the representation; and
2. Any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this Order.

VI.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this Order to all (1) current and future subsidiaries, (2) current and future principals, officers, directors, and managers, (3) current and future employees, agents, and representatives having responsibilities relating to the subject matter of this Order, and (4) current and future manufacturers and service providers of the Covered Products. Respondent shall deliver this Order to such current subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after service of this Order, and to such future subsidiaries, personnel, manufacturers, and service providers within thirty (30) days after the person assumes such position or responsibilities. For any business entity resulting from any change in structure set forth in Part VII, delivery shall be at least ten (10) days prior to the change in structure. Respondent must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of the Order pursuant to this section.

VII.

IT IS FURTHER ORDERED that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation(s) that may affect compliance obligations arising under this Order, including, but not limited to: a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation(s) about which respondent learns fewer than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission, all notices required by this Part shall be sent by overnight courier (not the U.S. Postal Service) to the Associate Director of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580, with the subject line In the Matter of TRENDnet, Inc., FTC File No. 1223090, Docket No. C-4426. Provided, however, that in lieu of overnight courier, notices may be sent by first-class mail, but only if an electronic version of any such notice is contemporaneously sent to the Commission at Debrief@ftc.gov.
VIII.

IT IS FURTHER ORDERED that respondent within sixty (60) days after the date of service of this Order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this Order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit an additional true and accurate written report.

IX.

This Order will terminate on January 16, 2034, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the Order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

A. Any Part in this Order that terminates in fewer than twenty (20) years;

B. This Order’s application to any respondent that is not named as a defendant in such complaint; and

C. This Order if such complaint is filed after the Order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: January 16, 2014
UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
William E. Kovacic
J. Thomas Rosch
Edith Ramirez
Julie Brill

In the Matter of

TWITTER, INC.,
a corporation.

DOCKET NO: C-4316

DEcision and order

The Federal Trade Commission, having initiated an investigation of certain acts and practices of the respondent named in the caption hereof, and the respondent having been furnished thereafter with a copy of a draft Complaint that the Bureau of Consumer Protection proposed to present to the Commission for its consideration and which, if issued, would charge the respondent with violation of the Federal Trade Commission Act, 15 U.S.C. § 45 et seq.;

The respondent and counsel for the Commission having thereafter executed an Agreement Containing Consent Order (“Consent Agreement”), an admission by the respondent of all the jurisdictional facts set forth in the aforesaid draft Complaint, a statement that the signing of said Consent Agreement is for settlement purposes only and does not constitute an admission by the respondent that the law has been violated as alleged in such Complaint, or that the facts as alleged in such Complaint, other than jurisdictional facts, are true, and waivers and other provisions as required by the Commission’s Rules; and

The Commission having thereafter considered the matter and having determined that it has reason to believe that the respondent has violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect, and having thereupon accepted the executed Consent Agreement and placed such Consent Agreement on the public record for a period of thirty (30) days for the receipt and consideration of public comments, and having duly considered the comments received from interested persons, now in further conformity with the procedure described in Commission Rule 2.34, 16 C.F.R. § 2.34, the Commission hereby issues its Complaint, makes the following jurisdictional findings, and enters the following Order:
1. Respondent Twitter, Inc. (“Twitter”) is a Delaware corporation with its principal office or place of business at 795 Folsom Street, Suite 600, San Francisco, CA 94103.

2. The Federal Trade Commission has jurisdiction of the subject matter of this proceeding and of the Respondent, and the proceeding is in the public interest.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, “respondent” shall mean Twitter, its successors and assigns, officers, agents, representatives, and employees.

2. “Consumer” shall mean any person, including, but not limited to, any user of respondent’s services, any employee of respondent, or any individual seeking to become an employee, where “employee” shall mean an agent, servant, salesperson, associate, independent contractor, or other person directly or indirectly under the control of respondent.

3. “Nonpublic consumer information” shall mean nonpublic, individually-identifiable information from or about an individual consumer, including, but not limited to, an individual consumer’s: (a) email address; (b) Internet Protocol (“IP”) address or other persistent identifier; (c) mobile telephone number; and (d) nonpublic communications made using respondent’s microblogging platform. “Nonpublic consumer information” shall not include public communications made using respondent’s microblogging platform.

4. “Administrative control of Twitter” shall mean the ability to access, modify, or operate any function of the Twitter system by using systems, features, or credentials that were designed exclusively for use by authorized employees or agents of Twitter.


I.

IT IS ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall not misrepresent in any manner, expressly or by implication, the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, including, but not limited to, misrepresentations related to its security measures to: (a) prevent unauthorized access to nonpublic consumer information; or (b) honor the privacy choices exercised by users.
II.

IT IS FURTHER ORDERED that respondent, directly or through any corporation, subsidiary, division, website, or other device, in connection with the offering of any product or service, in or affecting commerce, shall, no later than the date or service of this order, establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information. Such program, the content and implementation of which must be fully documented in writing, shall contain administrative, technical, and physical safeguards appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the nonpublic consumer information, including:

A. the designation of an employee or employees to coordinate and be accountable for the information security program.

B. the identification of reasonably-foreseeable, material risks, both internal and external, that could result in the unauthorized disclosure, misuse, loss, alteration, destruction, or other compromise of nonpublic consumer information or in unauthorized administrative control of the Twitter system, and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this risk assessment should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) information systems, including network and software design, information processing, storage, transmission, and disposal; and (3) prevention, detection, and response to attacks, intrusions, account takeovers, or other systems failures.

C. the design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems, and procedures.

D. the development and use of reasonable steps to select and retain service providers capable of appropriately safeguarding nonpublic consumer information such service providers receive from respondent or obtain on respondent’s behalf, and the requirement, by contract, that such service providers implement and maintain appropriate safeguards; provided, however, that this subparagraph shall not apply to personal information about a consumer that respondent provides to a government agency or lawful information supplier when the agency or supplier already possesses the information and uses it only to retrieve, and supply to respondent, additional personal information about the consumer.
E. the evaluation and adjustment of respondent’s information security program in light of the results of the testing and monitoring required by subparagraph C, any material changes to respondent’s operations or business arrangements, or any other circumstances that respondent knows or has reason to know may have a material impact on the effectiveness of its information security program.

III.

IT IS FURTHER ORDERED that, in connection with its compliance with Paragraph II of this order, respondent shall obtain initial and biennial assessments and reports (“Assessments”) from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. Professionals qualified to prepare such assessments shall be: a person qualified as a Certified Information System Security Professional (CISSP) or as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580. The reporting period for the Assessments shall cover: (1) the first one hundred and eighty (180) days after service of the order for the initial Assessment, and (2) each two (2) year period thereafter for ten (10) years after service of the order for the biennial Assessments. Each Assessment shall:

A. set forth the specific administrative, technical, and physical safeguards that respondent has implemented and maintained during the reporting period;

B. explain how such safeguards are appropriate to respondent’s size and complexity, the nature and scope of respondent’s activities, and the sensitivity of the nonpublic personal information collected from or about consumers;

C. explain how the safeguards that have been implemented meet or exceed the protections required by Paragraph II of this order; and

D. certify that respondent’s security program is operating with sufficient effectiveness to provide reasonable assurance to protect the security, privacy, confidentiality, and integrity of nonpublic consumer information and that the program has so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies. Respondent shall provide the initial Assessment to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessment has been prepared. All subsequent biennial Assessments shall be retained by respondent until the order is terminated and provided to the Associate Director of Enforcement within ten (10) days of request.
IV.

IT IS FURTHER ORDERED that respondent shall maintain and upon request make available to the Federal Trade Commission for inspection and copying, a print or electronic copy of:

A. for a period of three (3) years from the date of preparation or dissemination, whichever is later, all widely-disseminated statements, including, but not limited to, statements posted on respondent’s website that describe the extent to which respondent maintains and protects the security, privacy, confidentiality, or integrity of any nonpublic consumer information, with all materials relied upon in making or disseminating such statements, except that respondent shall not be required to provide any such statements that are made using the Twitter microblogging platform;

B. for a period of six (6) months from the date received, all consumer complaints directed at respondent, or forwarded to respondent by a third party, that relate to respondent’s activities as alleged in the draft complaint and any responses to such complaints;

C. for a period of two (2) years from the date received, copies of all subpoenas and other communications with law enforcement entities or personnel, if such communications raise issues that relate to respondent’s compliance with the provisions of this order;

D. for a period of five (5) years from the date received, any documents, whether prepared by or on behalf of respondent, that contradict, qualify, or call into question respondent’s compliance with this order; and

E. for a period of three (3) years after the date of preparation of each Assessment required under Part III of this order, all materials relied upon to prepare the Assessment, whether prepared by or on behalf of the respondent, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, for the compliance period covered by such Assessment.

V.

IT IS FURTHER ORDERED that respondent shall deliver a copy of this order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having responsibilities relating to the subject matter of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after service of this order, and to such future personnel within thirty (30) days after the person assumes such position or responsibilities.
VI.

**IT IS FURTHER ORDERED** that respondent shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in either corporate name or address. **Provided, however,** that, with respect to any proposed change in the corporation about which respondent learns less than thirty (30) days prior to the date such action is to take place, respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. All notices required by this Paragraph shall be sent by certified mail to the Associate Director, Division of Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.

VII.

**IT IS FURTHER ORDERED** that respondent shall, within sixty (60) days after the date of service of this order file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form in which respondent has complied with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, respondent shall submit additional true and accurate written reports.

VIII.

This order will terminate on March 2, 2031, or twenty (20) years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; **provided, however,** that the filing of such a complaint will not affect the duration of:

A. any Part in this order that terminates in fewer than twenty (20) years;

B. this order if such complaint is filed after the order has terminated pursuant to this Part.

**Provided, further,** that if such complaint is dismissed or a federal court rules that respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order as to such respondent will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date
such complaint is filed and the later of the deadline for appealing such dismissal or ruling and
the date such dismissal or ruling is upheld on appeal.

By the Commission.

Donald S. Clark
Secretary

SEAL
ISSUED: March 2, 2011
THOMAS P. O'BRIEN  
United States Attorney  
LEE WEIDMAN  
Assistant United States Attorney  
Chief, Civil Division  
GARY PLESSMAN  
Assistant United States Attorney  
Chief, Civil Fraud Section  
California State Bar No. 101233  
Room 7516, Federal Building  
300 North Los Angeles Street  
Los Angeles, California, 90012  
Telephone: (213) 894-2474  
Facsimile: (213) 894-2380  
Email: gary.plessman@usdoj.gov

Attorneys for Plaintiff United States of America

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,  
Plaintiff,  

v.  

VALUECLICK, INC., HI-SPEED MEDIA, INC., and E-BABYLON, INC.,  
Defendants.

Plaintiff, the United States of America, acting upon notification and authorization to the Attorney General by the Federal Trade Commission ("FTC" or the "Commission"), pursuant to Section 16(a)(1) of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 56(a)(1), has filed a complaint pursuant to Sections 5(a)(1), 5(m)(1)(A), 13(b), 16(a), and 19 of the FTC Act, 15 U.S.C. §§ 45(a)(1), 45(m)(1)(A), 53(b), 56(a), and 57b and under Section 7(a) of the Controlling the Assault of Non-
Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM" or the "CAN-SPAM Act"), 15 U.S.C. § 7706(a), to secure civil penalties, a permanent injunction, and other equitable relief for Defendants' violations of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), and Section 5(a) of CAN-SPAM, 15 U.S.C. § 7704(a).

Defendants have waived service of the Summons and Complaint; the parties have been represented by the attorneys whose names appear hereafter; and the parties have agreed to settlement of this action upon the following terms and conditions, without adjudication of any issue of fact or law and without Defendants admitting liability for any of the matters alleged in the Complaint.

THEREFORE, on the joint motion of the parties, it is hereby ORDERED, ADJUDGED AND DECREED as follows:

FINDINGS

1. This Court has jurisdiction over the subject matter of this action pursuant to 15 U.S.C. §§ 45(m)(1)(A), 53(b), 56(a), 57b, and 7706(a), and 28 U.S.C. §§ 1331, 1337(a), 1345, and 1355.

2. Plaintiff and Defendants consent to jurisdiction and venue in this District.

3. The activities of Defendants are in or affecting commerce, as that term is defined in Section 4 of the FTC Act, 15 U.S.C. § 44.

4. For purposes of any future proceeding brought by Plaintiff to enforce this order, the Complaint states a claim upon which relief may be granted against Defendants under Section 5(a) of the CAN-SPAM Act, 15 U.S.C. § 7704(a), and Sections 5(a),
5. Defendants have entered into this Stipulated Final Judgment For Civil Penalties and Permanent Injunctive Relief ("Order") freely and without coercion.

6. Defendants hereby waive all rights to appeal or otherwise challenge or contest the validity of this Order.

7. Defendants agree that this Order does not entitle Defendants to seek or to obtain attorneys' fees as a prevailing party under the Equal Access to Justice Act, 28 U.S.C. § 2412, and Defendants further waive any rights to attorneys' fees that may arise under said provision of law.

8. Entry of this Order is in the public interest.

9. This Final Order is for settlement purposes only, and does not constitute and shall not be interpreted to constitute an admission by Defendants or a finding that the law has been violated as alleged in the Complaint, or that the facts alleged in the Complaint, other than jurisdictional facts, are true, and in fact, Defendants specifically deny violating the FTC Act, the CAN-SPAM Act, or any other law or regulation.

**DEFINITIONS**

For the purpose of this Order, the following definitions shall apply:

1. "Commerce" shall mean as it is defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.

2. "Commercial electronic mail ('email') message" means any email message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service
(including content on an Internet website operated for a commercial purpose) and that further satisfies the requirements of 16 C.F.R. §§ 316.1 – 316.5, as they exist now and may be amended.


4. "Document" is synonymous in meaning and equal in scope to the usage of the term in Federal Rule of Civil Procedure 34(a), and includes writings, drawings, graphs, charts, photographs, audio and video recordings, computer records, and other data compilations from which information can be obtained and translated, if necessary, into reasonably usable form through detection devices. A draft or non-identical copy is a separate document within the meaning of the term.

5. "Electronic mail ('email') address" means a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the "local part") and a reference to an Internet domain (commonly referred to as the "domain part"), whether or not displayed, to which an email message can be sent or delivered.

6. "Electronic mail ('email') message" means a message sent to a unique email address.

7. "Initiate," when used with respect to a commercial email message, means to originate or transmit such message or to procure the origination or transmission of such message, but shall not include actions that constitute routine conveyance of
such message. For purposes of this Order, more than one person may be considered to have initiated a message.

8. "Landing page" means, in online marketing, a specific web page that a visitor reaches after clicking a link or advertisement in an email or banner ad. This page usually showcases content that is an extension of the link or ad.

9. "Person" means a natural person or a corporation, partnership, proprietorship, limited liability company, or other organization or legal entity, including an association, cooperative, or agency, or other group or combination acting as an entity.

10. "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a social security number; (f) credit and/or debit card information, including credit and/or debit card number, expiration date, and/or CVV or CVV2 security code information contained in card magnetic stripes or other storage media or otherwise printed or maintained on card surfaces in any form; (g) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (h) any other information from or about an individual consumer that is combined with any one of (a) through (g) above.
11. "Procure," when used with respect to the initiation of a commercial email message, means intentionally to pay or provide other consideration to, or induce, another person to initiate such a message on one's behalf.

12. "Recipient," when used with respect to a commercial email message, means an authorized user of the email address to which the message was sent or delivered. If a recipient of a commercial email message has one or more email addresses in addition to the address to which the message was sent or delivered, the recipient shall be treated as a separate recipient with respect to each such address. If an email address is reassigned to a new user, the new user shall not be treated as a recipient of any commercial email message sent or delivered to that address before it was reassigned.

13. "Sender," when used with respect to a commercial email message, means a person who initiates such a message and whose product, service, or Internet website is advertised or promoted by the message.

ORDER

I. PROHIBITION AGAINST FAILING TO DISCLOSE MATERIAL INFORMATION

IT IS THEREFORE ORDERED that Defendants ValueClick, Inc. and Hi-Speed Media, Inc., their successors, assigns, officers, agents, servants, and employees, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise are hereby permanently restrained and enjoined from:

A. In any email and online advertisement, or on any landing page associated with such email or online advertisement,
that contains any direct or implied representation made by
Defendants ValueClick, Inc. or Hi-Speed Media, Inc., or made by
any authorized agent on behalf of Defendants ValueClick, Inc. or
Hi-Speed Media, Inc., that a product is free, failing to
disclose, in the same color, font, and size, and within close
proximity to such representation, that a purchase is required, or
that purchases are required, to obtain such product, when such is
the case; and

B. On any landing page associated with any direct or
implied representation made by Defendants ValueClick, Inc. or Hi-
Speed Media, Inc., or made by any authorized agent on behalf of
Defendants ValueClick, Inc. or Hi-Speed Media, Inc., that a
product is free, failing to disclose, in a clear and conspicuous
manner:

1. A list of the monetary obligations a consumer is
   likely to incur to obtain the advertised product;

2. A list of any non-monetary obligations a consumer
   is likely to incur to obtain the advertised
   product, such as having to apply and qualify for
   credit cards or an automobile loan.

II. PROHIBITION AGAINST VIOLATING THE CAN-SPAM ACT

IT IS FURTHER ORDERED that Defendants ValueClick, Inc. and
Hi-Speed Media, Inc., their successors, assigns, officers,
agents, servants, and employees, and those persons in active
concert or participation with them who receive actual notice of
this Order by personal service or otherwise are hereby
permanently restrained and enjoined from violating the CAN-SPAM
Act, 15 U.S.C. §§ 7701 et seq., attached hereto as Attachment A,
and as it may be amended, by, including, but not limited to, initiating the transmission of a commercial email message with a subject header that misrepresents the content or subject matter of the message.

III. CIVIL PENALTIES

IT IS FURTHER ORDERED that Defendants ValueClick, Inc. and Hi-Speed Media, Inc. shall pay to Plaintiff a Civil Penalty, pursuant to Section 5(m)(1)(A) of the Federal Trade Commission Act, 15 U.S.C. § 45(m)(1)(A), in the amount of $2,900,000 as follows:

A. Defendants ValueClick, Inc. and Hi-Speed Media, Inc. shall make the payment required by this Part within ten (10) business days of the date of entry of this Order by electronic fund transfer or certified or cashier's check in accordance with the instructions provided by the Office of Consumer Litigation, Civil Division, U.S. Department of Justice, Washington, D.C. 20530, for appropriate disposition;

B. In the event of any default in payment, which default continues for ten (10) business days beyond the due date of payment, the entire unpaid penalty, together with interest, as computed pursuant to 28 U.S.C. § 1961, from the date of default to the date of payment, shall immediately become due and payable; and

C. This Civil Penalty arises from the past practices of Hi-Speed Media, Inc., and not any other subsidiary of ValueClick, Inc.
IV. PROHIBITION AGAINST MISREPRESENTATIONS

IT IS FURTHER ORDERED that Defendants ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., their successors, assigns, officers, agents, servants, and employees, and those persons in active concert or participation with them who receive actual notice of this Order by personal service or otherwise are hereby permanently restrained and enjoined from misrepresenting in any manner, expressly or by implication:

A. The existence or use of encryption to protect personal information collected from or about consumers;

B. The existence, purposes, features, functions, or efficacy of any hardware, software, or other electronic information solutions used to protect the privacy, confidentiality, and security of personal information belonging to consumers; and

C. The manner or extent to which the privacy, confidentiality, or security of any personal information collected from or about consumers is maintained or protected.

V. INFORMATION SECURITY PROGRAM

IT IS FURTHER ORDERED that, in connection with the online advertising, marketing, promotion, offering for sale, or sale of any product or service to consumers, in or affecting commerce, Defendants ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., and their successors and assigns, directly or through any corporation, subsidiary, division, or other device, and all other persons or entities within the scope of Fed. R. Civ. P. 65, are hereby permanently restrained and enjoined from, no later than the date of entry of this Order, failing to establish and
implement, and thereafter maintain, a comprehensive information
security program that is reasonably designed to protect the
security, confidentiality, and integrity of personal information
collected from or about consumers. Such program, the content and
implementation of which must be fully documented in writing,
shall contain administrative, technical, and physical safeguards
appropriate to the entity's size and complexity, the nature and
scope of the entity's activities, and the sensitivity of the
personal information collected from or about consumers,
including:

A. The designation of an employee or employees to
coordinate and be accountable for the information security
program;

B. The identification of material internal and external
risks to the security, confidentiality, and integrity of personal
information that could result in the unauthorized disclosure,
misuse, loss, alteration, destruction, or other compromise of
such information, and assessment of the sufficiency of any
safeguards in place to control these risks. At a minimum, this
risk assessment should include consideration of risks in each
area of relevant operation, including, but not limited to: (1)
employee training and management; (2) information systems,
including network and software design, information processing,
storage, transmission, and disposal; and (3) prevention,
detection, and response to attacks, intrusions, or other system
failures;

C. The design and implementation of reasonable safeguards
to control the risks identified through risk assessment, and
regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures;

D. The development and use of reasonable steps to retain service providers capable of appropriately safeguarding personal information they receive from the entity, requiring service providers by contract to implement and maintain appropriate safeguards, and monitoring their safeguarding of personal information; and

E. The evaluation and adjustment of the entity's information security program in light of the results of the testing and monitoring required by Paragraph C of this Part, any material changes to the entity's operations or business arrangements, or any other circumstances that the entity knows or has reason to know may have a material impact on the effectiveness of its information security program.

VI. PERIODIC AUDITS AND ASSESSMENTS

IT IS FURTHER ORDERED that, in connection with the online advertising, marketing, promotion, or offering for sale of any product that Defendants sell to consumers, in or affecting commerce, Defendants ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., and their successors and assigns, shall each obtain initial and biennial assessments and reports ("Assessments") from a qualified, objective, independent third-party professional, who uses procedures and standards generally accepted in the profession. The reporting period for the Assessments shall cover: (1) the first one hundred eighty (180) days after entry of the order for the initial Assessment, and (2) each two (2) year period thereafter for twenty (20) years after
entry of the order for the biennial Assessments. Each Assessment shall:

A. Set forth the specific administrative, technical, and physical safeguards that the entity has implemented and maintained during the reporting period to comply with Part V of this Order;

B. Explain how such safeguards are appropriate to the entity's size and complexity, the nature and scope of the entity's activities, and the sensitivity of the nonpublic personal information collected from or about consumers;

C. Explain how such safeguards meet or exceed the protections required by Part V of this order; and

D. Certify that the entity's security programs are operating with sufficient effectiveness to provide reasonable assurance that the security, confidentiality, and integrity of nonpublic personal information is protected and have so operated throughout the reporting period.

Each Assessment shall be prepared and completed within sixty (60) days after the end of the reporting period to which the Assessment applies by a person qualified as a Certified Information System Security Professional (CISSP); a person qualified as a Certified Information Systems Auditor (CISA); a person holding Global Information Assurance Certification (GIAC) from the SysAdmin, Audit, Network, Security (SANS) Institute; or a similarly qualified person or organization approved by the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580.
Defendants ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., and their successors and assigns, shall provide their initial Assessments to the Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, Washington, D.C. 20580, within ten (10) days after the Assessments have been prepared. All subsequent biennial Assessments shall be retained by Defendants ValueClick, Inc., Hi-Speed Media, Inc., and E-Babylon, Inc., and their successors and assigns, until the order is terminated and provided to the Associate Director for Enforcement within ten (10) days of request.

VII. COMPLIANCE MONITORING

IT IS FURTHER ORDERED that, for the purpose of monitoring and investigating compliance with any provision of this Order:

A. Within thirty (30) days of receipt of written notice from a representative of the Commission or Plaintiff, Defendants each shall submit additional written reports, sworn to under penalty of perjury; produce documents for inspection and copying; appear for deposition; and/or provide entry during normal business hours to any business location in such Defendant's possession or direct or indirect control to inspect the business operation;

B. In addition, the Commission and Plaintiff are authorized to monitor compliance with this Order by all other lawful means, including but not limited to the following:

1. Obtaining discovery from any person, without further leave of court, using the procedures
prescribed by Fed. R. Civ. P. 30, 31, 33, 34, 36, and 45;

2. Posing as consumers and suppliers to Defendants, Defendants' employees, or any other entity managed or controlled in whole or in part by Defendants, without the necessity of identification or prior notice; and

C. Within ten (10) days of receipt of written notice from a representative of the Commission, Defendants shall permit representatives of the Commission or Plaintiff to interview any employer, consultant, independent contractor, representative, agent, or employee who has agreed to such an interview, relating in any way to any conduct subject to this Order. The person interviewed may have counsel present.

Provided, however, that nothing in this Order shall limit the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1, to obtain any documentary material, tangible things, testimony, or information relevant to unfair or deceptive acts or practices in or affecting commerce (within the meaning of 15 U.S.C. § 45(a)(1)).

VIII. COMPLIANCE REPORTING BY DEFENDANTS

IT IS FURTHER ORDERED that, in order that compliance with the provisions of this Order may be monitored:

A. For a period of five (5) years from the date of entry of this Order, Defendants shall notify the Commission of any changes in corporate structure that may affect compliance obligations arising under this Order, including but not limited
to a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor entity; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order; the filing of a bankruptcy petition; or a change in the corporate name or address, at least thirty (30) days prior to such change, provided that, with respect to any proposed change in the corporation about which Defendants learn less than thirty (30) days prior to the date such action is to take place, Defendants shall notify the Commission as soon as is practicable after obtaining such knowledge;

B. One hundred eighty (180) days after the date of entry of this Order, Defendants each shall provide a written report to the FTC, sworn to under penalty of perjury, setting forth in detail the manner and form in which it has complied and is complying with this Order. This report shall include, but not be limited to:

1. A copy of each acknowledgment of receipt of this Order, obtained pursuant to Part X of this Order; and

2. Any changes required to be reported pursuant to Paragraph A of this Part;

C. For the purposes of this Order, Defendants shall, unless otherwise directed in writing by the Commission's authorized representatives, mail all written notifications to the Commission to:

Associate Director for the Division of Enforcement Federal Trade Commission 601 New Jersey Avenue, N.W.
Washington, D.C. 20580
Re: United States v. ValueClick, Inc., et al.
Case No. ______;

D. For the purposes of this Order, Defendants shall, unless otherwise directed in writing by a representative of Plaintiff, identify all written notifications required to be sent to Plaintiff as in reference to DJ# 102-3450, and mail them to:

Director, Office of Consumer Litigation
U.S. Department of Justice - Civil Division
P.O. Box 386
Washington, D.C. 20044; and

E. For purposes of the compliance reporting and monitoring required by this Order, representatives of Plaintiff and the Commission are authorized to communicate directly with Defendants.

IX. RECORD-KEEPING PROVISIONS

IT IS FURTHER ORDERED that Defendants are hereby restrained and enjoined from failing to create and retain the following records for the following periods:

A. For a period of eight (8) years from the date of entry of this Order the following records in connection with the marketing, advertising, or promotion of any product that Defendants represent, directly or by implication, is free:

1. Standard accounting records generated in the ordinary course of business including, but not limited to, balance sheets, income statements, and annual reports;

2. Personnel records accurately reflecting: the name, address, and telephone number of each person employed in any capacity by such business, including as an
independent contractor; that person's job title or position; the date upon which the person commenced work; and the date and reason for the person's termination, if applicable;

3. Customer files containing consumers' name, address, telephone number, offer completion status, gift redemption status, quantity of rewards shipped, description of rewards shipped, quantity of checks issued, and amounts of checks issued;

4. Complaints and refund requests from the prior five (5) years (whether received directly, indirectly or through any third party) and any responses to those complaints or requests;

5. Copies of all sales scripts, training materials, advertisements, or other marketing materials;

6. Records demonstrating reasonable policies and procedures to process and handle customer inquiries and complaints; and

7. Other than the records described in Paragraphs B and C of this Part, all records and documents necessary to demonstrate full compliance with each provision of this Order, including but not limited to, copies of acknowledgments of receipt of this Order required by Part X.B, and all reports submitted to the FTC pursuant to Part VIII of this Order;

B. For a period of five (5) years from the date of entry of this Order: Any documents, whether prepared by or on behalf of Defendants, that contradict, qualify, or call into question
Defendants' compliance with Parts IV, V, and VI of this order; and

C. For a period of three (3) years after the date of preparation of each Assessment required under Part VI of this order: All materials relied upon to prepare the Assessment, whether prepared by or on behalf of any Defendant, including but not limited to all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials relating to Defendants' compliance with Part VI of this order, Assessment.

X. DISTRIBUTION OF ORDER BY DEFENDANTS

IT IS FURTHER ORDERED that, for a period of five (5) years from the date of entry of this Order, Defendants shall deliver copies of this Order as directed below:

A. Defendants must deliver a copy of this Order to all current and future principals, officers, directors, and managers, and to all current and future employees, agents, and representatives having supervisory responsibilities relating to the subject matter of this Order. For current personnel, delivery shall be within ten (10) days of service of this Order upon Defendant. For new personnel, delivery shall occur prior to them assuming their responsibilities; and

B. Defendants must secure a signed and dated statement acknowledging receipt of this Order, within thirty (30) days of delivery, from all persons receiving a copy of this Order pursuant to this Part.
XI. ACKNOWLEDGMENT OF RECEIPT OF ORDER BY DEFENDANTS

IT IS FURTHER ORDERED that Defendants, within five (5) business days of receipt of this Order as entered by the Court, must submit to the Commission and Plaintiff a truthful sworn statement acknowledging receipt of this Order.

XII. FEES AND COSTS

IT IS FURTHER ORDERED that each party to this Order hereby agrees to bear its own costs and attorneys' fees incurred in connection with this action.

XIII. SEVERABILITY

IT IS FURTHER ORDERED that the provisions of this Order are separate and severable from one another. If any provision is stayed or determined to be invalid, the remaining provisions shall remain in full force and effect.

XIV. RETENTION OF JURISDICTION

IT IS FURTHER ORDERED that this Court shall retain jurisdiction of this matter for purposes of construction, modification, and enforcement of this Order.

XV. COMPLETE SETTLEMENT

The parties, by their respective counsel, hereby consent to entry of the foregoing Order, which shall constitute a final judgment and order in this matter. The parties further stipulate and agree that the entry of the foregoing Order shall constitute full, complete, and final settlement of this action.
FOR THE PLAINTIFF:

UNITED STATES OF AMERICA:

JEFFREY S. BUCHOLTZ
Acting Assistant Attorney General
Civil Division
U.S. Department of Justice

THOMAS P. O’BRIEN
United States Attorney
Central District of California
LEE WEIDMAN
Assistant United States Attorney
Chief, Civil Division

GARY PLESSMAN
Assistant United States Attorney
Chief, Civil Fraud Section
California State Bar No. 101233
Room 7516, Federal Building
300 North Los Angeles Street
Los Angeles, California, 90012
Telephone: (213) 894-2474
Facsimile: (213) 894-2380
Email: gary.plessman@usdoj.gov

EUGENE M. THIROLF
Director
KENNETH L. JOST
Deputy Director
Office of Consumer Litigation

JOHN W. BURKE
Trial Attorney
Office of Consumer Litigation
U.S. Department of Justice
P.O. Box 386
Washington, D.C. 20044
PHONE: 202-353-2001
FAX: 202-514-8742
josh.burke@usdoj.gov
FOR THE FEDERAL TRADE COMMISSION

_________________________
LOIS C. GREISMAN
Associate Director for Marketing Practices

_________________________
Stephen L. Cohen
Ethan Arenson
Attorneys, Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

_________________________
JOEL WINSTON
Associate Director for Privacy and Identity Protection
Burke Kappler
Attorney, Federal Trade Commission
601 New Jersey Avenue, N.W.
Washington, D.C. 20580

FOR THE DEFENDANTS:

M. Sean Royall
Gibson Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036-8546

ValueClick, Inc.

BY: __________________________
30699 Russell Road, Suite 250
Westlake Village, CA 91361

Hi-Speed Media, Inc.

BY: __________________________
30699 Russell Road, Suite 250
Westlake Village, CA 91361

E-Babylon, Inc.

BY: __________________________
30699 Russell Road, Suite 250
Westlake Village, CA 91361

SO ORDERED this ___ day of ________________, 2008.

__________________________
United States District Judge

Stipulated Final Judgment  Page 22 of 22