Boston Bar Association Intellectual Property 2014 Year in Review
Privacy & Data Security

Peter J. Guffin, Esq., CIPP/US
Pierce Atwood LLP
254 Commercial Street
Portland, ME 04101
P: 207-791-1199
E: pguffin@pierceatwood.com

Sara M. Benjamin, Esq., CIPP/US
Pierce Atwood LLP
100 Summer Street
Suite 2250
Boston, MA 02110
P: 617-488-8162
E: sbenjamin@pierceatwood.com

Biographical Information:

Peter J. Guffin is a partner at the law firm Pierce Atwood LLP. Peter is Chair of the firm's Intellectual Property and Technology Group and heads the firm's Privacy & Data Security practice. He has extensive experience in the areas of intellectual property, information technology, privacy and data protection and represents businesses in a wide range of industries, including information technology, energy, banking, retail, financial services, insurance and healthcare.

Sara M. Benjamin is an associate at the law firm Pierce Atwood LLP. Sara is a member of the firm's Intellectual Property and Technology Group and the firm's Privacy & Data Security practice. She focuses primarily on privacy and data security regulatory compliance as well as trademark, copyright and software licensing matters.

Introduction

The legal framework with regard to privacy and data security in the United States is a patchwork of federal, state, and industry-specific laws and regulations. There is no single, comprehensive, national law. As a result, ensuring compliance in an environment in which corporate data practices are quickly evolving is a challenge.

This manuscript provides an overview of recent selected enforcement actions by two of the most active federal regulatory agencies in the privacy and data security space—the Federal Trade Commission ("FTC") and the Department of Health and Human Services, Office of Civil Rights ("OCR")—and is intended to provide some guidance to companies striving to adopt and implement reasonable privacy

and data security policies and practices. It also provides a brief update on related litigation challenging the FTC's enforcement authority in this area.

I. FTC Regulatory Authority

FTC Generally. The primary privacy and information security legal regime applicable to most companies is the one overseen and enforced by the Federal Trade Commission ("FTC") under the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §§ 41-58. The FTC Act prohibits two kinds of conduct in trade: conduct that is "deceptive" and conduct that is "unfair."

- Jurisdiction. The FTC has jurisdiction over most, but not all, companies that engage in interstate commerce. Notable exceptions include banks, savings and loan institutions, federal credit unions, and common carriers. *See* 15 U.S.C. § 45(a)(2).

De Facto Guardian of Consumer Privacy. Using its powers under the Act, the FTC has become the *de facto* guardian of the privacy and security of consumer information at the federal level. Professor Daniel Solove, one of the nation's foremost scholars on privacy and the FTC, has observed that, "in practice, FTC privacy jurisprudence has become the broadest and most influential regulating force on information privacy in the United States – more so than nearly any privacy statute and any common law tort." *See* Daniel Solove, *The FTC and the New Common Law of Privacy*, Privacy + Security Training: News, Developments, and Insights (Aug. 20, 2013), http://www.teachprivacy.com/ftc-new-common-law-privacy/.

Key Legal Theories. Historically, the FTC has pursued two primary theories to meet its burden of showing that a privacy or data security incident violates the FTC Act:

- Deceptive Practices. Representations made to consumers about a company's privacy practices or protection of personal information should not be deceptive. More generally, the FTC considers an act to be "deceptive" if:
    - There is a representation, omission, or practice;
    - That misleads or is likely to mislead the consumer acting reasonably under the circumstances; and
    - That is likely to affect the consumer's conduct or decision with regard to a particular product or service.

- Unfair Practices. Unfair practices include a company's failure to take reasonable measures to safeguard personal information. More generally, the FTC considers an act to be "unfair" if it:

- Causes or is likely to cause consumer injury;
- Cannot be reasonably avoided by consumers; and
- Is not outweighed by countervailing benefits to consumers or competition.

The FTC's Enforcement Powers. The FTC has the power to issue cease and desist orders against companies, file complaints in court, and engage in civil investigations through the use of Civil Investigative Demands. A recent example of a Civil Investigative Demand issued by the FTC in the aftermath of a data breach is attached as Appendix A. The latter Civil Investigative Demand, among other things, is instructive of what the FTC may expect to see in an information security program. In practice, most consumer privacy and security enforcement actions have been resolved by agreement, with the company under investigation agreeing to a consent order requiring that it comply with certain requirements and subject itself to oversight by the FTC for a period of time. *See, e.g.*, *In re HTC Am, Inc.*, FTC File No. 122 3049, No. C-4406 (F.T.C. July 2, 2013) (consent order), *available at http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htcdo.pdf*, FTC File No. 102 3136, No. C-4336, at 4 (F.T.C. Oct. 13, 2011) (consent order), *available at* http://ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf. The content of these consent decrees has arguably evolved, over time, into a kind of "roadmap" of practices that companies should avoid.

Challenges to FTC Authority. Recently, however, there have been two major challenges to the FTC's authority to regulate privacy and data security under Section 5 of the FTC Act brought by Wyndham Worldwide Corp. and LabMD, Inc. Although still pending, the outcome of these cases could have a tremendous impact on the power of the FTC to regulate privacy and data security practices in the U.S.

FTC v. Wyndham Worldwide Corp. In the *Wyndham* case, hackers gained unauthorized access to Wyndham's computer network on three separate occasions, using similar techniques on each occasion. As a result, hackers were able to gain access to customers' personal information including payment card account numbers, expiration dates and security codes. The FTC found Wyndham's failure to take appropriate steps to prevent future network attacks, even after the first two incidents, was an unfair practice in violation of Section 5. Based on these allegations, the FTC brought a case against Wyndham, and Wyndham moved to dismiss. In this case, Wyndham:

- Challenges the authority of the FTC to bring unfairness claims against companies for failing to provide reasonable data security;

- Alleges that the FTC must formally promulgate regulations before bringing an unfairness claim; and

- Alleges that the FTC did not sufficiently meet its burden to demonstrate either unfairness or deception.

Status of FTC v. Wyndham Worldwide Corp. In April of 2014, the U.S. District Court for the District of New Jersey denied Wyndham's motion to dismiss. The Court found no evidence to support Wyndham's contention that the FTC's unfairness authority is incompatible with more recent data security legislation. Rather, it found subsequent data security legislation including FCRA, GLBA, and COPPA seem to complement—not preclude—the FTC's authority. The Court also disagreed with Wyndham as to the need for formally promulgated rules and regulations to provide fair notice and found that the FTC's complaint sufficiently pleads unfairness and deception claims.

In July of 2014, the U.S. Court of Appeals for the Third Circuit granted Wyndham's petition to appeal the April decision. The Court is expected to rule in 2015.

In the Matter of LabMD, Inc. In the *LabMD* case, billing information for over 9,000 consumers was found on a peer-to-peer file-sharing network, exposing consumer personal health information. Later, LabMD documents containing consumer personal information were found in the hands of identity thieves. LabMD moved to dismiss the FTC's complaint based on the FTC's lack of authority to address private companies' data security practices under the unfairness prong of Section 5. It further argued that the Health Insurance Portability and Accountability Act ("HIPPA"), which regulates the privacy and data security of protected health information, preempts any FTC authority with regard to health information.

Status of In the Matter of LabMD, Inc. In January of 2014, the FTC denied LabMD's motion to dismiss its administrative complaint. LabMD then petitioned the 11th Circuit Court of Appeals to hear the case, but the petition was dismissed in February 2014 based on lack of jurisdiction. Undeterred, LabMD filed suit again in U.S. District Court for the Northern District of Georgia, Atlanta Division seeking to enjoin the FTC enforcement action. In May 2014 the Georgia court, too, granted the FTC's motion to dismiss based on its lack of authority to enjoin an ongoing proceeding. LabMD appealed this decision and in August 2014, the 11th Circuit agreed to hear oral argument on the matter. Oral argument is expected to be heard in 2015.

Impact. Depending on their outcomes, the *Wyndham* and *LabMD* cases could have a significant impact on the FTC's authority to regulate data security under the unfairness prong of the FTC Act.

II. FTC Guidance Regarding Reasonable Privacy and Data Security Practices

FTC Enforcement Action Guidance. Although Wyndham argues the FTC must formally promulgate regulations to provide fair notice of its expectations, recent enforcement actions provide some lessons for companies striving to maintain reasonable privacy and data security practices. The following lessons from this past year are particularly noteworthy:

- Accurately describe your privacy and data security practices;
- Implement such practices as represented to customers; and
- Ensure mobile apps comply with privacy and data security obligations as well.

Accurately Describe and Implement Privacy and Data Security Practices. The following 2014 cases demonstrate the importance of accurately describing your company's privacy and data security practices and ensuring such practices are actually implemented.

- In the Matter of True Ultimate Standards Everywhere, Inc (TRUSTe). The FTC alleged TRUSTe falsely represented its recertification process by representing that it recertified all companies displaying a TRUSTe Certified Privacy Seal annually in order to ensure ongoing compliance. In fact, TRUSTe did not recertify all companies annually. And many of the companies recertified by TRUSTe had failed to update references to TRUSTe's corporate status, which changed from a non-profit to a for-profit entity in 2008. As part of the settlement, TRUSTe is prohibited from making misrepresentations about its recertification process and corporate status, and must pay $200,000.

- In the Matter of Snapchat, Inc. Snapchat, a photo messaging mobile app, allegedly misrepresented 1) the extent to which a message is deleted after being viewed by the recipient; 2) the extent to which Snapchat is capable of detecting or notifying the sending party when a recipient has captured a screenshot of, or otherwise saved, a message; 3) the categories of covered information collected; and 4) the steps taken to protect against misuse or unauthorized disclosure of covered information. As part of its settlement, Snapchat is prohibited from such misrepresentations and is required to establish, implement and maintain a comprehensive privacy program.

- EU-U.S. Safe Harbor Program. In an effort to strengthen EU-US relations, the FTC announced settlements with the following 14 companies regarding false claims of compliance with the EU-U.S. Safe Harbor

Program: American Apparel; Apperian, Inc.; Atlanta Falcons Football Club, LLC; Baker Tilly Virchow Krause, LLP; BitTorrent, Inc.; Charles River Laboratories International, Inc.; DataMotion, Inc.; DDC Laboratories, Inc.; Fantage, Inc.; Level 3 Communications, LLC; PDB Sports, Ltd., d/b/a Denver Broncos Football Club; Reynolds Consumer Products Inc.; Receivable Management Services Corporation; and Tennessee Football, Inc. Under these settlements, the aforementioned companies are prohibited from misrepresenting the extent to which they participate in any privacy and data security program sponsored by the government or any other self-regulatory or standard-setting organization.

Mobile Apps Must Also Comply with Privacy and Data Security Requirements. In 2014 the FTC highlighted the importance of ensuring mobile apps comply with privacy and data security obligations as demonstrated by the following cases.

- In the Matter of Fandango, LLC. Fandango provides a website and mobile apps that allow consumers to view movie information and purchase movie tickets. Fandango's app collected sensitive information (i.e., credit card and Fandango account information) and failed to validate SSL certificates, despite representations made to consumers that such information was securely stored. As part of its settlement, Fandango must establish a comprehensive security program designed to address security risks during the development of its mobile apps.

- In the Matter of Credit Karma, Inc. Credit Karma provides a website and mobile app that allow consumers to monitor and evaluate their credit and financial status. Like Fandango, the Credit Karma mobile app failed to validate SSL certificates, overriding the defaults provided by iOS APIs, despite its representation to consumers that it protected consumer information. As part of its settlement, Credit Karma must establish a comprehensive security program designed to address security risks during the development of its mobile apps.

- FTC v. Yelp Inc. Yelp settled with the FTC for $450,000 for its alleged violations of the Children's Online Privacy Protection Act (COPPA). Yelp developed a mobile app in which it collected age information from registered users but failed to screen out users under the age of 13. As a result, Yelp had knowledge it was collecting information from children and did not comply with COPPA by, among other things, requiring prior parental consent. For more information see Pierce Atwood's client alert on this topic, *available at* http://www.pierceatwood.com/caution-your-mobile-app-may-unintentionally-violate-coppa.

Workforce Training and FTC Enforcement Examples Over the Past Several Years. As illustrated by the examples below, the FTC has also consistently cited the failure to train as a basis for violation of the FTC Act.

- PLS Financial Services, Inc.

    - Facts. *PLS Financial Services* concerned a security breach involving operators of payday loan and check cashing stores ("PLS"). *See United States v. PLS Fin. Servs., Inc.*, No. 1:12-cv-08334 (N.D. Ill. Oct. 26, 2012) (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/11/121107plspaydaycmpt.pdf. PLS collected personal information from consumers in the course of providing its services; in connection with that collection, it provided consumers with a Privacy Notice that stated, "We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your nonpublic information." Notwithstanding this statement, documents containing consumer personal information were recovered from dumpsters near various PLS stores.

    - The Case. The U.S. Department of Justice, acting on notification and authorization by the FTC, sued PLC in federal district court, alleging, among other things, that PLC engaged in deceptive trade practices when it made the representation about security in its Privacy Notice. This representation was deceptive, in part, because PLS failed to implement employee training regarding "the physical security of sensitive consumer information; [and] the proper collection, handling, and disposal of sensitive consumer information."

- HTC America, Inc.

    - Facts. This case concerned a manufacturer of mobile devices ("HTC"). *See In re HTC Am. Inc.*, FTC File No. 122 3049, No. C-4406 (F.T.C. June 25, 2013) (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2013/07/130702htccmpt.pdf. HTC developed its mobile devices for use with Google's Android operating system and often pre-loaded third party applications onto devices that it sold to consumers. In doing so, HTC undermined the Android operating system's permission-based security model, which normally sought consumer consent before giving third party applications access to sensitive personal information on the device. HTC failed, among other things, to implement alternative security procedures to replace the bypassed Android security model, leaving consumer information exposed to viruses and other malware. Notably, no specific data breach took place prior to the filing of the FTC Complaint.

- The Case. The FTC Complaint alleged, among other things, that HTC committed an "unfair" trade practice by "fail[ing] to employ reasonable and appropriate security practices in the design and customization of the software on its mobile devices." These included the "fail[ure] to implement adequate privacy and security guidance or training for its engineering staff."

- EPN, Inc.

  - Facts. EPN, a debt collection company providing services to the healthcare industry, regularly collected and stored personal health information about consumers. *See In re EPN, Inc.*, FTC File No. 112 3143, No. C-4370 (F.T.C. June 7, 2012) (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/10/121026epncmpt.pdf. The company's Chief Operating Officer installed a filesharing application on his work computer, inadvertently providing the application with access to the EPN internal network. Several files containing personal health information were inadvertently made available for download over the peer-to-peer network.

  - The Case. The FTC Complaint alleged unfair trade practices, based in part on the failure of EPN to "adequately train employees about security to prevent unauthorized disclosure of personal information."

- UPromise, Inc.

  - Facts. UPromise offers consumers rebates for college savings if they shop at its partners' web sites (partners include companies like Macy's, Mobile, and Dell). *See In re Upromise, Inc.*, FTC File No. 102 3116, No. C-4351 (F.T.C. Mar. 27, 2012) (complaint), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2012/04/120403upromisecmpt.pdf. As part of its services, UPromise provided a downloadable "toolbar" that installed onto a user's web browser and, among other things, highlighted partner web pages in search results so that users would know where to shop to take advantage of UPromise's rebates. UPromise's Privacy Statement provided that the toolbar would collect some personal information "infrequently" but that any personally identifiable information would be removed prior to transmission to UPromise. It also stated that UPromise had "implemented policies and procedures designed to safeguard [customer] information." The UPromise toolbar in fact engaged in extensive information collection about

users' browsing activities, including capturing usernames, passwords, and the contents of secure web forms, all of which information was sent to UPromise in unencrypted form over the Internet. UPromise halted all data collection using the toolbar after an employee brought it to the company's attention.

- The Case. The FTC Complaint alleged that UPromise engaged "in a number of practices that, taken together, failed to provide reasonable and appropriate security for consumer information collected and transmitted by the [toolbar]," including "fail[ing] to ensure that employees responsible for the information collection program received adequate guidance and training about security risks and [UPromise's] privacy and security policies."

Summary and Conclusion. For most companies operating in the United States, the FTC is the most important and influential regulator in the areas of privacy and information security. The FTC has consistently demonstrated the importance of 1) accurately describing and implementing reasonable privacy and data security practices; 2) ensuring all technologies, including mobile apps, are compliant; and 3) instituting a comprehensive and tailored employee training program. For a broader treatment of the FTC's influence on privacy and information security, we recommend Daniel Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 Columbia L. R. 583 (2014), available at http://bit.ly/1u0dmi9.

Note: Additional Sources of Guidance in GLBA and HIPAA. In the United States, the most developed privacy and information security frameworks are the ones created pursuant HIPAA and the Graham-Leach-Bliley Act of 1999 ("GLBA"), which regulate the health care and financial services sectors, respectively. The FTC's jurisprudence tends to be consistent with these frameworks, so HIPAA and GLBA may also provide further guidance on what the FTC would consider reasonable and adequate, even for organizations not regulated by HIPAA or GLBA. For more information on requirements under HIPAA, see the discussion of HIPAA and OCR below. For more information on requirements under GLBA, see The Safeguards Rule, 16 CFR § 314.4 and Board of Governors of the Federal Reserve System, Interagency Guidelines Establishing Information Security Standards (August 2, 2013), available at http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm#v.

III. OCR Regulatory Authority

HIPAA Generally: HIPAA requires covered entities and their business associates to protect the privacy and security of health information. 45 C.F.R. Part 160 and Part 164, subparts A, C and E. The HIPAA Privacy Rule and Security Rule are enforced by the Department of Health and Human Services, Office of Civil Rights

("OCR"). Although HIPAA does not apply as broadly as the FTC legal regime, as mentioned above, it may provide a useful framework both for entities regulated by HIPAA and those that are not.

The Privacy Rule. The Privacy Rule, issued by the Department of Health and Human Services ("HHS") to implement HIPAA requirements, regulates the use and disclosure of protected health information by covered entities. The Privacy Rules requires that covered entities develop and implement written privacy policies and procedures designed to comply with the Privacy Rule requirements. 45 CFR § 164.530(i). It also requires covered entities train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their functions. 45 C.F.R. § 164.530(b).

The Security Rule. HHS also issued the Security Rule, which establishes security standards for the protection of certain health information that is held or transferred in electronic form. The Security Rule requires covered entities implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. 45 C.F.R. § 164.306. It also requires covered entities provide for appropriate authorization and supervision of workforce members who handle electronic protected health information and provide training on its security policies and procedures. 45 C.F.R. § 164.308(a).

OCR Enforcement Powers. OCR enforces the Privacy Rule and Security Rule and has the authority to conduct investigations of complaints alleging HIPAA violations by covered entities. 45 C.F.R. §§ 160.306(c) and 160.310(b). If the information collected indicates that the covered entity is not in compliance, OCR may attempt to resolve the case by obtaining: 1) voluntary compliance; 2) corrective action; or 3) a resolution agreement. OCR may further impose civil penalties on the covered entity, which are deposited in the U.S. Treasury.

IV. HIPAA Privacy and Data Security Guidance

OCR Enforcement Action Guidance. In recent years, OCR has increased its enforcement actions, offering guidance for both regulated and non-regulated companies. The following 2014 lessons from OCR are particularly noteworthy:

- Encrypt laptops containing electronic protected health information ("ePHI");
- Implement sufficient privacy and data security policies and procedures; and
- Conduct risk assessments and make changes based on identified gaps.

Encrypt laptops with ePHI and Make Changes Based on Gaps Identified in Your Risk Assessment. Under HIPAA, notification in the event of a data breach is only required for the breach of unsecured protected health information ("unsecured PHI"). 45 CFR § 164.404(a)(1). Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology, including by encryption. 45 CFR § 164.402. As a result, breach notification obligations are triggered in the event an *unencrypted* laptop containing ePHI is stolen or lost, assuming it is not otherwise secured. As Susan McAndrew, OCR's deputy director of health information privacy stated in a recent press release, "Our message to these organizations is simple: encryption is your best defense against these incidents" *see Stolen laptops lead to important HIPAA settlements* (April 22, 2014), available at http://www.hhs.gov/news/press/2014pres/04/20140422b.html.

HIPAA also requires covered entities implement policies and procedures to prevent, detect, contain, and correct security violations, including through the use of risk analyses. 45 CFR § 164.308(a)(1). It is not enough to merely conduct a risk assessment; covered entities should also correct violations and vulnerabilities identified. The following 2014 cases are illustrative:

- QCA Health Plan, Inc. An unencrypted laptop containing the ePHI of almost 150 people was stolen from a QCA employee's car. OCR's investigation also revealed QCA did not implement sufficient security policies and procedures or physical safeguards for workstations with access to ePHI. QCA settled for $250,000 and agreed to provide a risk analysis and corresponding risk management plan, provide security and awareness training, and report to OCR, among other things.

- Concentra Health Services. After receiving a report that an unencrypted laptop was stolen from a Concentra Health Services facility, OCR's investigation revealed Concentra had conducted a risk analysis recognizing the risk posed by unencrypted laptops. Despite this risk analysis, Concentra's efforts to encrypt were incomplete and inconsistent, and Concentra had insufficient security management processes in place. Concentra settled for $1,725,220 and the adoption of a corrective action plan.

Implement Sufficient Privacy and Data Security Policies and Procedures. HIPAA requires covered entities have written policies and procedures designed to comply with HIPAA. 45 CFR § 164.530(i). Among other things, such policies and procedures must require the implementation of sufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level. 45 C.F.R. § 164.306. The following recent cases illustrate the importance of developing and implementing such policies and procedures.

- Anchorage Community Mental Health Services. OCR investigated a breach of unsecured ePHI caused by malware, affecting over 2,700 individuals at Anchorage Community Mental Health Services ("ACMHS"), a nonprofit that provides behavioral health services. Although ACMHS had adopted sample Security Rule policies in 2005, these policies were not followed. ACMHS settled for $150,000 and the adoption of a corrective action plan including the revision and distribution of policies and procedures, training, security management and reporting to OCR.

- Skagit County, Washington. An investigation by OCR revealed that the ePHI of more than 1,500 individuals was accessible on the county's public web server and Skagit County failed to provide notification of the breach to affected individuals and implement sufficient security policies, procedures and training. Skagit County settled for $215,000 and agreed to post a notification of the breach on its website, as well as update its privacy, security and breach notification policies and procedures, among other things.

Workforce Training and OCR Enforcement Examples Over the Past Several Years. As illustrated by the examples below, the OCR has also consistently incorporated workforce training as an integral part of the corrective action obligations it imposes on companies.

- Parkview Health Systems, Inc.

    - Facts. On June 10, 2009, Dr. Christine Hamilton filed a complaint against Parkview Health Systems, Inc. ("Parkview") alleging violation of the Privacy Rule. *See Parkview Health System, Inc.*, Dept. of Health & Human Services Office for Civil Rights (Resolution Agreement), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/hhs-parkview-resolution-cap.pdf. An investigation conducted by OCR indicated that Parkview received thousands of Dr. Hamilton's patients' records and its employees left 71 cardboard boxes containing such medical records on Dr. Hamilton's driveway, unattended and accessible to unauthorized persons.

    - Corrective Action Training Obligations. Parkview was required to comply with the Privacy Rule and provide general safeguards training to all workforce members who have access to protected health information. OCR further required all training materials be submitted to OCR for its approval, and each member required to attend the training was required to certify such training was received. OCR also specified that all training materials must be reviewed periodically and updated to reflect any changes in

Parkview's policies and procedures, federal law, OCR guidance, and/or any material compliance issues discovered during audits and reviews. One year after OCR has approved the training materials, Parkview is also required to submit a Final Report, including a copy of all training materials used and a written description of the training, including a summary of the topics covered, the length of the session(s), and a schedule of when the training session(s) were held and/or the days during which on-line training was provided.

- Alaska Department of Health and Social Services ("DHSS").

  - Facts. A portable electronic storage device, potentially containing electronic protected health information, was stolen from a DHSS computer technician's vehicle. *See Alaska Dept. of Health and Human Services*, Dept. of Health & Human Services Office for Civil Rights (Resolution Agreement), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/alaska-agreement.pdf. OCR investigated and found DHSS had not, among other things, completed security training for DHSS workforce members as required by HIPAA.

  - Corrective Action Training Obligations. OCR required DHSS provide both general Security Rule training and specific training related to the new policies and procedures required under the same corrective action obligations. The training had to be reviewed annually, and where appropriate, DHSS was required to update the training to reflect changes to the law, OCR guidance, any issues discovered during audits or reviews, and any other relevant developments. No workforce members were allowed to use or access protected health information unless they had certified that they had received the required training. The Final Report to OCR required, among other things, a copy of all training materials, a description of the training, including a summary of the topics covered, the length of the session(s) and a schedule of when the training session(s) were held.

- Providence Health & Services ("PH&S").

  - Facts. Four backup tapes and two optical disks containing unencrypted electronic protected health information were stolen from the care of a PH&S employee. *See Providence Health & Services*, Dept. of Health & Human Services Office for Civil Rights (Resolution Agreement), *available at* http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/agreement.pdf. Subsequently, several laptops containing unencrypted

electronic protected health information were left unattended and were stolen from workforce members.

- Corrective Action Training Obligations. PH&S was required to provide training to all workforce members on the updated policies and procedures required under the corrective action obligations. Training attendees further had to certify they attended the training and provide the date of the training. PH&S was also required to annually review the training and update it to reflect any changes in federal law, OCR guidance or any issue(s) discovered during audits or reviews. OCR required PH&S submit an implementation report within 120 days of approval for its policies and procedures, including a copy of all training materials used for the training, a description of the training, including a summary of the topics covered, the length of the session(s), and a schedule of when the training session(s) were held.

Conclusion

There is no one-size-fits-all approach to privacy and data security but there are some common mistakes from which to learn. The FTC and OCR enforcement actions discussed above provide some guidance and should be used as a starting point for companies striving to adopt and implement reasonable privacy and data security practices.

Appendix A: Example FTC Civil Investigative Demand

*This Appendix contains a recent example Civil Investigative Demand (in redacted form) issued by the Federal Trade Commission in the aftermath of a data breach incident. Among other things, it is instructive of what the FTC may expect to see in an information security program. S*ee *Civil Investigative Demand §§ III(A)(8)(d), (e), (f);* id. *§ III(B)(3)(f).*

CIVIL INVESTIGATIVE DEMAND
SCHEDULE FOR DOCUMENTS AND ANSWERS TO
WRITTEN INTERROGATORIES

I. DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

A. **"And,"** as well as "or," shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in this Schedule all information that otherwise might be construed to be outside the scope of the specification.

B. **"Any"** shall be construed to include **"all,"** and **"all"** shall be construed to include the word **"any."**

C. **"Breach Incident"** shall mean the incident that resulted in the Company sending data breach notification letters to consumers in _____.

D. **"CID"** shall mean the Civil Investigative Demand, including the attached Resolution and this Schedule, and including the Definitions, Instructions, and Specifications.

E. **"Company"** shall mean [Company]**,** its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

F. **"Document"** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book or label. **"Document" shall also include Electronically Stored Information.**

G. **"Each"** shall be construed to include "every," and "every" shall be construed to include **"each."**

H. **"Electronically Stored Information" or "ESI"** shall mean the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any information created, manipulated, communicated, stored, or utilized in digital form, requiring the use of computer hardware or software. This includes, but is not limited to, electronic mail, instant messaging, videoconferencing, and other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and video and sound recordings, whether stored on: cards; magnetic or electronic tapes; disks; computer hard drives, network shares or servers, or other drives; cloud-based platforms; cell phones, PDAs, computer tablets, or other mobile devices; or other storage media. "ESI" also includes such technical assistance or instructions as will enable conversion of such ESI into a reasonably usable form.

I. **"FTC"** or **"Commission"** shall mean the Federal Trade Commission.

J. **"Identity"** or **"the identity of"** shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable.

K. **"Unnamed Service Provider"** shall mean the unnamed service provider referenced in the Company's _____, breach incident press release.

L. **"Information Security Program"** shall mean the Company's procedures to protect personal information.

M. **"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 consumer's email address); (d) a telephone number; (e) a Social Security number; (f) checking account information, credit card information, or debit card information (such as account or card numbers); (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, (h) smart grid data and/or utility usage/consumption pattern data; or any information from or about an individual consumer that is combined with any of (a) through (h) above.

N. **"Referring to"** or **"relating to"** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

O. **"Service Provider"** shall mean any third party that receives, maintains, processes, or otherwise is permitted access to personal information in the course of providing services to the Company.

P. **"You"** and **"your"** shall mean the person or entity to whom this CID is issued and includes the "Company".

II. INSTRUCTIONS

A. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11 (c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. **Meet and Confer:** You must contact **[Name]** at **[Telephone #]** as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your response, including but not limited to a discussion of the submission of Electronically Stored Information and other electronic productions as described in these Instructions.

C. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the request shall be from **[Date] until the date of full and complete compliance with this CID.**

D. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;

2. the names, addresses, positions, and organizations of all authors and recipients of the item; and

3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8 A(b).

E. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. §§ 1505,1519.

F. **Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later man twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

G. **Modification of Specifications:** If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with **[Name]** at **[Telephone #].** All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

H. **Certification:** A responsible corporate officer or a duly authorized manager of the Company shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

I. **Scope of Search:** This CID covers documents and information in your possession or under your actual or constructive custody or control including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, directors, officers, employees, and other agents and consultants, whether or not such documents and information were received from or disseminated to any person or entity.

J. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Federal Trade Commission, Division of Privacy and Identity Protection, 601 New Jersey Avenue, NW, Mail Stop NJ-8122, Washington, DC 20001. Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS. Notice of your intended method of production shall be given by mail or telephone **[Name]** at **[Telephone #]** at least five days prior to the return date.

K. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the documents) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files or as electronically stored and without being manipulated or otherwise rearranged; if documents are removed from their original folders, binders, covers, containers, or electronic source in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, container, or electronic media or file paths from which such documents came. In addition, number by page (or file, for those documents produced in native electronic format) all documents in your submission, preferably with a unique Bates identifier, and indicate the total number of documents in your submission.

L. **Production of Copies:** Unless otherwise stated, legible photocopies (or electronically rendered images or digital copies of native electronic files) may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of originals may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request Copies of marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

M. **Electronic Submission of Documents:** The following guidelines refer to the production of any Electronically Stored Information ("ESI") or digitally imaged hard copy documents. Before submitting any electronic production, you must confirm with the Commission counsel named above that the proposed formats and media types will be acceptable to the Commission. The FTC requests Concordance load-ready electronic productions, including DAT and OPT load files.

1. **Electronically Stored Information:** Documents created, utilized, or maintained in electronic format in the ordinary course of business should be delivered to the FTC as follows:

    a. Spreadsheet and presentation programs, including but not limited to Microsoft Access, SQL, and other databases, as well as Microsoft Excel and PowerPoint files, must be produced in native format with extracted text and metadata. Data compilations in

Excel spreadsheets, or in delimited text formats, must contain all underlying data un-redacted with all underlying formulas and algorithms intact. All database productions (including structured data document systems) must include a database schema that defines the tables, fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements, including the use of any report writers and custom user data interfaces;

b. All ESI other than those documents described in (1)(a) above must be provided in native electronic format with extracted text or Optical Character Recognition (OCR) and all related metadata, and with corresponding image renderings as converted to Group IV, 300 DPI, single-page Tagged Image File Format (TIFF) or as color JPEG images (where color is necessary to interpret the contents);

c. Each electronic file should be assigned a unique document identifier ("DocID") or Bates reference.

2. **Hard Copy Documents:** Documents stored in hard copy in the ordinary course of business should be submitted in an electronic format when at all possible. These documents should be true, correct, and complete copies of the original documents as converted to TIFF (or color JPEG) images with corresponding document-level OCR text. Such a production is subject to the following requirements:

a. Each page shall be endorsed with a document identification number (which can be a Bates number or a document control number); and

b. Logical document determination should be clearly rendered in the accompanying load file and should correspond to that of the original document; and

c. Documents shall be produced in color where necessary to interpret them or render them intelligible;

3. For each document electronically submitted to the FTC, you should include the following metadata fields in a standard ASCII delimited Concordance DAT file:

a. **For electronic mail:** begin Bates or unique document identification number ("DocID"), end Bates or DocID, mail folder path (location of email in personal folders, subfolders, deleted or sent items), custodian, from, to, cc, bcc, subject, date and time sent, date and time received, and complete attachment identification, including the Bates or DocID of the attachments (AttachlDs) delimited by a semicolon, MD5 or SHA Hash value, and link to native file;

b. **For email attachments:** begin Bates or DocID, end Bates or DocID, parent email ID (Bates or DocID), page count, custodian, source location/file path, file name, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;

c. **For loose** electronic **documents (as retrieved directly from network file stores, hard drives,** etc.): begin Bates or DocID, end Bates or DocID, page count, custodian, source media, file path, filename, file extension, file size, author, date and time created, date and time modified, date and time printed, MD5 or SHA Hash value, and link to native file;

d. **For imaged hard copy documents:** begin Bates or DocID, end Bates or DocID, page count, source, and custodian; and where applicable, file folder name, binder name, attachment range, or other such references, as necessary to understand the context of the document as maintained in the ordinary course of business.

4. If you intend to utilize any de-duplication or email threading software or services when collecting or reviewing information that is stored in your computer systems or electronic storage media, or if your computer systems contain or utilize such software, you must contact the Commission counsel named above to determine whether and in what manner you may use such software or services when producing materials in response to this Request.

5. Submit electronic productions as follows:

a. With passwords or other document-level encryption removed or otherwise provided to the FTC;

b. As uncompressed electronic volumes on size-appropriate, Windows-compatible, media;

c. All electronic media shall be scanned for and free of viruses:

d. Data encryption tools may be employed to protect privileged or other personal or private information. The FTC accepts TrueCrypt, PGP, and SecureZip encrypted media. The passwords should be provided in advance of delivery, under separate cover. Alternate means of encryption should be discussed and approved by the FTC.

e. Please mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:

MAGNETIC MEDIA - DO NOT X-RAY MAY BE OPENED FOR POSTAL INSPECTION.

6. All electronic files and images shall be accompanied by a production transmittal letter which includes:

a. A summary of the number of records and all underlying images, emails, and associated attachments, native files, and databases in the production; and

b. An index that identifies the corresponding consecutive document identification numbers) used to identify each person's documents and, if submitted in paper form, the box number containing such documents. If the index exists as a computer file(s), provide the index both as a printed hard copy and in machine-readable form (provided that the Commission counsel named above determines prior to submission that the machine-readable form would be in a format that allows the agency to use the computer files). The Commission counsel named above will provide a sample index upon request.

A Bureau of Consumer Protection Production Guide is available upon request from the Commission **counsel named above. This guide provides detailed directions on how to fully comply with this instruction.**

N. **Predictive Coding:** If the company or its agent uses or intends to use software or technology to identify or eliminate potentially responsive documents and information produced in response to this Request, including but not limited to search terms, predictive coding, near-deduplication, deduplication, and email threading, the company must provide a detailed description of the method(s) used to conduct all or any part of the search. If search terms will be used, in whole or in part, to identify documents and information that are responsive to this Request, provide the following: (1) a list of the proposed search terms; (2) a word dictionary or tally list of all the terms that appear in the collection and the frequency with which the terms appear in the collection (both the total number of appearances and the number of documents in which each word appears); (3) a glossary of industry and company terminology (including any code words related to the subject matter of the CID); (4) a description of the search methodology (including the planned use of stem searches and combination (or Boolean) searches); and (5) a description of the applications that will be used to execute the search. The Commission strongly recommends that the company provide these items prior to conducting its collection of potentially responsive information and consult with the Commission to avoid omissions that would cause the company's response to be deemed deficient.

O. **Sensitive Personally Identifiable Information:** If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please redact the sensitive information or, if redaction is not appropriate, contact us to discuss encrypting any electronic copies of such material with encryption software such as SecureZip and provide the encryption key in a separate communication.

For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth, Social Security number, driver's license number or other state identification number, or a foreign country equivalent, passport number, financial account number, credit card number, or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

P. **Information Identification:** Each specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specification^) or subspecification(s) to which it is responsive.

Q. **Certification of Records of Regularly Conducted Activity:** Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

III. SPECIFICATIONS

A. Interrogatories

Corporate Information

1. State the Company's complete legal name and all other names under which it has done business, its corporate mailing address, all addresses from which it does or has done business, and the dates and states of its incorporation.

2. Describe the Company's corporate structure and state the names of all parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which it exercises supervision or control. For each such entity, describe the nature of its relationship to the Company.

3. State the Company's total number of employees, annual revenues, annual number of customers, and locations of such customers by state.

4. Briefly describe each type of product and service provided by the Company and state whether personal information is collected or maintained in connection with each such product and service.

Information and Business Practices

5. State each type of personal information from or about consumers that is or has been collected or maintained by or for the Company.

6. For each type of personal information described in response to Interrogatory

   a. indicate all sources from which the Company has obtained personal information;

   b. describe how the Company has used, maintained, and stored each type of information;

   c. describe the flow path of personal information over the Company's computer network, including the initial collection point for personal information (such as a website), the entry and exit points to and from the network, and all intermediate points within the network; and

   d. indicate whether the Company maintains (or has maintained) database(s) of personal information, and if so, name each database, describe the specific types of information contained in the database(s), the

format in which the information is maintained, and how the Company uses the information contained in each database.

7. For each type of information described in response to Interrogatory 5, state whether, when, and under what circumstances such information is or was made available to service providers.

Information Security

8. Describe the Company's information security program, including but not limited to the following:

   a. any physical or electronic security measures taken to protect personal information, including but not limited to practices to monitor and record unauthorized access (such as intrusion detection systems, password requirements, employee turnover procedures, service provider contracts and/or turnover procedures, procedures for transporting personal information, and log retention policies);

   b. the means by which the Company's computer network may be accessed externally describing the Company's Virtual Private Network ("VPN") protocol and VPN authentication method;

   c. any written policies, practices or procedures that relate to the privacy, security, and confidentiality of personal information and the dates such policies, practices, and procedures were implemented or materially revised;

   d. the title and job description of employees that receive training related to employees' obligations to protect the security and confidentiality of personal information, describing the training the Company provides, including the name(s) and titles of all person(s) who provide this training, and stating the times at which employees receive such training (e.g., annually, as-needed);

   e. whether the Company has provided training to service providers regarding obligations to protect the security and confidentiality of personal information, describing any such training, including the name(s) and titles of all person(s) who provide this training, and stating the times at which service providers receive such training (e.g., annually, as-needed);

   f. the means by which the Company's information security program measures and written policies, practices and procedures are (i) communicated to employees and (ii) made mandatory for employees;

g. the means by which the Company's information security program measures and written policies, practices and procedures are or have been (i) communicated to service providers and (ii) made mandatory for service providers;

h. any assessments undertaken to ascertain the risks to the security and confidentiality of personal information, including the dates and results of any such assessments, and the name(s) and title(s) of the person(s) responsible for conducting the assessment(s);

i. any completed testing, monitoring, or evaluation of the Company's information security program ("program testing"), including the dates on which each such program testing occurred; and

j. any plans and procedures for future testing, monitoring, or evaluation of the program.

9. Describe how you have reviewed, evaluated, or otherwise monitored the effectiveness of and compliance with the information security program described in your response to Interrogatory 8, setting forth specifically any changes made to your information security program during the applicable time period, with an explanation for the bases for any changes or modifications made.

10. Identify all persons responsible for creating, developing, approving, implementing, overseeing, and ensuring compliance with the policies, practices, and procedures described in your response to Interrogatory 8. For each such person, indicate the dates of the person's employment or affiliation with the Company, all title(s) or position(s) held at the Company, and whether the person is currently employed by the Company.

Service Providers

11. Describe the Company's policies, practices, and procedures relating to its screening, selection, and approval of service providers who will have access to personal information.

12. Identify each service provider to whom the Company has furnished personal information from or about consumers and explain how the service provider has obtained such information.

13. For each service provider that has received, maintained, processed, or otherwise been permitted access to personal information in the course of providing services to you:

a. provide a narrative that explains in detail the duties, scope, and responsibilities of the service provider; the term of the service provider's

relationship with the Company, and the business reasons for the service provider's access to such information;

b. describe the types and location within your databases and/or computer system(s) of personal information to which the service provider has or had access;

c. describe the form and manner of such access (such as physical access to your office or remote access to your computer system(s);

d. describe what if any steps the Company has taken to ensure that service providers protect personal information from misuse or unauthorized access or disclosure.

Breach Incident

14. Describe in detail the breach incident, setting forth specifically:

a. the facts and circumstances surrounding the incident, including how and when the Company learned of the breach and how it determined the cause, location(s), and extent of the breach;

b. actions involving information technology personnel or resources to determine the cause, location(s), and extent of the breach;

c. whether the breach incident is limited to personal information of a certain State, and if not, indicate the other States;

d. the number and location by State of consumers whose personal information was subject to the breach incident;

e. any forensic analysis, evaluation, or reporting conducted by the Company or on its behalf;

f. how you monitored the service provider to confirm that it had implemented and maintained security safeguards adequate to protect the confidentiality and integrity of personal information; and

g. whether and how the Company has changed its information security program in response to the breach, or if it has plans to do so.

15. Identify the Unnamed Service Provider described in your _____ _____ press release and describe with specificity what this entity was contracted by you to do. Your response should include but not be limited to:

a. all duties and responsibilities assigned to the Unnamed Service Provider by the Company;

b. the size of the contract (e.g. dollar value, tenure, labor hours, number of workers);

c. the business reasons the service provider had access to personal information; and

d. each type of personal information to which the service provider was permitted access.

16. State how many individuals participated in the unauthorized access related to the breach incident and for each such individual, provide his/her name, title, job category, and relation to the service provider or the Company.

17. Describe the effect of the breach incident on the Company's revenue and expenses, including an itemization of the actual cost of each change made to the Company's information security program.

18. Describe the Company's efforts to identify and assist consumers whose information was or may have been obtained without authorization through the breach incident.

19. Describe in detail the Company's policies, practices, and procedures relating to the retention, storage, deletion, and archiving of electronic data, including e-mail.

20. If, for any request, there are documents that would be responsive to this CID, but they were destroyed, mislaid, transferred, deleted, altered, or over-written, describe the date and circumstances of any such event.

B. Document Requests

1. Provide copies of all claims, representations, and statements made to consumers by or for the Company regarding your collection, disclosure, use, storage, destruction, and protection of personal information, including any claims, representations or statements relating to the security of personal information, indicating for each such claim, representation, or statement, the date(s) when it was made and all means by which it was distributed.

2. Provide exemplars of all materially different enrollment or promotional materials relating to the products and services described in response to Interrogatory 4 in which personal information is collected or maintained.

3. Provide documents sufficient to describe the Company's information security program, including but not limited to the following:

a. any physical or electronic information security measures taken to protect personal information, including but not limited to building or office alarm systems, all practices to control, monitor and record access to personal information, including practices to monitor and record unauthorized access (such as intrusion detection systems), password requirements, employee turnover procedures, service provider turnover procedures, procedures for transporting personal information, and log retention policies;

b. the means by which the Company's computer network(s) may be accessed externally, including the Company's VPN protocol and VPN authentication method;

c. the technical configurations of devices and programs the Company has used to implement its information security program, including but not limited to configurations of firewalls or other means used to control, monitor, and record access to personal information;

d. any assessments undertaken by the Company to ascertain the risks to the security and confidentiality of personal information, including the results of any such assessments and how your information security program addresses each identified risk;

e. any completed or planned testing, monitoring, or evaluation of the Company's information security program ("program testing") including documents that describe and explain in detail: the manner in which the Company or another person or entity tests, monitors, and/or evaluates the effectiveness of and compliance with the information security program; when testing, monitoring, and/or evaluations were conducted and completed; plans and procedures for future testing, monitoring, and/or evaluation of the information security program; findings, reports, and recommendations resulting from such program testing; whether and when the Company adopted or implemented any such recommendations, and changes made to your information security program as a result of program testing; and

f. information security training and the dates such training was provided to network users (such as employees and service providers), including the dates of such training and any materially different versions of such documents.

4. Provide documents sufficient to identify by name, location, and operating system each computer network the Company uses to collect and store personal information. For each such network provide:

a. a high-level diagram(s) that set out the components of the network. The diagram(s) should indicate and locate (within the network) computers; servers; firewalls; routers; internet, private line, and other connections;

connections to other internal and external networks; virtual private networks; remote access equipment (such as wireless access points); websites; and security mechanisms and devices (such as intrusion detection systems). Your response may include blueprints and diagrams that set out the components, topology, and architecture of the network;

b. documents sufficient to describe (i) each computer, server, or other device used to collect and store personal information, and (ii) for each computer, server, or device described in response to subsection (b)(i), each program, application, or other means (collectively, "databases") used to collect and store personal information; and

c. documents sufficient to describe the type and source of personal information stored or maintained in each database described in response to Document Request 4(b), and the records of the number of consumers whose information is contained in the database.

5. For each service provider identified in the response to Interrogatory 12, provide:

a. documents sufficient to describe the types of personal information to which the service provider has or had access;

b. documents sufficient to describe the manner of the service provider's access to personal information (such as physical access to paper documents in the Company's offices or remote access to its computer network(s);

c. copies of all contracts and policies, procedures, or practices that relate to each service provider's handling of personal information;

d. documents that describe any measures the Company took to select and retain the service provider to ensure that it is capable of appropriately protecting personal information the Company has provided or made available to the service provider; and

e. documents that describe how the Company has monitored the service provider to confirm that it has implemented and maintained security measures adequate to protect the security, integrity, and confidentiality of personal information, including documents sufficient to show how and when such requirements are communicated and to which service providers.

To the extent that responsive documents are the same for different service providers, provide a set of responsive documents and identify the individual service providers for which the documents are responsive.

6. Provide all documents relating to the breach incident, including documents regarding:

   a. the facts and circumstances surrounding the breach incident, including: how the Company learned of the breach incident, where and when it began, the time period over which it occurred, the points of entry, the path(s) the intruders) likely followed from the point of entry to the personal information that was or may have been accessed through final exporting or downloading of the information (including all intermediate steps), and indicating the type(s), locations, and amounts(s) of information that may have been accessed without proper authorization;

   b. the Company's communications with law enforcement regarding the breach incident;

   c. each action the Company has taken in response to the breach incident;

   d. the number of consumers whose information was or may have been accessed without authorization as a result of the breach incident and their geographic location by state; and

   e. any consumer complaints or inquiries regarding the breach incident.

   Responsive documents relating to the breach incident should include, but not be limited to: interim and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in the breach; penetration tests; gap analyses; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, websites, and network components used in providing services (such as whether an application was misconfigured); reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of the breach prepared internally and/or by third-parties; documents that describe in detail how affected websites, databases, or systems were identified and were or may have been exploited; and other records relating or referring to the breach, including minutes or notes of meetings attended by Company personnel and documents that identify the intruders).

   Provide copies of all documents relating to information security practices that the Company provided to the Unnamed Service Provider and the dates such documents were provided. This response should include but not be limited to all contracts between the Unnamed Service Provider and the Company.

9. Provide documents sufficient to describe any investigations of or complaints filed with or against, or communicated to, the Company regarding the privacy, security, and confidentiality of personal information, including any documents filed with Federal, State, foreign or local government agencies, including the United States Congress, Federal or State courts, and Better Business Bureaus.

10. Submit documents sufficient to show the Company's policies, practices, and procedures described in your response to Interrogatory 19 relating to the retention, storage, deletion, and archiving of electronic data, including e-mail.

11. Provide all other documents described in your response to any Interrogatory that have not been specifically requested in Document Requests 1-10, indicating, for each document produced, the Interrogatory response(s) in which the document is described.

CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY
Pursuant to 28 U.S.C. § 1746

1. **I,** _____, have personal knowledge of the facts set forth below and am competent to testify as follows:

2. I have authority to certify the authenticity of the records produced by [Company] and attached hereto.

3. The documents produced and attached hereto by [Company] are originals or true copies of records of regularly conducted activity that:

a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

b) Were kept in the course of the regularly conducted activity of [Company]**;** and

c) Were made by the regularly conducted activity as a regular practice of [Company]**.**

I certify under penalty of perjury that the foregoing is true and correct.

Executed on _____

_____
Signature