Cybersecurity Law Report
An Acuris company

cslawreport.com

January 8, 2020

FTC ENFORCEMENT

Eight Data Security Best Practices Revealed by Recent AG and FTC Enforcement Actions

By Ann-Marie Luciano and Jawaria Gilani, *Cozen O'Connor*

Although there is no standard set of measures that a company can implement to guarantee that it will be safe from data breaches – or from regulatory enforcement action should a data breach occur – recent multistate settlements with state Attorneys General (AGs) and the FTC provide valuable insight into what regulators view as reasonable and sufficient data security practices and illustrate practical steps that companies can take to reduce the likelihood of a data breach.

This article focuses on eight common requirements in recent AG and FTC settlements falling into three overall categories: (1) access control; (2) threat awareness; and (3) advanced technical security measures.

See "How Facebook's $5-Billion FTC Settlement Is Shaping Compliance Expectations" (Aug. 7, 2019).

The Role of FTC Guidance, Settlements and the Courts

Start With Security

Recent settlements typically include provisions requiring security measures similar to those discussed in the FTC's June 2015 guide, Start with Security: A Guide for Business, in which the FTC shared best-practice advice to help companies better secure their data. The guide, which drew on more than 50 data security enforcement actions by the FTC, notes that "learning about alleged lapses that led to law enforcement can help your company improve its practices." The guide provides ten recommendations, which continue to underlie recent requirements imposed by AGs and the FTC, such as access control, authentication, network segmentation and vulnerability detection.

See "FTC Launches Stick With Security Series, Adding Detail and Guidance to Its Start With Security Guide (Part One of Two)" (Sep. 13, 2017); Part Two (Oct. 11, 2017).

Judicial Scrutiny

Following the Eleventh Circuit's decision in *LabMD, Inc. v. FTC*, which held that the lack of specificity in the FTC's cease-and-desist orders to LabMD for the creation and implementation of data security protective measures made them unenforceable, the FTC has entered into subsequent settlements that require more specific security practices, several of which are discussed below. Notably, the Eleventh Circuit recently ordered the FTC to pay LabMD for the attorney's fees and expenses accrued during its litigation with the FTC.

Prescriptive Settlements

In July 2019, Facebook entered into a Stipulated Order with the FTC following a lawsuit alleging that the company violated the FTC Act by making deceptive claims regarding users' control over the privacy of their personal information.

Although there was no data breach, the Stipulated Order (which has not yet been approved or signed by the court) contained several requirements related to securing the personal data on Facebook's network, such as: (1) establishing and maintaining a comprehensive data security program; (2) documenting incidents when data of 500 or more users has been compromised and the efforts to address such incidents; (3) conducting a privacy review of every new and modified product, service or practice before its implementation (and documentation of the decisions made about privacy); and (4) exercising greater oversight over third-party applications.

In addition to mandating adherence to common industry standards, such as the Payment Card Industry Data Security Standard (PCI DSS) for companies handling payment card information and the Health Insurance Portability and Accountability Act (HIPAA) for companies handling health information, recent AG and FTC settlements require defendant companies to undertake a number of additional specific data security measures and practices. While there is variation among the settlements due to a number of factors, including: the nature of the organization suffering the data breach; the type of data breached; and the technical details of the breach's origins, there are common requirements.

Access Control

Limiting access to networks with sensitive information can reduce the risk of data-related incidents. Recent settlements stress proper access control measures, such as strengthening the security requirements for accessing sensitive information in the first instance and limiting the scope of access.

1) Security Requirements to Access Sensitive Information

Recent settlements require that companies institute increasingly stringent access control procedures. In addition to requiring strong passwords and password rotation policies, these procedures include:

- Two-factor (2FA) or multi-factor authentication (MFA) ("authentication through verification of at least two of the following authentication factors: (i) knowledge factors, such as a password; or (ii) possession factors, such [as] a token or text message on a mobile phone; or (iii) inherence factors, such as a biometric characteristic");
- The use of password vaults (software programs that keep a number of passwords in a secure and encrypted digital location and provide a single password to access multiple passwords) or encryption, especially for administrative-level passwords; and
- Hashing (*i.e.*, scrambling) passwords stored online using a hashing algorithm that is not vulnerable to a collision attack (a hacking attack that seeks to find two inputs producing the same hash value to "unscramble" the hashing), together with an appropriate salting policy (*i.e.*, adding

additional values at the end of the hashed password in order to make it even more secure from a collision attack).

The stringency of the security measures required often correlates with the sensitivity of the information being protected. For example, the July 2019 Consent Decree 50 AGs reached with Equifax Inc., where hackers allegedly stole names, home addresses, dates of birth, Social Security numbers and driver's license numbers through an unpatched known vulnerability, required Equifax to implement all of the above-referenced safeguards on password-protected accounts.

By contrast, a September 2018 Consent Decree between 51 AGs and Uber, where it was alleged that certain Uber drivers' names and driver's license numbers were inappropriately accessed by individuals outside of the company, mandated strong, unique password requirements and MFA or equivalent levels of protection through other methods such as single sign-on, appropriate account lockout thresholds and access logs.

Some settlements also impose restrictions on access from personal devices. Under the terms of the July 2019 Final Judgment and Permanent Injunction reached by 30 AGs with Premera Blue Cross (Premera Judgement), following a data breach in which a hacker allegedly was able to breach the health insurer's network and access sensitive personal information of millions of its members, Premera agreed to restrict access to its network via personal devices to only the data, systems and other network resources required for the individual's job, which must be accessed through a secured connection using a virtual private network and MFA or other security safeguards.

See "The Growing Role of State AGs in Privacy Enforcement" (Nov. 28, 2018).

2) Limiting Scope of Access

Several recent settlements mandate that companies restrict sensitive data access to those for whom access is necessary and appropriate and that they regularly review users' access privileges.

Under the terms of the Premera Judgement, Premera was required to restrict access to personal, health and medical information "based on necessity and job function" and regularly review whether access privileges remain appropriate.

In a June 2019 Consent Order between the FTC and LightYear Dealer Technologies, LLC, d/b/a Dealerbuilt (LightYear), where an employee allegedly attached an unauthorized storage device to the company's backup network that contained consumers' personal information, LightYear was obligated to limit "employee access to what is needed to perform that employee's job function."

Threat Awareness

An organization's threat awareness must encompass many levels – from network monitoring to detect data breach attempts in near real time to training employees to understand both the importance of data security and the proper steps they must take to protect the data entrusted to them. Recent AG and FTC settlements include multiple measures designed to address alleged deficiencies in a company's awareness of threats.

3) Frequent Network Monitoring and Logging

To minimize the delay between data breach and detection, many settlements require frequent scanning and monitoring for threats, with some requiring near real-time monitoring.

After Neiman Marcus Group, LLC experienced a breach of customer payment card data that was allegedly stolen through malware installation, a January 2019 AVC with 43 AGs required Neiman Marcus to maintain a system to collect, monitor and log network activity and to monitor the logs in near real-time (or use a security information and event management tool properly configured to report anomalous activity).

The Equifax Consent Decree similarly required Equifax to implement measures to provide near real-time notification of unauthorized modifications to its network, as well as to establish a threat management program that uses automated tools to continuously monitor its network for active threats, which were required to be monitored daily.

The FTC's Consent Order with LightYear also required it to implement technical measures to monitor all its networks and systems in order to identify data security events, and the FTC's November 2019 Proposed Consent Order with InfoTrax Systems, L.C., where it was alleged that the company failed to take reasonable measures to secure consumers' data, required InfoTrax to implement measures to detect and address anomalous activity, including an intrusion prevention or detection system, file integrity-monitoring tools and data-loss-prevention tools.

FTC settlements also have included requirements for monitoring the sufficiency of security safeguards. For example, a Consent Order with ClixSense.com, arising out of hackers allegedly gaining access to users' personal information, including Social Security numbers, required ClixSense to assess the sufficiency of its installed safeguards at least once every 12 months or after an attempted data breach, including the measures taken to prevent, detect and respond to attacks, intrusions and system failures. Similar requirements were also included in an April 2019 Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief with Unixiz, Inc. d/b/a i-Dressup.com (i-Dressup), relating to i-Dressup's alleged violation of the Children's Online Privacy Protection Act by failing to secure the personal information it had collected.

See "Far-Reaching Google and YouTube Settlement Offers COPPA Compliance Lessons" (Sep. 18, 2019).

4) Penetration Tests

Increasingly, settlements mandate the identification of network vulnerabilities through periodic penetration tests, also referred to as ethical hacking. For example, Equifax, as part of its Consent Decree, was required to implement and maintain a penetration testing program for its network that included at least one annual penetration test of all externally facing applications and at least one weekly vulnerability scan – a process of inventorying network elements, such as terminals and servers, then identifying publicly reported vulnerabilities for these elements—of all systems within the network.

5) Training of Employees and Agents Regarding the Safeguarding of Personal Information

Recognizing that human error often contributes to data breaches and that proper education and training could reduce data security-related risks, recent settlements frequently mandate training employees and agents regarding proper data security hygiene practices.

For example, the Premera Judgement required the company to provide training on safeguarding and protecting sensitive information to all employees who handle such information with responsibility for any aspects of its security. In addition, Premera was required to provide its designated privacy official with the appropriate training to be able to implement and ensure compliance with HIPAA.

Equifax's Consent Decree included a requirement that on an at least annual basis, the company provide training on safeguarding and protecting personal information to its employees that handle such information with responsibility for its safety. In addition, Equifax is to provide specialized training on safeguarding and protecting consumer personal information to employees responsible for the security of that information.

Similarly, under the terms of its Consent Decree, Uber agreed to train employees and temporary, contract and contingent workers concerning the proper handling and protection of sensitive information, including the safeguarding of passwords and security credentials, and develop and implement an annual training program for employees regarding Uber's code of conduct.

See the CSLR's three-part guide to cybersecurity training; "Program Hallmarks and Whom to Train" (Oct. 16, 2019); "What to Cover and Implementation Strategies" (Oct. 23, 2019); and "Assessing Effectiveness and Avoiding Pitfalls" (Oct. 30, 2019).

Advanced Technical Security Measures

6) Network Segmentation

Settlements often require segmentation of an organization's network to separate those sections in which sensitive information is collected, processed, stored or accessed from other sections of the network. In order to perform appropriate segmentation, companies must periodically scan and map their networks to understand where sensitive data is handled and the avenues of traffic that provide access to the sensitive information.

Recent settlements have been clear about a company's responsibility to reduce the amount of communication between the segments that handle sensitive data and the rest of the network. For example, the Equifax Consent Decree required protocols and policies that "at a minimum, ensure that systems communicate with each other in a secure manner and only to the extent necessary to perform their business and/or operational functions." The Consent Decree also required the regular performance of a full asset inventory on all components of Equifax's network to identify the asset's criticality rating, whether the asset handles sensitive information and any security updates or patches applied to the asset, among other things.

Similarly, the Premera Judgment required Premera to implement and maintain segmentation protocols and policies that are reasonably designed to properly segment the company's network and to regularly evaluate and, if needed, restrict and disable any unnecessary ports of service on its network.

7) Timely Patching

Settlements often require measures to expeditiously patch – apply a change in software code to fix an error or a vulnerability that could be exploited by hackers – and upgrade networks to make them less vulnerable to newly discovered threats. In the Equifax Consent Decree, the AGs alleged that Equifax failed to fully patch its systems, despite knowledge regarding a critical vulnerability in its software. Under the terms of the settlement, Equifax agreed to ensure the appropriate and timely application of all security patches and to maintain a tool that included an automated common vulnerabilities and exposures (CVE) feed.

Specifically, the Consent Decree required Equifax to:

- maintain a patch-management solution to manage software patches;
- rate all patches and/or updates according to their criticality and, no later than within 48 hours of rating a security update or patch as critical, either apply the update or patch or take the identified application offline until it could be successfully updated or patched;
- keep detailed records with respect to each critical security update or patch, including logging the date that each patch or update was applied, the assets to which it was applied, and whether it was applied successfully;
- appoint a "Patch Supervisor" to lead a "Patch Management Group" of other individuals responsible for regularly reviewing and maintaining the patching requirements set forth in the Consent Decree; and
- on at least a biannual basis, perform an internal assessment of the company's management and implementation of security updates and patches.

The Premera Judgment also contained provisions related to patching. Specifically, Premera was required to maintain patch management software on its network as well as conduct an asset inventory for all assets that identifies the dates that patches are applied.

8) Encryption

The continuing need to implement rigorous encryption measures has been a component of many recent AG and FTC settlements. Recent settlements have required encryption of sensitive data both when such data is being stored and when it is being transmitted over a network. For example, Uber was required to use encryption when personal information resides in backup databases that are stored on a third-party cloud-based service or platform, either by encrypting the information itself or by encrypting the backup file or the location of its storage.

Under the terms of the Premera Judgment, Premera was obligated to encrypt all electronic personal information, protected health information or medical information stored or in transmission "except where Premera determines that encryption is not reasonable and appropriate and it documents the rationale for this decision."

Similarly, under the terms of the FTC's Consent Order with InfoTrax, the company was required to encrypt Social Security numbers, payment card information, bank account information and authentication credentials including user IDs and passwords stored on its network.

See "Is Encryption Obligatory? HHS Upholds Texas Hospital $4.3M HIPPA Fine" (Jul. 11, 2018).

Recent Settlements Highlight a Framework of Security

The recent settlements discussed above highlight the data security measures deemed by state and federal regulators to comprise the best set of practices to secure sensitive information as risks and threats continue to evolve. By investing in a framework of practices, tools and policies designed to (1) restrict access to sensitive information, (2) increase threat awareness, and (3) implement advanced technical security measures, organizations can mitigate the likelihood of a future data breach and reduce the risk that regulators will find fault in the reasonableness of their data security practices.

Ann-Marie Luciano is a partner in the state attorneys general practice at Cozen O'Connor, where she regularly advises clients evaluating and managing risks associated with data privacy and information security practices. She has defended companies facing investigations by State AGs in every state as well as FTC-initiated investigations into a wide range of issues, including data privacy and security practices, data breaches, marketing and advertising practices and antitrust.

Jawaria Gilani is an associate in the state attorneys general practice at Cozen O'Connor and represents clients involved in inquiries, investigations and lawsuits initiated by State Attorneys General across the country in matters involving data privacy, security, consumer protection and antitrust.