The CYBERSECURITY LAW REPORT

Vol. 4, No. 3 February 14, 2018

FTC ENFORCEMENT

Lessons and Trends from FTC's 2017 Privacy and Data Security Update: Workshops and Guidance (Part Two of Two)

By Jill Abitbol

The Cybersecurity Law Report

In its most recent Privacy & Data Security Update (Update) the FTC recapped its 2017 enforcement actions, workshops and other guidance, providing information on best privacy and data security measures for companies, big and small. In this second article of our two-part series, legal and technical experts distill valuable lessons from the agency's 2017 workshops and guidance and discuss what to expect from the agency in 2018. In the first article, we examined enforcement highlights and steps companies can take to comply with applicable laws and steer clear of the FTC's reach.

In addition to its enforcement actions in 2017, the Update highlights the agency's workshops, guidance and reports, much of which focused on likely areas of future FTC enforcement, such as IoT devices, payment systems, artificial intelligence (AI) and blockchain technologies. The Update also references the FTC's creation of several videos for businesses on NIST's cybersecurity framework, data breach response, ransomware and email authentication.

See also "FTC Priorities for 2017 and Beyond" (Jan. 11, 2017).

FinTech Workshops Focused on Evolving Technology

The FTC's second FinTech Forum focused on two evolving types of financial technology: peer-to-peer payment systems and crowdfunding platforms. Its third FinTech Forum examined the consumer implications of AI and blockchain.

See also "How Blockchain Will Continue to Revolutionize the Private Funds Sector in 2018" (Jan. 17, 2018).

Peer-to Peer Payments

Peer-to-peer payment systems are "technology ripe for scams," Michael Coden, the head of the cybersecurity consulting practice at BCG Platinion, a subsidiary of The Boston Consulting Group, told The Cybersecurity Law Report. In cybersecurity, "one of the first things to look at is the motive of the adversary and the most common motive is making money." With payment systems, adversaries can direct payments towards themselves rather than the intended payee, and trick the payer to pay them, rather than the intended recipient, he said.

Given this landscape, Coden advised providers of these services to: "(1) encrypt data in transit as well as at rest; and (2) ensure good identification and authentication of the payer and the payee using multi-factor authentication, or continuous authentication if possible." He recognized that requiring multi-factor authentication "adds a level of inconvenience" but noted that "there is always a trade-off between user identification and ease of use."

Crowdfunding

Crowdfunding presents slightly different issues. It involves individuals "investing in a potential product or service." While the concept is beneficial in that it allows companies starting up to "collect money from a lot of small angels," it is "ripe for criminals to take advantage of the system," Coden explained, advising crowdfunding platforms to "properly vet the small companies that are looking for financing."

Coden predicted that there will be a scenario within the next few years where consumers are harmed and then, "crowdfunding will end up getting regulated." A potential theft scenario might involve a person who asks for money to help develop a desirable product on a crowdfunding platform. Then, that person can take the money, "go to some country [from which] he or she can't be extradited, never making the product, and live in the lap of luxury."

"Any time there is a unique new system for transferring money that is widely distributed, the criminals are going" to adapt and use that technology to obtain other people's money, Coden cautioned. "This is not a new motive; it has been around since Cain wanted what Abel had."

Blockchain

The FTC's third FinTech Forum examined how blockchain offers services to consumers, its potential benefits and consumer protection implications.

There is a view that "the blockchain is secure because it is validated by a large number of disinterested users. The basic concept of the cryptocurrencies is that there are miners who are constantly processing the blockchain and affirming it has not been tampered with

and, therefore, is secure," Coden explained. However, recent attacks and successful compromises on various cryptocurrency exchanges, with tremendous losses of money, indicate "that blockchain is not as secure as everybody would like to believe it is."

While thus far any "real benefit" of blockchain has eluded him, he said he believes that in the "long term we will find that happy medium where the ledger provides value, especially in its ability to provide auditability along with the transaction history, and there will be a way of doing it economically but that may require regulation. That is why the FTC is watching it so closely."

In the meantime, organizations using blockchain technology should take steps to protect sensitive consumer data. "If insurance companies and medical healthcare providers are thinking about treating the blockchain as a secure method of data transfer, they should realize that blockchains are a distributed database. In other words, medical records stored in a blockchain are widely distributed and if someone is able to crack that blockchain they will have access to all of that PHI data," Coden advised. Thus, perhaps they are "better off keeping all of that data in a somewhat less distributed database, which is under their control, and really make sure the data is not leaving their data centers or cloud providers and being distributed all over the internet."

See our three-part series on blockchain technology: "Basics of the Blockchain Technology and How the Financial Sector Is Currently Employing It" (Jun. 14, 2017); "How Financial Service Providers Can Use Blockchain to Improve Operations and Compliance" (Jun. 28, 2017); and "Blockchain and the Financial Services Industry: Potential Impediments to Its Eventual Adoption" (Jul. 12, 2017).

Artificial Intelligence

"AI could be an even more popular buzzword than blockchain, which may say something about blockchain not catching on as quickly as it could," Coden suggested. While organizations are using AI to improve profitability and business functions, "unfortunately, the adversaries are also using AI" to penetrate an organization's system and, once they do, "adversaries today are using AI to explore all of the internal computer devices and to find the systems with the most value."

There is an "asymmetric problem" in cybersecurity where the adversary only needs to find one way in and organizations have to be able to protect themselves against all of the possible entry points to their systems, Coden explained. "AI is a double-edged sword in that case," he said.

The most advanced users of AI are, of course, the big search engines. "Consumers are willing to give up tons of private information in exchange for some free service, whether it be search information or the ability to use documents online or free email or ability to

do spreadsheets online without paying for the software," Coden said. Before the FTC can protect consumer information, "consumers need to be worried about privacy." He added, "The end result is that the information is out there, being used by AI software product engines," and noted, "Google does make a very good attempt at making their privacy statements very short, clear and concise, however consumers are willing to freely give up their private information in exchange for the free services."

See "Understanding and Using Bot Technology to Address Privacy and Security Challenges" (Nov. 8, 2017).

Perspectives on Reports & Surveys

Email Authentication Technology

The Update references the FTC's staff perspective finding that most major online businesses are using proper email authentication technology to prevent phishing emails, but few of these businesses are taking full advantage of the latest technologies to combat phishing.

"Many ransomware attacks happen as a result of spear phishing and anything that can help organizations verify and independently determine whether an email is accurate is extremely important," Matthew Meade, a Buchanan, Ingersoll & Rooney shareholder, told The Cybersecurity Law Report. He suggested that companies use learning tools to train employees – a fake spear phishing email is sent and if an employee clicks on it, he or she will get a tutorial of why that was wrong. "Those are extremely effective and I would recommend that those exercises be used by every company, big or small," Meade advised.

See "Overcoming the Challenges and Reaping the Benefits of Multi-Factor Authentication in the Financial Sector (Part One of Two)" (Jul. 26, 2017); Part Two (Aug. 9, 2017).

IoT Devices

The Update also notes the FTC's IoT Home Inspector Challenge, which encourages developers to create innovative tools to help protect consumers from security vulnerabilities in the software of home devices connected to the Internet of Things. Based on the FTC's IoT reports, Coden believes that there will be more regulation on IoT devices in the future. "There are going to be too many of these devices and the dangers will just be too extraordinary. The industry will not be able to get its act together and regulate itself. So I believe the government is going to have to step in because we are going to see more and more serious cyber events due to a proliferation of IoT devices and the fact that human use of them is not going to be as intelligent as the devices themselves are."

See "New NIST and DHS IoT Guidance Signal Regulatory Growth" (Nov. 30, 2016).

Small Business Guidance

In 2017, the FTC made a concerted effort to educate small businesses on cybersecurity threats and response. It created a website specifically for small business owners, providing education and tips on cyber risks and response details for data breaches. Further, the FTC presented and held several roundtables throughout the country regarding small businesses and data security.

The FTC's efforts for small business owners indicate that the agency "gets it," Meade opined. While not necessarily an issue at a Fortune 100 or 500 company, "there is still a perception at the mid- to small-sized businesses that cybersecurity and protection of consumer data is an IT problem. As much as it seems that is an ancient idea, it still is prevalent."

For cybersecurity to work within an organization, Meade said there "needs to be a full top-down commitment to cybersecurity. Too often we see clients that have policies and procedures in place but there is no teeth behind them and nobody is really enforcing them and no one is even checking to see if they are actually working, which is even worse." Small to mid-sized companies still have large amounts of data. "For example, a W-2 breach that involves 500 employees is extremely significant to a small organization. If every employee's information were compromised, that can be catastrophic," he explained.

See "How Small Businesses Can Maximize Cybersecurity Protections and Prioritize Their Spending" (Jul. 12, 2017).

Small Business Guidance on Passwords

The Update emphasizes the importance of passwords. "As elementary a message as 'use strong passwords' is, there are many companies that don't use strong passwords," Meade pointed out. There are still companies where "people have never changed their passwords, and those that don't have processes in place to de-activate a person's password when they leave the organization."

Thus, Meade said he believes the FTC guidance is helpful. "We are seeing a lot of incidents happening from insecure remote access," and the guidance provides tips on that. The FTC guidance can be particularly helpful to companies with limited resources because those companies can review and evaluate the guidance and then decide whether to engage an IT professional or counsel. Meade recommended engaging a third party, at least "to address implementation because the training component and employee awareness is extremely important."

See also "Designing, Implementing and Assessing an Effective Employee Cybersecurity Training Program (Part One of Three)" (Feb. 17, 2016); Part Two (Mar. 2, 2016); and Part Three (Mar. 16, 2016).

NIST

The FTC also covers its view of the NIST Cybersecurity Framework. "If it is reasonable for companies to be able to apply and follow them, NIST guidelines are absolutely a good signpost." If there are smaller companies that are "scared away by some of NIST's provisions," it would then be helpful for them to "have a qualified IT professional look at it and evaluate," Meade advised.

See "Demystifying the FTC's Reasonableness Requirement in the Context of the NIST Cybersecurity Framework (Part One of Two)" (Oct. 19, 2016); Part Two (Nov. 2, 2016).

What to Expect in 2018

On the FTC front, there are certainly a lot of hot-button issues like how much can it police the deficiencies of a company's cybersecurity measures. Experts expect certain issues that fall under this umbrella to be specifically watched in 2018.

Data Collection and Emerging Technologies

Surreptitious data collection requires some vigilance, Fried Frank partner Una Dean told The Cybersecurity Law Report. Areas on which to focus include "issues of emerging technology, mobile apps and privacy," and how third-party vendors are managing data. "Companies are much more focused these days than ever before on third-party vendor issues, especially because they are being held liable for any deficiencies in their vendors," she said, noting that contractual language preserving the ability to monitor vendors is key.

See "The Regulators' View of Best Practices for Social Media and Mobile Apps" (Apr. 13, 2016).

What Constitutes Harm

Official clarification on what constitutes a specific injury could be forthcoming in 2018, Sidley partner Christopher Fonzone predicted. There was an FTC workshop in December around what a consumer injury is in privacy and data security and "an important change in how the FTC looks at these things" could come out of that process, Fonzone, former Deputy Assistant and Deputy Counsel to President Obama and the Legal Adviser to the National Security Council, said. There was an expectation that there would be big chances

in this area due to the new administration in 2017 but, "there was more continuity with approaches taken in the past." However, especially with the new nominees for commissioner, "there could be changes coming down the road – in particular, the definition of injury to consumers."

Dean agreed that the definition of harm "certainly could play a big role in 2018." Not only is it "a foundational question in terms of what the FTC is going to focus on," but it is also an ongoing process in the courts following the Supreme Court's decision in *Spokeo*, she said. "What the bar is for when these injuries occur is something that is going to be crucial for the FTC and a host of other regulators."

See "A Wake-Up Call: Data Breach Standing Is Getting Easier" (Jan. 17, 2018).

No Downturn in Enforcement

According to Meade, the FTC's goals are constant and it is unlikely that in 2018 there will be "any downturn in ensuring consumer personal information is protected and that reasonable security is being implemented at companies that are subject to FTC oversight."

In light of enforcement expectations, Meade recommended three things companies should be doing now to ensure compliance with the FTC's privacy and data security expectations:

1. take a proactive approach to cybersecurity including implementing policies and procedures designed to protect consumer and employee data;
2. train employees specifically on what steps they can take to protect and secure the data with which the organization is charged; and
3. ensure relationships with third parties that are entrusted with the company's most sensitive data are protected by contracts with strong cybersecurity requirements.

Ransomware

The Update also references the FTC's ransomware guidance. One piece of this that Meade said he finds particularly important is the recommendation that "all companies regardless of size understand what they have to do if they get a ransomware demand."

Ransomware is one of the "biggest items on the cybersecurity agenda this year and, I suspect, for years to come," Coden said. The number of companies affected and the amount of money that was lost due to WannaCry and NotPetya (destructware) attacks

was enormous, he noted.

Preparation for a ransomware attack means having an incident response plan and practicing it, which entails if you have cyber liability insurance, knowing when to notify the carrier, Meade advised. It is also important to understand "how your back-ups are maintained – are they separate, are they part of a flat network so back-ups may get encrypted by the malware as well?"

Regarding whether to pay a ransom, Meade acknowledged that "the FBI's recommendation is not to pay but there are certain times when there are business necessities or life necessities. I've represented smaller covered entities under HIPAA, where a ransomware attack has created a life-safety issue because the ransomware prevented the company from accessing patient records. In that situation, payment is warranted. It is really a case-by-case evaluation." On one hand, "the FBI's point makes good sense. You don't want to encourage criminal activity. On the other hand, if there are situations where safety is involved, payment might be the right direction to move in," Meade suggested.

See "Defending Against the Rising Threat of Ransomware in the Wake of WannaCry" (May 31, 2017).

Improved Data Breach Response

While "there is a huge focus on breach prevention, data breach response is a very underserved part of the cybersecurity issue," Coden observed. Companies should recognize that they "will be compromised, and they must be prepared to deal with that inevitable event." He cited a four-factor equation to explain the importance of beach response: Losses = Threats x Vulnerabilities x Consequences (L = T x V x C), noting that if T, V or C ccould equal zero then losses would be zero. Unfortunately, "threats are totally out of our control and vulnerabilities will never get to zero."

Vulnerabilities can be significantly reduced, however, Coden said. He suggested three important steps companies can take to reduce vulnerabilities, including:

1. *Identify the crown jewels.* Companies need to determine what to protect. "Too many companies are trying to protect everything and that is not possible. If you identify the things that would put your company out of business or cause you the most harm. Whether it is financial harm or loss of life, you need to identify those most important things and focus on protecting the few really key crown jewels." It helps to "ask the CEO what the five most important assets are in the company that need to be protected. If he or she doesn't know, you have a problem."
2. *Determine who can access key assets and isolate the systems that contain those*

assets. Colleagues trusting each other can be a problem. "The worst example of an environment of trust was the one where Mr. Snowden was able to ask 25 of his colleagues who trusted him to lend him their passwords so it would be easier for him to finish a "special project." He didn't have access to all of those documents but he and his 25 friends did. We have to get to a point where only the people who really need access to these crown jewels do have access."

3. *Make prevention part of the culture of your organization.* Signs and well-known safety guidelines can help. A manufacturing company or an oil company will have a sign in every plant that says "237 days since the last industrial accident. Nobody who walks under that sign wants to be the one who resets that counter to zero. That is built in to the culture of almost all companies today." At other companies, there are safety rules such as a requirement to hold a handrail on the stairs or a plant with a big bucket of safety glasses next to the door. "Twenty years ago, people complained that was a nuisance. Today it is a habit. We have to get cybersecurity culture to the point where one colleague can tell another that even though they trust their colleague, they will not share their password." What Coden believes works best is an approach he calls "frontline manager transformation." Instead of a top-down approach that "forces training" on employees, "we work with people at the lowest level of the organization and their managers – janitorial groups, people running machines, copiers and printers, the executive assistants and managers of those groups and ask them to compile the best cybersecurity practices," including mistakes and successes, to share with each other. Then, "they build this into their daily routine as a cultural thing and they become a self-support group. That cultural change works its way up the organization rather than down. On the other hand, regulatory fines are a really good incentive to change things. So if companies don't find a way to change the culture, the government will."

The "consequence" management factor of the equation is the part that incorporates data breach response plans, which need to be practiced, Coden advised. When some companies are breached, "the executives don't seem to have a plan to deal with the breach. Or, if they did have a plan, they probably had not practiced it because they make a large number of mistakes causing public outrage and class action lawsuits." When companies have a well prepared plan, practice the plan, and execute the plan, they can greatly reduce the damages due to a breach. A good example is the credit card breach at Home Depot. Because the executives properly managed the consequences and communications, there was virtually no loss of revenue or customer loyalty. In fact, most people don't even remember that the breach occurred.

See "Lessons From the Equifax Breach on How to Bolster Incident Response Planning (Part One of Two)" (Sep. 27, 2017); Part Two (Oct. 11, 2017), and also our three-part guide to developing and implementing a successful cyber incident response plan: "From

Data Mapping to Evaluation" (Apr. 27, 2016); "Seven Key Components" (May 11, 2016); and "Does Your Plan Work?" (May 25, 2016).
