Federal Trade Commission

Data Security:
Why It's Important, What the FTC is Doing About It

Jessica Rich[1]
Director, Bureau of Consumer Protection, FTC

National Consumers League
Alliance Against Fraud Coalition
March 24, 2014

I. Introduction

Hello. I am delighted to be here today to talk about the FTC's work on the important issue of data security. Thanks so much to NCL and the Alliance Against Fraud for inviting me.

Everyone in this room is well aware of data breaches and their impact on consumers. But these days, you don't have to be a consumer protection expert to know this – look no further than today's headlines. Recent reports of data breaches have been unrelenting – Target, Neiman Marcus, and the University of Maryland, just to name a

[1] The views expressed here are my own and do not necessarily represent the views of the Federal Trade Commission or any Commissioner. Special thanks to Molly Crawford for assisting in the preparation of these remarks.

few. These events remind us that consumers' data is at risk. Hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers' sensitive information, and misuse it in ways that can cause serious harm to consumers and businesses.

But let's be clear: these breaches are not a new phenomenon. In fact, we have been hearing about them for some time now. Every year, new incidents are reported that reignite concern about data security, as well as debate about the best way to provide it.

The need for companies to implement strong security measures is clear: if sensitive information falls into the wrong hands, the results can be devastating. Consumers face the risk of fraud, identity theft, and other harm. As one example, the Bureau of Justice Statistics estimates that 16.6 million people – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012. Apart from the significant impact on individual consumers' lives, there are broader ramifications – data breaches can harm a business's reputation and bottom line, and also result in the loss of consumer confidence in the marketplace.

II. The FTC's Approach to Data Security

The FTC has long been at the forefront of data security – since 2001, when we developed our Safeguards Rule under the Gramm Leach Bliley Act, and also began challenging data security violations under our general FTC Act authority. Today we promote strong data security protections using all of the tools at our disposal – law enforcement, workshops, studies, reports, and consumer education and business guidance.

The Commission's law enforcement actions have challenged the failure by companies to provide reasonable protections for consumers' personal information. We've obtained 50 settlement orders against such companies, halting harmful data security practices; requiring the companies to accord strong protections for consumer data going forward; and raising awareness about the risks to data, the need for reasonable security, and the types of security failures that raise concerns. Our settlements have addressed the risks to a wide variety of consumer data, including Social Security numbers, health data, data about children, credit card information, bank account information, and usernames and passwords, in a broad range of sectors and platforms.

We have based these actions on several laws we enforce. First, the Safeguards Rule, which I just mentioned, imposes data security requirements on non-bank financial institutions. Second, the Fair Credit Reporting Act requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information. Third, the Children's Online Privacy Protection Act requires reasonable security for children's information collected online.

Finally, we've used our authority under Section 5 of the FTC Act to challenge unfair or deceptive practices relating to the security of consumer data. Our deception authority allows us to challenge materially misleading statements or omissions about data security. Our unfairness authority requires proof of various elements but, in a nutshell,

allows us to challenge data security practices that create unreasonable risk of harm to consumers.

The touchstone of the FTC's approach to data security, under whatever law we are applying, is reasonableness: a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. Using this approach, the Commission challenges practices that are unreasonable in light of the full range of circumstances. We *don't* impose strict liability for a breach, and I think it's fair to say that none of our cases have been "close calls." Instead, the FTC recognizes that there is not such thing as perfect security; that reasonable security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.

Our cases illustrate this approach. For example, in our most recent case – notably, our 50th data security settlement – the FTC settled allegations that GMR Transcription Services – an audio file transcription service – violated the FTC Act. According to the complaint, GMR relied on service providers and independent typists to transcribe files for their clients, which include healthcare providers. As a result of GMR's failure to implement reasonable security measures and oversee its service providers, at least 15,000 files containing sensitive personal data – including consumers' names, birthdates, and medical histories – were available to anyone on the Internet.

Also, the FTC recently announced its first "Internet of Things" case involving a video camera designed to allow consumers to monitor their homes remotely. The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring, and claimed in numerous product descriptions that they were "secure." In fact, the cameras had faulty software that left them open to online viewing – and even in some cases listening – resulting in hackers posting 700 consumers' live feeds on the Internet.

Our best known data security case may be the one we brought back in 2006 against data broker ChoicePoint. We alleged that ChoicePoint sold sensitive information (including Social Security numbers in some instances) about more than 160,000 consumers to data thieves posing as ChoicePoint clients. In many instances, the thieves used that information to steal the consumers' identities. According to our complaint, ChoicePoint failed to use reasonable procedures to screen prospective purchasers of the consumers' information and ignored obvious security red flags. For example, the company approved as purchasers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from public commercial photocopying facilities. In settling the case, ChoicePoint agreed to pay $10 million in civil penalties for violations of the FCRA and $5 million in consumer redress for identity theft victims, and agreed to undertake comprehensive data security measures.

The huge breaches that occurred in the ChoicePoint matter were considered, at the time, a wake-up call for the industry and the public about the need for stronger data

security protections in the commercial marketplace. That was almost a decade ago and, unfortunately, we continue to experience these wake-up calls again and again as breaches continue to occur, compromising consumer data. In fact, during the last decade, we have brought cases against TJX, LexisNexis, DSW Shoe Warehouse, BJ's Warehouse, Microsoft, Guess, Petco, Tower Records, LifeLock, and many others for data security misrepresentations and harmful breaches that could have been avoided. We alleged that all of these companies failed to secure consumer data, and all of them are now under FTC orders, subject to substantial fines for violations.

Now I want to emphasize that securing data is a task that every company can and must undertake. Many of the steps needed to secure data are common sense, within a company's ability to learn and implement for itself. In a nutshell, companies should:

First, assign someone to take charge of the process – accountability is critical.

Second, do a thorough risk assessment of the risks to data in their operations – what data is collected, who has access to it, how long is it kept, what are the weak spots where someone could obtain unauthorized access to it, etc. This risk assessment should include learning about what risks are out there in the marketplace through software newsletters and bulletins – there is a lot of great, free guidance out there.

Third, design a security program to control and limit these risks. This should be done in all areas of a company's operations – this means employee training, physical and computer security, incident response, service provider oversight, etc.

And finally, of course, adjust the program as needed to address changes to the business and to the risks.

III. CONSUMER EDUCATION AND BUSINESS GUIDANCE

And that's a good transition to our educational mission. In addition to enforcement, we use consumer education and business guidance to promote stronger security measures for consumer data. On the business guidance side, we publish a truly wonderful brochure that provides a step-by-step approach to data security, along the lines I just described – *Protecting Personal Information*. We also have many other materials on our website, www.ftc.gov.

On the consumer education side, we provide information and tools to consumers so they can take steps to protect themselves. For example, the FTC sponsors OnGuard Online, a website designed to educate consumers about basic computer security, as well as its Spanish-language counterpart, Alerta en Línea. Together, these sites average more than 2.2 million unique visits per year.

For consumers who may have been affected by the recent Target and other breaches, the FTC has posted information online about steps they should take to protect themselves. We recommend that consumers review their credit card and bank statements; check their credit reports every few months; and delete phishing emails or text messages that ask consumers to confirm or provide account information.

We also have tools for consumers who learn that they have become a victim of identity theft. For example, the FTC has long published a victim recovery guide and

other resources to explain the immediate steps consumers should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; and how to file a police report.

And to help consumers avoid having their information compromised in the first place, we publish materials recommending that consumers (1) keep up with security updates on browsers and operating systems; (2) make sure any website they use to transmit financial information is encrypted, which they can tell by making sure the URL starts with https (the "s" stands for secure); and (3) create strong passwords and keep them safe.

In the end, however, there are some measures that are simply outside of consumers' control. If their information is sitting in an insecure company database, or collected insecurely at the point of sale, even the most sophisticated consumer cannot avoid the harm of a data breach. This is why it critical that businesses take appropriate steps to protect consumer information from unauthorized access.

IV. Data Security Legislation

The last issue I'd like to address is the pressing need for data security legislation. Although the FTC has been able to accomplish a lot with its existing authority, the current laws don't cover all of the businesses that collect sensitive consumer data. Perhaps most importantly, they generally don't allow us to seek civil penalties for violations – a remedy that is critical to deterrence in this area. For that reason, the Commission continues to reiterate its longstanding bipartisan call for a strong federal data security and breach

notification law. The Commission is about to provide testimony for the fourth time, since only the beginning of this year, on the urgent need for such legislation.

There are a number of data security bills that have been proposed in the current Congress. While we have not taken a position on any specific legislation, there are certain key elements that we examine carefully in any legislative proposal.

First, we look at the types of data and entities covered under a bill. For example, the FTC believes it's important to cover non-profits because many of the breaches in recent years have occurred at universities and other non-profit entities. In addition, we want to ensure that legislation covers the key types of data that can be used to harm consumers. For example, some bills don't cover Social Security numbers alone. However, because children often have Social Security numbers without any financial history linked to them, a child's Social Security number alone can be paired with another person's information in order to commit identity theft.

Second, we look at the trigger for when notice is required. Is it "reasonable risk of harm?" Is it "substantial risk of identity theft?" Is notice required for any breach at all? Striking the right balance is critical for both consumers and businesses. We want to ensure that consumers learn about breaches that could harm them so they can take steps to protect themselves. But we don't want to notify consumers when the risk of harm is negligible, especially since over-notification could lead consumers to become numb to the notices, and fail to spot or act on risks that truly are significant.

Third, we believe any legislation should include FTC rulemaking authority, which would enable the FTC to respond to changes in the marketplace and in technology that create risks to consumer data. For example, a decade ago, we would never have thought about the need to protect information about an individual's precise geo-location because no one collected that data. Today, the explosion of mobile devices has made such information readily available to companies, and it needs to be protected. Rulemaking authority would allow the Commission to respond to these types of changes.

Fourth, as I mentioned above, legislation should give the FTC the ability to seek civil penalties to help deter unlawful conduct. Under current laws, the FTC only has the authority to seek civil penalties in limited instances.

Finally, let me briefly mention preemption. The vast majority of states have some kind of data security or breach notification law in place, and state Attorneys General have been working alongside the FTC to protect consumers in this area. Our Chairwoman has testified that she would support preemption of these laws, but only if a federal standard offers strong protections for consumers and is enforceable by the states.

V. Conclusion

In closing, I want to emphasize that data security remains a top priority for the Commission. We will continue to use our existing tools to promote better security practices, and we will continue to support enactment of new laws to add to our tools in this area. But we can't do this alone. We need the help of advocates, industry, policymakers, and other partners – like everyone in this room – to spot problems in the

marketplace, and to help us educate consumers and businesses about the need to secure data, and how to do it.

Thank you for having me here today – I am happy to take questions.