Remarks of Lydia B. Parnes[1]
Director, Bureau of Consumer Protection, Federal Trade Commission
National Association of Mortgage Brokers
2007 Legislative & Regulatory Conference

I. Introduction

Good morning. I am pleased to be here and would like to thank the NAMB for inviting me to speak today. Home ownership is a part of the American dream. Your industry is an important component of providing that dream to millions of consumers. Our job at the Federal Trade Commission is to make sure that consumers have the tools they need to make knowledgeable decisions, and are not treated deceptively or unfairly in the process. We do that through education – educating both businesses and consumers – partnering with industry, and law enforcement. I look forward to continuing to work with NAMB on our many issues of common interest.

Educating consumers and businesses is an essential part of the FTC's mission. We have both general information on our web site – www.ftc.gov – and specific information where we notice trends or areas where consumers are confused. One such issue was discussed at the last panel – unsolicited phone calls from mortgage marketers using so-called "trigger lead lists." Many consumers are confused about why they are receiving these calls; others are concerned that their current lenders are revealing their personal information. To address this subject, the FTC released a consumer alert a few weeks ago, entitled "*Shopping for a Mortgage? Your Application May Trigger Competing Offers."* The alert describes the process of prescreening

[1] The views expressed herein are my own and do not necessarily represent those of the Federal Trade Commission or of any Commissioner.

based on inquiries. It also tells consumers how to stop receiving these calls if they don't want them: by exercising their right to opt out of prescreened offers and by placing their phone numbers on the National Do Not Call Registry.

And we have made sure that those options are meaningful through enforcement. This past fall, the Commission brought a case against a mortgage services company and a telemarketer based in Maryland for violating the Do Not Call provisions of the FTC's Telemarketing Sales Rule.[2] The FTC charged that these companies called consumers whose numbers were listed on the Do Not Call Registry to market mortgage products and services. The companies settled those charges for a combined penalty of over $500,000 and a permanent injunction against further violations.

The Do Not Call Registry has been quite successful – the humorist Dave Barry called it the most popular government program since the Elvis stamp. More than 130 million telephone numbers have been registered since 2003. Most entities covered by the DNC Rule comply with the law. For those who do not, tough enforcement is a high priority for the FTC.

Another area of focus for us both in terms of education and enforcement has to do with data security, a top priority for the FTC. We all regularly hear news reports of security breaches exposing consumers' personal information and putting them at risk for identity theft. TJ Maxx, Johns Hopkins University Hospital, and Chase Bank are just a few names from the headlines in the past few months. Identity theft costs consumers and businesses billions of dollars each year. But, it's not just about money – data breaches threaten consumer confidence, both in the business

---

[2] *United States v. USA Home Loans, Inc., et al.*, No. 1:06-cv-02850-JFM (D. Md. Oct. 31, 2006); *see* 16 C.F.R. Part 310.

that suffered the breach and in our marketplace as a whole. Many surveys have shown that consumers are less willing to engage in electronic transactions because of the fear that their data will be stolen. For these reasons, it is critical that the business world – and the government – devote the time, resources, and management attention necessary to secure sensitive information.

The mortgage industry is faced with unique challenges in the data security arena. The most serious form of identity theft occurs when a criminal obtains certain sensitive information – like Social Security number, driver's license, birthdate, mother's maiden name – and uses that data to open new accounts in the consumer's name. Of course, your industry *needs* to collect this information about your customers. But, that makes you a tempting target for identity theft. And you may have to keep some of this information for extended periods of time. This means that you must secure data as you collect it, and continually reassess whether your storage methods are adequate as threats and technologies change over time.

The data security challenge can seem daunting, but the Commission has made substantial efforts to help industries like yours meet that challenge. Later, I will summarize some of our education and outreach efforts. But first, I would like to focus on the legal framework governing data security and the Commission's enforcement program.

II. Data Security Laws

A patchwork of laws govern the confidentiality standards for different businesses and information. For example, the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA) protects the confidentiality of consumers' medical information.[3] And the Driver's Privacy Protection Act (DPPA) limits the sale or disclosure of drivers license

[3] 45 C.F.R. Parts 160, 162 and 164.

numbers.[4]

Three federal data security laws are most relevant to your industry. First, the Gramm-Leach-Bliley Act, which requires you to provide annual privacy notices to your customers, also directs you to protect consumers' personal financial information.[5] The FTC and the federal bank regulators have issued Safeguards rules implementing this requirement.[6] Second, the Fair Credit Reporting Act contains provisions on the proper disposal of credit report information.[7] Again, the FTC and the bank agencies have fleshed out these provisions through our Disposal Rule.[8] Third, the Commission has used the Federal Trade Commission Act, which prohibits unfair or deceptive practices, to act against companies that failed to reasonably protect sensitive consumer data.[9]

Over the past few years, the Commission has brought fourteen data security enforcement actions for alleged violations of these laws and rules. Four of those cases involved mortgage companies, which perhaps underscores the challenges your industry faces in protecting consumer data.

III. Reasonable and Appropriate Measures

The core principle underlying all of our data security cases is that companies must

---

4 18 U.S.C. § 2721, *et seq.*

5 15 U.S.C. § 6801, *et seq.*

6 16 C.F.R. Part 314

7 15 U.S.C. § 1681, *et seq.*

8 16 C.F.R. Part 682.

9 15 U.S.C. § 41, *et seq.*

implement ***reasonable and appropriate procedures*** to protect consumers' sensitive information. This is a flexible standard, and allows different types of companies to implement security in ways that are compatible with their organizational structure and operations. It also is adaptable to changes over time – changes in technology, changing threats to data security, changes in a company's way of doing business. The "reasonable procedures" standard also recognizes that breaches can happen despite reasonable precautions. In fact, the FTC has declined to take action against a number of companies that had breaches but had reasonable protections in place.

You may ask what lessons can be learned from the FTC's four data security cases involving the mortgage industry. Let's take a look.

IV. Safeguards Cases

In four of these cases, the FTC enforced the GLB Safeguards Rule. By way of refresher, the Safeguards Rule requires financial institutions to protect the security, confidentiality, and integrity of customer information. How? By developing a comprehensive written information security program that contains reasonable administrative, technical and physical safeguards. The Rule sets forth basic requirements – the financial institution must assign one or more employees to oversee the program; must conduct a risk assessment; must put safeguards in place to control the risks identified in the assessment and regularly test and monitor them; must require service providers, by written contract, to protect consumers' personal information; and finally, must periodically update its security program.

In late 2004, the FTC settled cases against two mortgage companies– Nationwide

Mortgage Group,[10] a mortgage broker in Virginia, and Sunbelt Lending Services[11] in Florida – both for allegedly failing to comply with the Rule's basic requirements for risk assessment and control. The Commission charged that Nationwide stored sensitive customer information on a computer network that was accessible to all employees and accessible through the Internet. And Nationwide did not monitor its network for vulnerabilities that would expose customer information to attack. As to Sunbelt, the FTC alleged that it failed to oversee the security practices of its service providers and loan officers working from remote locations throughout the State of Florida. These cases were not close calls – the FTC alleged clear, specific, and multiple violations of the basic requirements of the Safeguards Rule. The settlement agreements bar the companies from further violations of the Rule and require them to undertake independent audits of their security systems every other year for ten years.

Then, in September of 2005, Superior Mortgage Corporation,[12] a lender with 40 branch offices in 10 states and multiple web sites, settled FTC charges that it failed to provide reasonable security for the sensitive information it gathered from customers. Superior, contrary to statements on its web site, failed to encrypt or otherwise protect sensitive customer information before sending it by email; failed to implement appropriate password policies for company systems containing sensitive customer information; and failed to assess risks to

---

[10] *In the Matter of Nationwide Mortgage Group, Inc. and John D. Eubank,* (Docket No. 9319) (consent order) http://www.ftc.gov/os/adjpro/d9319/index.htm

[11] *In the Matter of Sunbelt Lending Services*, (Docket No. C-4129) (consent order) http://www.ftc.gov/os/caselist/0423153/04231513.htm

[12] *In the Matter of Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005) http://www.ftc.gov/os/caselist/0523136/0523136.htm

customer information until more than a year after the Safeguards Rule took effect. In other words, it took an approach to data security that was too little, too late.

Finally, in an example of a "low-tech"data security problem, the FTC settled an enforcement action in May of 2006 with Nations Title,[13] a real estate services company, alleging, among other violations, that the company threw documents containing sensitive consumer information into an open dumpster. Thankfully, the documents did not fall into the hands of identity thieves; they were, however, found by a news reporter. The message is clear: how you get rid of the information is as important as how you store it.

V. Business Outreach

Designing a good information security program is not as difficult as you may think. And the FTC has some tools to help you along the way.

As I mentioned earlier, we offer business guidance and publications on how organizations can protect their customers' personal data. It's all available online at ftc.gov/IDtheft. To give just a few examples, we have a publication on computer security to help you identify the most common computer vulnerabilities so you can evaluate your own system to make sure it's protected.[14] We also have a brochure on the Safeguards Rule, which explains the rule's requirements and offers specific steps on how to implement them.[15] Should a breach

---

[13] *In the Matter of Nations Title Agency, Inc., Nations Holding Company, and Christopher M. Likens*, FTC Docket No. C-4161 (June 19, 2006) (consent order) http://www.ftc.gov/os/caselist/0523117/0523117.htm

[14] *Security Check: Reducing Risk to Your Computer Systems,* http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm

[15] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*. http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm

occur, we have material to help you evaluate when and how to notify law enforcement, affected businesses, and individual consumers, including a model letter to send to consumers. [16]

Finally, I am very pleased to announce the recent release of *Protecting Personal Information: A Guide for Business*.[17] This brochure articulates five key steps that are part of a sound data security plan: (1) Take stock; (2) Scale down; (3) Lock it; (4) Pitch it; and (5) Plan ahead. Let's talk about what each of those steps entails.

First, Take Stock – you need to know what consumer information you have and who has access to it. What data do you collect? Where do you store it? What do you share with service providers and where do they store that information?

Second, Scale Down – you need to determine whether you really need all the information you gather. Do you need to keep records for completed transactions? Do you use all the pieces of data you collect? Is access to data limited to those who need it to perform their jobs?

Third, Lock It. If you are going to keep it , you have to keep it safe. Electronic security – encryption, firewalls, and other IT defenses – are important, but a comprehensive information security program includes more. Look at the physical security of your building. Do you lock file cabinets, office doors, and outer doors? Are visitors escorted at all times?

Employee training is an extremely important component in your security plan. Employees need to know how to use the electronic and physical security measures in place, and how to avoid old-fashioned scams. A lot of attention has been paid lately to pretexting, though

---

[16] *Information Compromise and the Risk of Identity Theft: Guidance for Your Business* http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus59.htm

[17] http://www.ftc.gov/infosecurity

the practice has been around for a long time. Criminals contact businesses and impersonate their account holders, in order to obtain customer account records. The Commission is currently pursuing complaints against companies and individuals that allegedly obtained detailed telephone records and call information through false pretenses, in some cases posing as a consumer and convincing phone company personnel to send them the records. Employee training should emphasize proper procedures to verify the identity of individuals seeking to obtain business records.

Fourth, Pitch It. You have to make a decision on how to dispose of your information in a secure and timely fashion. Determine how long you need to retain information and then make a schedule for disposing of it.

Too many data breaches have involved information companies no longer needed. Our brochure suggests alternatives for destruction and disposal.

Finally – Plan Ahead. Because security can never be perfect, the last step in creating a sound information security program is to develop a plan for responding to data breaches. Having a plan in place beforehand helps you mitigate effects quickly and in an organized fashion. The FTC provides information to help you determine when it is appropriate to notify consumers their information has been compromised, as well as a model notification letter.

VI. Service Providers

The Safeguards Rule also requires companies to oversee their service providers. You must take reasonable steps to choose and retain service providers that can maintain appropriate safeguards for customer information, and require by contract that they implement and maintain safeguards standards.

Before outsourcing any business function – payroll, web hosting, customer call center operations, or data processing – investigate the company's data security practices and compare their standards to yours. This applies whether you are outsourcing across town or across continents.

When you are satisfied that the service provider can maintain appropriate safeguards for your customer information, memorialize these standards in your contract. You should also consider including contract provisions that build in the flexibility to revisit standards as threats and technology evolve. After the relationship has been established, include a review of your service provider in the ongoing review of your own security plan.

VII. Conclusion

Creating an effective security plan and fostering a "culture of security" is not complicated, but it does require a commitment. A commitment to security is not only good for consumers, it's just good business. A recent survey by Ponemon Institute found that the average data breach costs a business about $4.8 million, and $180 per lost customer record.[18] And that's not the end of the loss. Consumers whose information is compromised lose confidence in the company and may take their business elsewhere. One survey found that 20% of consumers who receive a breach notice terminate their relationship with the company, and another 40% say they might.[19]

There is no such thing as perfect security. But any business that maintains personal

---

[18] http://www.pgp.com/newsroom/mediareleases/2006/ponemon.html

[19] *Id.*

information about consumers must be proactive in protecting it. I hope my message today has been helpful to you. Working together we can give consumers access to the American dream. Thank you.