Federal Trade Commission

Remarks of FTC Chairman Deborah Platt Majoras [1]
ID Theft and Cyber-crime: Where Thieves
Victims, Industry and Government Intersect
San Francisco, CA
February 6, 2007

"The FTC: Promoting a Culture of Security for Sensitive Personal Information"

I. Introduction

Thank you so very much, Orson. I am deeply honored to receive this award from RSA. And to have it presented by my dear friend, Orson Swindle, a national hero who taught me a great deal about how to do my job, is a genuine treat. I accept this recognition, though, on behalf of the staff at the Federal Trade Commission. Friends, I understand why it is so easy to bash Washington and federal workers; many make us an easy target. But I wish you could see what I have had the good fortune to see for the last two and a half years at the FTC: a group of talented, creative, balanced public servants who work tirelessly for the consumers of this great nation – not for recognition and certainly not for high salaries; they do it because they understand that our unique and highly effective economic system only works when consumers have confidence in it, and they know that we can make a positive difference. We so appreciate that you have recognized our work, and you have my word that we will continue moving forward in our mission.

---

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

II. The Federal Trade Commission

The FTC is a relatively small law enforcement agency with 1,000 lawyers, economists and support staff. There are five Commissioners, each appointed by the President and confirmed by the Senate. Despite our small size, the FTC has a very broad mandate: it is the United States' primary consumer protection agency *and* it is charged with promoting competition through enforcement of the country's antitrust laws. Our integrated approach to competition and consumer protection helps to provide a safe and well-lit marketplace for all consumers and legitimate businesses.

In fulfilling its consumer protection mandate, the Commission enforces a number of specific statutes, including the Children's Online Privacy Protection Act and the Fair Credit Reporting Act. But our primary authority derives from Section 5 of the FTC Act, which empowers the Commission to take action against deceptive and unfair practices in or affecting commerce. The flexible nature of our Section 5 authority allows the Commission to protect consumers and competition from conduct that has not been specifically addressed through other legislation. As such, we are often at the forefront of new markets, new technologies, and unfortunately, new illegal practices.

The explosive growth of the Internet and the development of sophisticated computer systems and databases have made it easier than ever for companies to gather and use information about their customers. These new information systems provide tremendous benefits for consumers, who can contact customer service hotlines 24-hours-a-day, easily access credit, and shop whenever and wherever it is convenient for them. At the same time, if we do not protect

sensitive information adequately, consumers can be harmed and lose confidence in the marketplace. The balance must be carefully struck: ask consumers if they care about privacy, and you will get a resounding "yes;" ask consumers if they will tolerate being inconvenienced, and you will get a resounding "no." This is our shared challenge.

Identity theft – a term that ten years ago had not entered common parlance – has become a significant consumer privacy concern in our information-based economy. In 1998, the Identity Theft Assumption and Deterrence Act ("the Identity Theft Act") assigned the FTC a unique role in combating identity theft and coordinating government efforts.[2] While we cannot prosecute the crime because we have only civil jurisdiction, we receive 15,000 to 20,000 consumer communications per week and maintain the Identity Theft Data Clearinghouse, a centralized database of victim complaints used by 1,300 law enforcement agencies. We also assist victims and consumers who wish to avoid becoming victims by providing information; educate businesses on sound security practices; and assist in training local law enforcement officials on how to handle this crime and its victims.

A consumer from Los Angeles recently contacted the FTC and reported that his employer had experienced a data breach, in which the consumer's employee records, including Social Security number, were compromised. An identity thief opened five credit card accounts in the consumer's name, resulting in thousands of dollars in charges. In addition, the thief deposited a fraudulent $2,500 check into the consumer's checking account and immediately withdrew $1,900. Of course the check bounced, resulting in the consumer losing the $1,900. In the month since discovering the theft, this consumer has spent literally hundreds of hours trying to resolve

[2] Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028).

this issue. In another incident reported to the FTC, an Indianapolis woman had at least nine credit card accounts opened in her name, with more than $9,000 in charges in one month's time. Regrettably, these two examples, involving thousands of dollars in fraudulent charges and significant expenditures of time, are all too typical for identity theft victims. Although there is a debate about the precise number of identity theft victims each year, there is no question that there are far too many and that this crime imposes profound financial and emotional tolls on its consumer victims and is highly costly for businesses.

III. FTC's ID Theft Strategy: Coordination, Outreach, and Law Enforcement

The Commission's ultimate goal is, of course, to protect consumers from identity theft. But with perpetrators employing a seemingly endless number of techniques – from high tech phishing to low tech dumpster diving – achieving this goal is a substantial challenge. By necessity, our approach is creative and multi-faceted. For those in the audience who share my love of sports, our approach can be seen as a combination of various defensive schemes. The Commission combines a "zone defense," through our cooperative efforts as part of the interagency Identity Theft Task Force; with a "prevent defense," through our consumer and business education; and adds a "full-court press," in the form of aggressive law enforcement actions. I will highlight the key elements of each "defense" and then lay out some practical principles that can be applied by those in the private sector.

A. Identity Theft Task Force

In 2006, President Bush issued an Executive Order establishing the Federal Identity Theft Task Force, which is charged with developing a comprehensive national strategy to combat identity theft. The President directed the Task Force to make recommendations on ways to

improve the effectiveness and efficiency of the federal government's efforts in the areas of identity theft awareness, prevention, detection, and prosecution. The Task Force, which is comprised of 18 federal agencies, is chaired by Attorney General Gonzales and co-chaired by me. Each member of the Task Force brings a particular expertise in a substantive area or "zone" in the fight against identity theft.

Drawing upon each member's zone of expertise, in September, the Task Force issued a series of interim recommendations.[3] These recommendations include: development of government-wide guidance addressing whether and how to provide notice to individuals in the event of a government agency data breach and the development of a universal police report that identity theft victims can use to present their case to creditors and credit reporting agencies. Following issuance of the interim recommendations, the Task Force solicited public comments to supplement its research and analysis, and to identify areas where additional recommendations may be warranted.[4] The Task Force asked for comments on, among other things, whether there is a need for a comprehensive analysis of the private sector's use of Social Security numbers.

We received approximately 150 comments before the comment period closed on January 19. While I cannot address any specific public comments at this time, I can note generally that many concerned the use and, in some instances, the overuse of Social Security numbers, which are the most valuable piece of consumer information for identity thieves. Some comments suggest ways that less valuable identifiers might be used in their place. Other comments, while

---

[3] *See* FTC Press Release, *Identity Theft Task Force Announces Interim Recommendations* (Sept. 19, 2006), *available at* http://www.ftc.gov/opa/2006/09/idtheft.htm.

[4] *See* FTC Press Release, *Identity Theft Task Force Seeks Public Comment* (Dec. 26, 2006), *available at* http://www.ftc.gov/opa/2006/12/fyi0688.htm.

recognizing that alternate identifiers could potentially work, point to the value of Social Security numbers in matching consumers to their information and how such matching can, in fact, prevent fraud. Clearly, the issue of the how to properly use Social Security numbers is an important one for both government and the private sector. This Spring, the FTC will host a workshop to explore better methods for authenticating individuals, as limitations in current authentication methods have created opportunities for identity thieves to open new accounts and to use stolen identities. We anticipate publishing a Federal Register notice on this important workshop in the very near future and encourage your participation.

In addition, the Task Force received many comments stressing the need to increase the prosecution of identity theft, and a number of submissions discussing the issue of national standards for data security. The Task Force is in the process of reviewing the comments and preparing a final strategic plan and recommendations.

B. Consumer and Business Outreach

The FTC has long been a leader in educating consumers and businesses about identity theft. The Commission guides consumers and business on how to avoid identity theft in the first place (thus, my reference to it as "prevent defense").

Our premier nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend,"[5] was launched last year. The message for consumers is that they can:

- DETER identity thieves by safeguarding their personal information;

[5] *See* FTC Press Release, *FTC Launches Nationwide Id Theft Education Campaign* (May 10, 2006), *available at* http://www.ftc.gov/opa/2006/05/ddd.htm.

- DETECT suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and
- DEFEND against ID theft as soon as they suspect it. Quick action is essential.

Our tools for this campaign include not only direct-to-consumer brochures, but also materials that others can use to extend the reach of this education. We have created identity theft training kits, which employers, community groups, members of Congress and others can use to educate their constituencies. The kits contain a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video that organizations can use to educate their employees, their customers, and their communities about identity theft.

The Deter, Detect, Defend campaign has been very popular – we have distributed more than 1.5 million brochures and 30,000 kits. And we have formed many partnerships to help us broaden our reach. For example, the National Association of Realtors, which has 1.2 million members, partnered with the FTC to educate homebuyers. And the U.S. Postal Inspection Service just started a large-scale outreach campaign that is placing the FTC's educational materials on subway cars in Washington D.C., New York, Chicago, and San Francisco. Indeed, just this week, posters started appearing on the BART and MUNI systems. U.S. Postal is also placing paid advertising in college newspapers and on campuses around the country, including San Jose State, Stanford, and U.C. Berkeley. I hope you will consider using these materials within your organizations. Information about this education campaign – and all of the necessary materials – are on our website, www.ftc.gov. All you have to do is click on the link on the main page that says "Avoid ID Theft."

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[6] The website provides information on specific topics such as phishing, spyware, and spam. OnGuardOnLine was developed in partnership with other government agencies, the technology sector, and organizations like the SANS Institute, which I understand is offering tutorials at this conference. OnGuardOnline is branded independently of the FTC, and we did that for a reason: We want other organizations to make the information their own and to disseminate it in ways that reach the most people and suit their particular business. Since its launch in late 2005, OnGuardOnLine has attracted more than 3 million visits.

As you can probably see, I put a lot of stock in consumer education. An educated consumer is an empowered consumer, and this year's theme for National Consumer Protection Week (which is this week), sponsored by the FTC in cooperation with hundreds of federal, state, and local agencies and national advocacy organizations, is "Read Up and Reach Out. Be an Informed Consumer."[7] We are working with private sector entities on several outreach events as part of National Consumer Protection Week. For example, PayPal is working with us to conduct an online workshop this Friday about phishing, online auctions, and online shopping. Ebay is posting a video blog with a PayPal employee who is promoting OnguardOnline as well. These are the kinds of partnerships that we welcome.

---

[6] *See* FTC Press Release, *FTC and Partners Urge Consumers to Be OnGuard Online* (Sept. 27, 2005), *available at* http://www.ftc.gov/opa/2005/09/onguardonline.htm.

[7] *See* FTC Press Release, *National Consumer Protection Week: A Time to Read Up and Reach Out* (Feb. 5, 2007), *available at* http://www.ftc.gov/opa/2007/02/ncpw.htm.

The FTC's prevent defense also includes business-focused outreach that offers guidance on how organizations can protect their customers' personal data. We offer advice for businesses on reducing risks to their computer systems, and for example, a publication, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business*, which gives tips on managing data compromises and guidance on when it would be appropriate for an entity to notify law enforcement and consumers in the event of a breach of personal information. And in the very near future, the FTC will publish a general data security business education guide, designed to assist different types of businesses in addressing data security issues.

All of these materials are available in English and in Spanish. To date, the FTC has distributed more than 22 million publications on identity theft.

C. Law Enforcement

As you probably know, the Commission's multifaceted approach to combating identity theft also includes strong law enforcement against companies that fail to take reasonable steps to protect sensitive consumer information.

The news is full of reports detailing incidents in which the security of highly sensitive consumer information – Social Security numbers, financial account records, health information – has been breached. There is no doubt that there is no perfect security and sometimes even responsible security measures will not stop a thief. Nonetheless, companies and organizations that maintain sensitive consumer data must ensure that they have reasonable and appropriate systems in place, or they certainly will open the door to identify theft. Those who have failed to take reasonable security measures have faced the Commission's "full court press" of aggressive law enforcement. Since 2001, the FTC has brought 14 enforcement cases against businesses that

have failed to provide reasonable data security.[8] These enforcement actions can provide some lessons for businesses.

First, if you make claims about data security, be sure that they are accurate. The Commission has brought several cases against companies that allegedly misrepresented their own security procedures. In actions against Microsoft, Petco, and Tower Records, the FTC challenged claims on the companies' websites that each had strong security procedures in place to protect consumer information. The FTC alleged that, contrary to these claims, the companies did not have even the most basic security measures in place.

Second, be aware of well-known and common security threats and protect against them. In many of our cases, we alleged that companies failed to protect their customer information from a simple and well-known type of attack – an SQL injection – to install hacker tools on the companies' computer networks. In other cases, we have challenged failures to protect data from obvious low-tech security threats such as dumpster diving. For example, we sued a mortgage company that had, among other things, thrown consumer loan files into a dumpster.

Third, know with whom you are sharing your customers' sensitive information. Perhaps our most well-known security case was against ChoicePoint, which sold 160,000 consumer files to identity thieves posing as clients. In its complaint, the Commission alleged that ChoicePoint lacked reasonable procedures to verify the legitimacy of its customers.[9]

---

[8] *See generally* FTC Privacy Initiatives, *available at* http://www.ftc.gov/privacy.

[9] *See* FTC Press Release, *ChoicePoint Settles Data Security Breach Charges; To Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* (Jan. 26, 2006), *available at* http://www.ftc.gov/opa/2006/01/choicepoint.htm. In settling the matter, ChoicePoint agreed to pay a $10 million penalty and another $5 million to compensate identity theft victims. The Commission has mailed more than 1,400 claims forms to possible victims and has created a

Fourth, do not retain sensitive consumer information that you do not need. In cases we announced last year against BJ's Warehouse and DSW Shoe Warehouse, the companies stored full magnetic stripe information unnecessarily – long after the time of the transaction, when the companies no longer had a business need for the information. The magnetic stripe information was unencrypted and had weak access controls. As a result, thieves were able to hack into a single store's database and from there into the company's central database, where they obtained hundreds of thousands of credit card numbers and security codes.

Ultimately, all of our data security cases stand for the basic proposition that companies must maintain reasonable and appropriate measures to protect sensitive consumer information. The standard is process-oriented, rather than technology-oriented, recognizing that risks, technologies, and circumstances change over time, and that a specific technical standard would soon be obsolete – and might also stifle innovation. To return to the sports analogy, good data security procedures must be flexible and agile enough to react to the game plan of your opponent - in this case, the identity thief. As the Colts demonstrated in winning the Superbowl this weekend, you can't just doggedly stick to your original playbook – you need to make mid-game adjustments as necessary. Similarly, data security is a process – in this age of rapidly changing technology, it simply does not make sense to have a set of rigid, hard-and-fast rules in this area.

Moreover, there is no one-size-fits-all, cookie-cutter plan that will work for all businesses. Any security plan should be adapted to the size and nature of the business, the

---

website where consumers can download claims forms and obtain information about the claims process.

nature of the information the business maintains, the security tools that are available, and the security risks the business is likely to face.

I can assure you that none of the cases we have brought has been a close call – in each case, vulnerabilities were multiple and systematic, and simple, readily available, low cost, measures were available to prevent them. Further, the violation alleged in each of these cases was not the breach itself, but the failure to take reasonable precautions. The standard is not perfection; it is reasonableness. I was always taught to practice what I teach, and I can tell you that the FTC uses the same "reasonableness standard" in protecting the security of the data we collect and maintain. Marc Groman, the FTC's Chief Privacy Officer, is participating in the round table session this afternoon, and he will be able to discuss some of the steps the Commission has taken to ensure that our own house is in order.

As we move ahead in our enforcement program, we will continue to implement the identity theft provisions of the Fair and Accurate Credit Transactions Act ("FACT Act"), a law that amended the Fair Credit Reporting Act. These provisions establish a number of new rights and tools for consumers to help them avoid identity theft, and to restore their good names when they are victimized, including the right to obtain a free credit report annually; the right to put a fraud alert on a credit file; and the right to obtain underlying documentation for transactions that may have resulted from identity theft.

Additionally, the law requires sellers to truncate credit card numbers on receipts and requires companies to dispose of credit report information in a secure manner. Because these provisions have been implemented fairly recently, the Commission is keeping a close eye on

their effectiveness in fighting identity theft as well as the extent to which covered entities are complying with their obligations to consumers.

In addition, the FTC and the federal bank regulators are hard at work on the so-called "Identity Theft Red Flags" rule, which is required under the FACT Act. Once promulgated, this rule will require businesses that maintain personal consumer information to implement procedures to identify signs of possible identity theft.

IV. BEYOND IDENTITY THEFT

There are two other areas of consumer fraud that I think are particularly germane to a discussion of the Commission's efforts to protect the security of consumer information: telephone records pretexting and spyware.

A. Phone Pretexting

Phone pretexting, of course, is the short-hand term used to describe the use of false pretenses to obtain sensitive phone records, including lists of calls made and the dates and duration of such calls. The phone records are then sold to third parties without the knowledge or consent of the actual account holder. In a typical scenario, a pretexter calls the consumer's telephone company, pretends to be the consumer, and asks for his recent phone bill to be faxed to him. Another technique includes opening an online account for the subscriber and accessing the records online. This disturbing practice was made infamous last fall with the well-publicized Hewlett-Packard case.

This past May, even before the Hewlett-Packard pretexting story became national news, the Commission filed five cases against Web-based operations that obtained and sold consumers' confidential telephone records to third parties. The FTC's complaints allege that the

unauthorized sale of phone records is an unfair practice in violation of the FTC Act and seek a permanent halt to the sale of the phone records. The Commission has settled one of these cases and secured a ban on obtaining or selling phone records and a prohibition against pretexting to obtain other consumer personal information. Additionally, the defendants must give up profits made from their sale of phone records.

The Commission's efforts against phone pretexting are ongoing. In addition to our own pending cases and investigations, on January 12, 2007, President Bush signed into law the Telephone Records and Privacy Protection Act, which criminalizes obtaining confidential records by making false statements to a telephone service provider. In light of this new law, the Commission is likely to develop criminal law enforcement referrals.

B. Spyware

The Commission has brought nine spyware enforcement actions in the past two years. These actions have reaffirmed three key principles: First, a consumer's computer belongs to him or her, not the software distributor. Second, buried disclosures do not work, just as they have never worked in more traditional areas of commerce. And third, if a distributor puts a program on a consumer's computer that the consumer does not want, the consumer must be able to uninstall or disable it.

The Commission illustrated these principles in its most recent spyware settlement with Zango, Inc., formerly known as 180solutions.[10] Zango provides advertising software programs, or adware, that monitor consumers' Internet use in order to display targeted pop-up ads. The

[10] *See* FTC Press Release, *Zango, Inc. Settles FTC Charges* (Nov. 3, 2006), *available at* http://www.ftc.gov/opa/2006/11/zango.htm.

consent order settles allegations that the company installed its advertising software programs on consumers' computers without adequate notice or consent. Zango's distributors frequently offered consumers free programs or software, such as screensavers, peer-to-peer file sharing software, and games, without disclosing that downloading it would also result in installation of Zango's adware. In other instances, Zango's third-party distributors exploited security vulnerabilities in Web browsers to install the adware via "drive-by" downloads. As a result, millions of consumers received pop-up ads without knowing why and had their Internet use monitored without their knowledge.

Moreover, the company deliberately made these adware programs difficult for consumers to identify, locate, and remove from their computers so consumers were stuck with them no matter how they tried to get rid of them. The company used its adware to send billions of pop-up ads over several years. As part of the settlement, Zango agreed to disgorge $3 million in ill-gotten gains derived from its past actions. The company also agreed to injunctive provisions that will protect consumers against these practices in the future.

In another recent case, the Commission persuaded the U.S. District Court for Nevada to shut down the Media Motor spyware program operated by ERG Ventures, LLC, and its affiliates.[11] The Commission complaint charged that the defendants tricked consumers into downloading malevolent software by hiding the Media Motor program within seemingly innocuous free software, including screensavers and video files. Once installed, the Media Motor program downloaded "malware" that changed consumers' home pages, added difficult-to-

[11] *See* FTC Press Release, *Court Shuts Down Media Motor Spyware Operation* (Nov. 13, 2006), *available at* http://www.ftc.gov/opa/2006/11/mediamotor.htm.

remove toolbars, tracked Internet activity, generated disruptive and sometimes pornographic pop-up ads, added advertising icons, altered browser settings, degraded computer performance, and attacked consumers' anti-spyware and anti-virus software.

V. CONCLUSION

All organizations, as well as the consumers we serve, must contribute to creating and maintaining a culture of security for our sensitive personal information. If we are to achieve the full benefits of the information age, we cannot fall short. The Federal Trade Commission will continue our efforts, and we look forward to working with all of you. Thank you again for the opportunity to speak to you today.