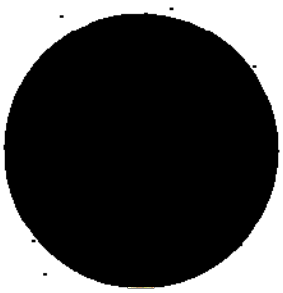

Federal Trade Commission

Remarks of Chairman Deborah Platt Majoras[1]

Protecting Consumer Information in the 21st Century: The FTC's Principled Approach

The Progress and Freedom Foundation, Securing the Internet Project

gigabytes of data. And technological developments – announced at a dizzying pace – suggest that "We ain't seen nothin' yet." This is good news for the marketplace and good news for consumers, both here and abroad. With many great innovations, however, come risks. There always are those who for financial gain, or simply for thrills, seek to exploit advancements in technology. Security threats lurk in every digital nook and cranny of the Internet.

As today's agenda suggests, we all have a role to play in the quest for a safer and more secure Internet and in the widespread adoption of a "culture of security." The FTC has made the protection of consumers' privacy, on and off-line, a priority. Through bringing more than a dozen recent law enforcement actions, we are grabbing the attention of those that hold consumers' sensitive information and raising their standards for security. But law enforcement alone will not suffi

those risks, set up a system to implement protections, and review and possibly amend the policies periodically, because risks evolve over time.

When evaluating the reasonableness of a company's information security program, even outside of the Gramm-Leach-Bliley context, the Safeguards Rule principles are the touchstone. In our investigations, we look at the overall security system that the firm has implemented and its *reasonableness* in light of the size and nature of the business, the nature of the information it maintains, the security tools that are available, and the security risks it faces.

I emphasize that the standard is "reasonableness," not perfection. Thus, the fact that a company suffered a breach does not, in and of itself, establish that its practices were unreasonable, although it could be evidence of that fact. In many investigations, the staff has concluded that, although a breach occurred, the company did have reasonable procedures in place to safeguard the data.

B. Overview of Law Enforcement Actions: The Data Security Thirteen

The best way to ensure that consumers' data receives the protection it deserves is to have clear, workable standards, supported by aggressive enforcement. Over the past 12 months, the FTC has deployed the agency's full arsenal of statutory tools to bring cases against companies that failed to implement reasonable measures to protect sensitive consumer information. The Commission's enforcement tools derive from Section 5 of the FTC Act,[3] which prohibits unfair or deceptive acts or practices, the Safeguards Rule, and the Fair Credit Reporting Act ("FCRA").[4] Today, the Commission announced our 13th case involving data security, Nations Title Agency. NTA is a privately-held company that provides real-estate related services through 57 subsidiaries in 20 states and that promised consumers that it maintained "physical,

electronic and procedural safeguards." Although many of our data security cases emphasize high-tech security issues, this case serves as a reminder not only that securing high-tech data is essential, but that we cannot forget the low-tech. Reasonable security practices include both. In this case, we allege that the respondents failed to provide reasonable and appropriate security for consumers' personal information, and that on at least one occasion, a hacker – using a common website attack – was able to obtain access to the subsidiaries' computer network. In addition, we allege that one of NTA's subsidiaries disposed of documents containing personal consumer information by simply tossing the documents into an unsecured dumpster. The complaint states claims for violations of the GLB Safeguards and Privacy Rules and under Section 5 of the FTC Act. Respondents have agreed to settle the charges by entering into a Consent Order that requires them to implement a comprehensive security program and obtain a third-party audit showing compliance.

The Commission did not allege violations of the FACTA Disposal Rule, which requires businesses and individuals to take reasonable and appropriate measures to dispose of sensitive information derived from consumer reports, because the dumpster incident occurred prior to the effective date of that Rule. But going forward, I think you can safely assume that tossing personal consumer report information into an unsecured dumpster runs afoul of the Disposal Rule.

Unfortunately, the recent investigations have shown us that data security has been surprisingly lax in a large number of companies. No one need worry that the FTC is looking for "perfect" security, or that we are developing a de facto strict liability standard for when a breach occurs, because the cases we have brought have not been close calls. The ChoicePoint high-

profile breach that occurred last year provides an example.[5] In the resulting case, we alleged that consumer data broker, ChoicePoint, Inc., failed to use reasonable procedures to screen prospective subscribers and that these failures allowed identity thieves to obtain access to the personal information of more than 160,000 consumers, including nearly 10,000 consumer reports, and to commit identity theft. For example, the company allegedly approved as customers individuals who lied about their credentials, used commercial mail drops as business addresses, and faxed multiple applications from nearby public commercial locations. The Commission obtained $10 million in civil penalties for the FCRA violations – the highest civil

cause substantial injury to consumers; (2) are not outweighed by countervailing benefits to consumers or competition; and (3) cause injury that consumers could not have reasonably avoided.[7] In short, the modern view of "unfairness" is a flexible and rational legal standard that allows the Commission to weigh the harms caused to consumers against the cost of preventing them.

The FTC's 2006 Chairman's Annual Report states that uncertainty is "the primary enemy of efficiency in law enforcement." The FTC has worked to increase the clarity of our legal standards and that will continue. The primary goal of our law enforcement efforts is not to rack up big cases and big fines. Rather, it is to push industry to develop reasonable security practices that consumers can count on.

Looking at the unfairness cases, the unfair act at issue is the failure to implement and maintain reasonable and appropriate measures to safeguard consumers' sensitive information.[8] In each case, the FTC alleged that the companies engaged in a number of activities, taken together, that failed to provide reasonable security for sensitive consumer information. In the case against BJ's Warehouse, for example, the FTC alleged that the company: (1) failed to encrypt sensitive data; (2) created unnecessary risks to the information by storing it for up to 30 days even when it no longer needed the information; (3) stored the information in files that could be accessed easily by an unauthorized party; (4) failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and (5) failed to monitor and detect unauthorized access to networks or to conduct security investigations.[9] The allegations in the DSW and CardSystems cases are similar – the respondents engaged in a number of practices, *taken together*, that failed to supply reasonable security for sensitive consumer information.[10]

Each investigation revealed that the respondents had a number of security failures. While any one of the failures may have been a problem, combined, they created an open invitation for a cyberheist.

1. Substantial Consumer Injury – The Primary Focus of Unfairness

The first premise of the unfairness analysis provides that in order for an act or practice to be unfair, the consumer injury must be substantial. This means the injury must be real. Some have argued that there is no direct injury to consumers caused by the failure to implement reasonable procedures to protect information. I disagree. Consider the allegations against BJ's, DSW, and CardSystems. In all three cases, the FTC alleged that an unauthorized party obtained access to credit and debit card information.

What is the substantial injury to American consumers? First, millions of dollars of fraudulent purchases were made using personal information obtained from the companies' computer networks. Some customers may end up liable for some of these fraudulent purchases, particularly if they failed to spot fraudulent purchases on their statements in a timely manner. In addition, some customers experienced substantial injury in the form of inconvenience and time spent dealing with the blocking and re-issuance of their credit and debit cards.[11] The banking and credit card system also experienced staggering costs associated with blocking and reissuing cards that were or may have been compromised, as well as increasing fraud monitoring efforts. In some cases, issuing banks may pass on to customers costs associated with the fraudulent purchases that the banks do not recover.

And in DSW, we alleged that an intruder stole not only the credit and debit card information of more than 1.4 million consumers, but the checking account and driver's license

data of more than 96,000 consumers. In that case, consumers whose checking accounts were compromised incurred substantial costs closing accounts and opening new accounts, including the costs of ordering new checks and penalties for bounced checks.

These harms to consumers are neither trivial nor speculative. They are real and substantial. Just ask any victim of identity theft.

2. Countervailing Benefits

Once we determine that there is substantial injury, the next step is to determine whether the injury is outweighed by countervailing benefits to consumers or competition. This is a cost-benefit analysis, meaning we must compare the injury to consumers and competition to the cost the defendant would have incurred to prevent it. The Commission recognizes that "most business practices entail a mixture of economic and other costs and benefits for purchasers,"[12] and will not find that a practice unfairly injures consumers unless it is injurious in its net effects. For example, perfect security, if it existed, would come at such a high cost that the failure to have perfect security would not violate the Commission's unfairness standard – unless, perhaps, you are guarding the secret formula to develop nuclear weapons.[13] The kinds of security failures alleged in the FTC's unfairness cases are so fundamental that the scale decidedly tips against any potential benefits.

In BJ's, DSW, and CardSystems, the alleged failures to adopt reasonable security measures provided no cognizable offsetting benefits to consumers or competition. In each case, the security vulnerabilities we alleged were well-known within the information technology industry, and they could have been prevented by simple, readily available, low-cost measures. Instead, the companies left their digital doors open. Indeed, we alleged that the companies did

not even have a business reason for storing consumers' personal information in the first place.

3. Reasonably Avoidable Injury

Finally, for an act or practice to be unfair, the injury must be one that consumers could not reasonably avoid. Through this analysis, the FTC does not second-guess the wisdom of particular consumer decisions but rather attacks those practices that prevent consumers from effectively making their own choices.[14] "If consumers could have made a different choice, but did not, the Commission should respect that choice."[15]

In the cases we have brought, consumers could not reasonably have avoided the harm caused by respondents' security failures. With respect to DSW and BJ's, customers could not know that their personal information was vulnerable on respondents' computer networks, and thus had no reason to avoid using their credit and debit cards at these stores. Further, after providing their information to BJ's or DSW, customers could not prevent the breach from occurring. Finally, there was nothing that customers could do to avoid the resulting inconvenience and time spent dealing with the actual or potential compromise of their personal information. And in the case of payment processor CardSystems, consumers did not even know that CardSystems processed their transactions, let alone that it stored their personal information on its computer network, or left their information vulnerable.

At bottom, all of our data security cases, whether based on conduct alleged to be unfair, on a violation of the Safeguards Rule,[16] or on a deceptive practice[17] stand for the proposition that record keepers must protect sensitive consumer information. Companies must take information security seriously, integrate it into their day-to-day operations, and remain aggressive in identifying and addressing risks. Many companies already have shown leadership on these

issues, and I applaud them. But others have failed to implement basic information security procedures.

Today, creating a "culture of security" is good business. Sometimes I hear from corporate privacy officials that they have a difficult time convincing senior management to invest in security because there is no immediate "return on investment." Such thinking is shortsighted. Consider the cost to your business if it becomes the latest news headline after suffering a data breach. Worse yet, consider the costs if consumers lose all confidence in e-commerce or the use of credit cards. Consumer information is the currency of our information economy. Just as we know that businesses keep their cash safe, we must insist that they keep consumers' sensitive information safe.

It is not the role of the FTC to determine which type of lock to install on a door or which security program to install on a computer network. Individual companies must make these decisions based on an individual assessment of risks. Our cases recognize that security is an ongoing, individualized process, and not a set of rigid technical standards. And this is not a game of "cybersecurity gotcha" – we are not trying to catch companies with their digital pants down; rather, we are trying to encourage companies to put their data security defenses up.

IV. Consumer and Business Education

Innovative and timely consumer education is a critical element in building a security culture. The hallmark of our cybersecurity campaign is OnGuardOnline.gov, an innovative multimedia website designed to educate consumers about basic computer security practices. This tool, which was developed through a partnership with cybersecurity experts, consumer advocates, online marketers, and other federal agencies, is a great example of public-private

cooperation.

The campaign is built around seven tips about online safety that will remain relevant even as technology evolves.[18] In addition, the site currently hosts modules on specific topics, such as phishing, spyware, and spam, which include articles, videos, and engaging interactive quizzes – in English and in Spanish.[19] The FTC will soon release our tenth module addressing the critically important issue of wireless security. We will help computer users learn about encryption and other steps they can take to secure their wireless networks, and this latest module includes a new interactive learning tool, "Invasion of the Wireless Hackers: Beat Back the Hack Attack." Finally, the website provides information about where to get help, ensuring that consumers know that they are not alone as they travel through cyberspace.

Notably, we deliberately branded OnGuardOnline independently of the FTC to encourage other organizations to make the information their own and to disseminate it in ways that reach the mo

have published a business education brochure on managing data compromises, *Information Compromise and the Risk of Identity Theft: Guidance for Your Business.*[22]

unfairness jurisdiction. The Rule, which provides a strong, but flexible requirement to make sure that information is maintained securely, only applies to customer information collected by "financial institutions." The principles embodied in the Safeguards Rule make sense for other entities that maintain sensitive consumer information. And indeed, as we have discussed this morning, to some extent they do apply to other entities through the application of the Commission's Section 5 authority. But a clear statutory requirement that companies implement and maintain appropriate safeguards would enhance the FTC's enforcement authority in this area and go a long way towards promoting a culture of security.

Second, the Commission has recommended that Congress consider whether consumers should be notified if sensitive information about them has been breached – but only if the breach creates a significant risk of identity theft. Prompt notice in appropriate circumstances can help consumers avoid or mitigate identity theft. At the same time, however, requiring notices for security breaches that pose little or no risk may create confusion and impose unnecessary costs on both businesses and consumers. Formulating the right balance is difficult, and there are different notice triggers that could be considered, with the goal of requiring notice only when it is useful to do so, that is, when there is a real risk of harm.

Third, our experience in the data breach area suggests that the ability to impose civil penalties is essential for effective law enforcement. We must send the strongest possible message that in an information economy, good security is critical. An individual company's failure to take reasonable measures to protect sensitive information impacts not only that company, but the entire system.

Finally, last June, the FTC submitted a report to Congress recommending legislation

called the US SAFE WEB Act – Undertaking Spam, Spyware, and Fraud Enforcement with Enforcers across Borders.[23] The proposed legislation would enable the FTC to share key information with foreign partners, assisting international law enforcers in pursuing security breaches in their countries that impact U.S. consumers. The legislation also would help the FTC fight deceptive spam and spyware by allowing the agency to investigate more fully messages transmitted through facilities outside the United States. The legislation has passed in the Senate.

B. Global High Tech Hearings – Exploring the Future

We will continue to educate ourselves, other policy-makers, and the public as the high-tech world propels forward. This fall, for example, the FTC will host a public forum to explore the challenges and opportunities that consumers will face in the next "Tech-ade." These high tech hearings will bring together the experts to engage in a robust dialogue on the state of technology and the future of consumer protection.

But as the saying goes, "if you want to know where you are going, it helps to reflect on where you have been." Accordingly, we first will look back at the significant consumer protection issues that emerged over the past decade. We have some tough questions to answer. Did we forecast their occurrence? Was our response effective and appropriate? And what can we learn from the past ten years?

Next, we will look forward and attempt to predict the next generation of challenges in the global marketplace. And again, we will address difficult questions. How can we best protect consumers in a marketplace that now knows no bounds, that is virtual, 24-7, and truly global?

The dialogue already has begun. Our request for suggested agenda items generated scores of thoughtful suggestions from the full spectrum of interested parties. I invite all of you

to attend this forum and to be a part of the process.

VII. Global Issues Demand Global Responses

It goes without saying that the Internet and associated technology have created a global community. Globe-trotting data effortlessly crosses international boundaries, providing tremendous benefits for consumers worldwide who can now get what they want, when they want it. Similarly, and unfortunately, though, fraud and deception know no borders. Spammers, spyware operators, hackers, identity thieves, and other scam artists can strike quickly on a global scale and disappear nearly without a trace – along with their ill-gotten gains. Thus, in addition to its law enforcement and education efforts, the Commission has taken an active role in promoting cybersecurity internationally.

When I discuss the FTC's efforts in the international arena, I am reminded of that well-known saying about real estate. The three most important elements are location, location, and location. In the context of consumer protection in this globalized marketplace, the three most important elements are cooperation, cooperation, and cooperation.

The FTC is not new to international cooperation on high tech consumer protection issues. We have a proven track record with many countries around the world. For years, we have worked with colleagues in the Americas and Europe. We have worked together to develop strategies and provide one another with targeted assistance on individual investigations. But now we are reaching further. I recently traveled to Asia and met with government officials in Japan, Korea, and China, on both competition and consumer protection issues. The desire on the part of these counterpart agencies to work together with us was clear. Indeed, in China, we met with officials at agencies with which we had no prior relationship, including the Ministry of

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

[2] 15 U.S.C. § 6801(b); Standards for Safeguarding Customer Information, 16 C.F.R. Part 314 ("Safeguards Rule"), *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf.

[3] 15 U.S.C. § 45.

[4] 15 U.S.C. §§ 1681-1681x.

[5] The FTC issued a four count complaint against ChoicePoint: Counts I and II alleged violations of the FCRA, Count III alleged that ChoicePoint engaged in unfair practices in violation of Section 5 of the FTC Act, and Count IV alleged that ChoicePoint engaged in deceptive acts or practices in violation of Section 5 of the FTC Act. *United States v. ChoicePoint*, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006)

[6] Christopher Wolf, *Dazed and Confused: Data Law Disarray,* Business Week Online, April 2, 2006, *available at* http://www.businessweek.com/technology/content/apr2006/tc20060403_290411.htm?campaign_id=search.

[7] 15 U.S.C. § 45(n).

[8] Other practices challenged by the Commission as unfair include unilateral breach of contract, unauthorized billing, excessive mousetrapping, email spoofing, spyware, and pretexting. [*insert case citations*]

[9] *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. C-4148 (Sept. 20, 2005).

[10] *In the Matter of DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006); *In the Matter of CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (proposed settlement posted for public comment on Feb. 23, 2006);.

[11] In particular, many customers temporarily lost use of their accounts; many first learned that their cards had been blocked when an authorization request for a purchase was declined; and many had to change account numbers and personal identification numbers, and notify creditors making automatic charges or withdrawals on the cards of the changes.

[12] FTC Policy Statement on Unfairness, *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[13] Similarly, it would be unreasonable to expect a small local bank to employ the same security measures as Fort Knox. The potential injury to consumers or the marketplace would not justify the costs of such measures.

[14] FTC Policy Statement on Unfairness, *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

[15] J. Howard Beales, III, *The FTC's Unfairness Authority: It's Rise, Fall, and Resurrection*, (May 30, 2003), *available at* http://www.ftc.gov/speeches/beales/unfair0603.htm

[16]

http://www.ftc.gov/reports/ussafeweb/USSAFEWEB.pdf. Senator Gordon Smith introduced S. 1608, the "US SAFE WEB Act," on July 29, 2005. The Senate passed the bill by voice vote on March 16, 2006.