Remarks of J. Howard Beales, III[1]

Director, Bureau of Consumer Protection

Federal Trade Commission

before the

2003 Symposium on the Patriot Act, Consumer Privacy, and Cybercrime hosted by

The University of North Carolina's Journal of Law & Technology

September 26, 2003

Introduction

I am delighted to be here this morning. Among the many issues confronting law enforcers today, consumer privacy and cybercrime are among the most challenging. The Federal Trade Commission's role as the nation's chief consumer protection agency requires us to focus carefully on these – and a whole host of consumer protection issues – using the unique tools available to us. Even as we track trends and adopt new technologies, our fundamental mission

[1] The views expressed by Howard Beales do not necessarily reflect the views of the Federal Trade Commission or any individual Commissioner.

remains the same: ***to identify*** the most egregious forms of fraud and deception;[2] ***to bring cases***, on our own and with our law enforcement partners;[3] and ***to educate*** – ourselves about emerging issues, industry about complying with the law, and consumers about how best to protect themselves from fraud and deception.[4]

Today, I want to discuss the FTC's efforts to address consumer's concerns about personal privacy, and the critical role that online and offline security play in that program.

Fighting Internet Fraud

First let me say a word about our role in fighting one growing type of Cybercrime, consumer fraud. Although the Internet has empowered consumers with instant access to a breadth of information about products and services that would have been unimaginable 20 years ago, fraud artists have also proven adept at exploiting this new technology for their own gain. They are the ultimate "early adopters" of new technology. And, they've seized on the Internet as a ready vehicle to find victims for their scams. In fact, our consumer complaint data show that

---

[2] Consumers reach the Commission through our *Consumer Response Center* which provides phone, mail, and web-based consumer access. The complaints are stored in *Consumer Sentinel*, our web-based database of consumer fraud complaints, and an investigative cyber tool with more than 750 law enforcement agencies as members; and in the FTC's *Identity Theft Clearinghouse*, which provides victim assistance and data for law enforcers.

[3] The Commission brings cases pursuant to its authority under Section 5 of the FTC Act which prohibits unfair or deceptive acts or practices in or affecting commerce. 15 U.S.C. § 45(a). Our law enforcement efforts target fraud and deception and address the full range of consumer protection issues. In our telemarketing fraud efforts, for example, the FTC has organized and led 50 federal-state enforcement sweeps against fraudulent telemarketers since 1995, resulting in 1,725 law enforcement actions.

[4] Virtually all of the Commission's 400 consumer and business education publications are available at our comprehensive Website, www.ftc.gov. In just the last year, the Commission distributed more than 3.86 million publications, including 78,000 in Spanish, and recorded more than 15 million page views of consumer and business information on the FTC Website, including more than 250,000 on pages with Spanish information.

consumers increasingly report the Internet as the initial point of contact for fraud, and that the Internet has now outstripped the telephone as the source of first contact for fraud.[5]

Many of these frauds are simply online variations of familiar, offline scams. However, we also see more sophisticated practices that exploit the very technology of the Internet, sometimes going as far as literally taking control of the consumers' computers away from them.

To combat these new frauds, the FTC has brought over 200 Internet-related enforcement actions. This is also one of a number of areas where we are looking for ways to work closely with criminal law enforcement agencies. For example, last year the Commission sued John Zuccarini for "mousetrapping" consumers.[6] Zuccarini, registered some 6,000 domain names that were misspellings of popular websites. Surfers who looked for a site but misspelled its Web address were taken to the defendant's sites.[7] Once they arrived, Zuccarini's Websites were programmed to take control of the consumers' Internet browsers, and hold the consumers captive while they were forced to view dozens of websites advertising products such as online gambling, psychic services, and adult websites. The obstruction was so severe in this case that consumers were often forced to choose between taking up to twenty minutes to close out all of the Internet windows, or turning off their computers, and losing all of their "pre mousetrap" work.

---

[5] Complaint data, of course, may not be representative, particularly regarding the level of violations occurring. We have just completed field work on a nationally-projectable survey that will give us much better information on the incidence of fraud, and the means that fraudsters use to reach out and pluck someone.

[6] *FTC v. John Zuccarini,* No. 01-CV-4854 (E.D. Pa.).

[7] For example, Zuccarini registered 15 variations of the popular children's cartoon site, www.cartoonnetwork.com, ("cartoon netwok" instead of "cartoon network") and 41 variations on the name of teen pop star, Britney Spears.

After being sued, Mr. Zuccarini disappeared.[8] Fortunately, as a result of a cooperative working relationship between FTC attorneys and the United States Attorney's Office for the Southern District of New York, he was arrested in a south Florida hotel room.[9] At the time of his arrest, Mr. Zuccarini was surrounded by computer equipment and cash, all of which was seized by criminal authorities. He was not left empty-handed, however. A United States Postal Inspector served him with the Final Court Order in our case.

Similarly, we all know that unsolicited commercial email, or spam, is a nuisance, but we now know it is also a ready source of fraud. We are probably the only people in the country that actually like to get spam, and we are currently collecting over 100,000 spams a day that are forwarded to us from all over the country. When we looked at the content of this spam, we found that two-thirds contained clear indicia of falsity.[10] Just one example are spams selling bogus domain names. After September 11th these spams even urged consumers to "Be Patriotic! Register .USA Domains," and at one point even peddled ".God" domain names.[11] The only

---

[8] In light of this development, the Court permitted the Commission to serve Mr. Zuccarini electronically.

[9] Benjamin Weiser, *Spelling It 'Dinsey,' Children on Web Got XXX*, N.Y. TIMES, Sept. 4, 2003, § B (Late Edition), at 1. The indictment charged Zuccarini with violations of the Truth in Domain Names Act, 18 U.S.C. § 2252(B)(b), a section of the new Amber Alert law that makes it a crime to divert children to obscene material. It is the first prosecution under the statute, which President Bush signed this past spring.

[10] FTC MARKETING PRACTICES REPORT, FALSE CLAIMS IN SPAM (Apr. 30, 2003), *available at* <http://www.ftc.gov/reports/spam/030429spamreport.pdf>. Furthermore, our analysis of spam has found that it is rarely sent by established businesses. In fact, in a random sample of 114 pieces of spam, we found that none was sent by a Fortune 500 company and only one was sent by a Fortune 1000 company. Based on this sample, we can be 95% confident that less than 5 % of the 11.6 million pieces of spam in our database came from Fortune 1000 companies.

[11] *FTC v. TLD Network, Ltd.*, No. 02-C-1475 (N.D. Ill.)

trouble is, neither domain is usable on the Internet. We estimated these scammers took in more than $1 million before we got a court order shutting them down and freezing their bank accounts and other assets. And again we got help from our law enforcement partners, this time the Office of Fair Trading of the United Kingdom, where the defendants were located.[12]

Emergence of Consumer Privacy

In addition to fighting online fraud, protecting consumer privacy is a priority of the FTC's consumer protection program. Privacy has always been an important issue for American consumers. But, fueled by the development of the Internet, privacy emerged as a major consumer issue in the mid 1990s. Given the breadth and depth of the concerns, almost everyone in government wanted to do *something* about consumer privacy. *What* to do was less clear. Although consumers expressed high levels of concern about their perceived loss of privacy,[13] they also expected and relied on the benefits of our information-driven economy. For example, few consumers seem worried about the many companies that have to share their information to clear checks or, for that matter, to process ATM transactions. They generally understand that the information must be collected and shared to complete the transaction. Indeed, surveys reveal

---

[12] The U.K.'s Office of Fair Trading ("OFT") assisted the FTC staff in its investigation of the defendants and serving legal process. OFT later negotiated written assurances from defendants that they would not publish similar advertisements for the registration of domain names. *See* OFT Press Release, August 29, 2002, <http://www.oft.gov.uk/News/Press+releases/2002/PN+53-02+Misleading+domain+name+ads+stopped.htm>.

[13] That concern has been expressed in many public opinion polls. *See e.g.,* Alan F. Westin/Harris Interactive, *Privacy On and Off the Internet: What Consumers Want* (Nov. 2001); IBM/Harris Interactive, *Multi-National Consumer Privacy Survey* (Oct. 1999); Lorrie Faith Cranor et al., *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy*, AT&T Labs-Research Technical Report TR 99.4.1 (Mar. 1999).

that most Americans are "privacy pragmatists," who care about privacy but are willing to share information when they see tangible benefits and they believe care is taken to protect that information.[14]

By the time FTC Chairman Timothy Muris and I arrived at the Commission in June 2001, the agency had spent several years developing a sophisticated understanding of privacy issues through conferences and workshops. Industry, spurred by consumer interests and the Commission's activity, had begun addressing consumers' concerns, especially by posting privacy policies on commercial Websites. Nevertheless, at that time many people equated support for privacy protection as support for legislation requiring "notice, access, and choice" (otherwise known as "Fair Information Practices") before personal information was collected on the Internet.[15] That seemed to us to be an odd form of consumer protection. Why should

---

[14] According to the March 2003 Westin/Harris Interactive poll, 64% of adults polled are "privacy pragmatists" who are often willing to permit the use of their personal information if they are given a rationale and tangible benefits for such use and if they sense that safeguards are in place to prevent the misuse of their information. *See* www.harrisinteractive.com/harris_poll/index.asp?PID=365>. As discussed below, however, in a notice and choice system, most of these consumers are unlikely to take the time and effort to understand the benefits and costs of a specific sharing of information in individual transactions.

[15] In its 1998 Report, PRIVACY ONLINE: A REPORT TO CONGRESS, the FTC summarized widely-accepted principles regarding the collection, use, and dissemination of personal information, known as Fair Information Practices (FIPs): (1) **notice**: data collectors must disclose their information practices before collecting personal information from consumers; (2) **choice**: consumers must be given options about how personal information collected from them may be used for purposes beyond those for which the information was provided; (3) **access**: consumers should be able to view and contest the accuracy and completeness of data collected about them; and (4) **security**: data collectors must take reasonable steps to assure that information collected from consumers is accurate and secure from unauthorized use. The report also identified **enforcement** – the use of a reliable mechanism to impose sanctions for noncompliance with these fair information practices – as a critical ingredient in any governmental or self-regulatory program to ensure privacy online. *See* PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), *available at* www.ftc.gov/reports/privacy3/priv-23.htm.

information collected via paper and pencil be treated differently than the same information collected online? And why should legislation discriminate against the burgeoning development of e-commerce?

The New Framework

One of our first efforts was to develop a framework for addressing consumers' privacy concerns. Privacy was a new topic for us, one that we studied in-depth. We held dozens of meetings with groups with diverse perspectives on privacy – ranging from consumer groups to trade associations to information technology executives to professors. We read academic, legal, and policy literature in addition to numerous briefing memos from the FTC staff. We found widespread agreement on the importance of privacy issues and the importance of the FTC in protecting consumers' privacy.

The debate over privacy showed clearly the importance of relying on strong principles to guide an institution like the FTC through new territory. Grappling with the issues surrounding privacy required careful consideration of the basic questions of common law – why should the government protect privacy and what role should the government play in defining and enforcing privacy rules for private exchange? Strong principles were needed to ensure that if the Commission went beyond enforcing a particular contract provision to provide new "rules of the game," it would develop those rules based on a deep understanding of the issues and an appreciation of the possible harm of restricting the many consumer benefits that an information-based economy offers.

The Inadequacy of "Fair Information Practices"

One of our first steps was to evaluate the adequacy of the Fair Information Practices

("FIPs") approach to privacy protection. This is an appealing model because it is seemingly based on consumer consent, on contracts between consumers and businesses. In practice, however, consent is illusory. For most consumers, the costs of exercising the choice – although not high – are not worth the perceived benefits. Consider the billions of privacy notices sent to consumers under Gramm-Leach-Bliley. Very few consumers have exercised their right to opt-out of information sharing. Part of the problem, no doubt, is the difficulty of understanding some of the notices. Hopefully, we can improve the notices, but a more fundamental problem exists. Exercising just one opportunity to opt-out may take only a few minutes, but opting out for each of the companies you do business with would take much longer. Consumers have many other options – not to mention demands – for their time – from paying bills to getting dinner on the table to helping children with homework. Given that time is scarce and even reading the notice takes effort that could be spent elsewhere, it is not surprising that few consumers opt-out, even when it is seemingly easy.[16]

Nor is opt-in the solution. Because most consumers will not expend the time and effort to consider the choice, opt-in is only the correct default if most fully-informed consumers would refuse to share information.[17] Explaining the benefits and costs of information sharing is beyond the competence of even the best drafted short notice. We cannot *make* people focus on this, or

---

[16] Of course, some consumers may care a great deal about protecting their privacy, and be willing to make the effort to exercise choice. Under an opt-out regime, these consumers will identify themselves by opting out. In essence, only those who believe the issue is worth seriously considering bear the costs of considering the choice.

[17] Under opt-in, consumers who value highly the benefits information sharing makes possible must make the effort to exercise choice. Those who are more concerned about privacy can ignore the choice.

any other, issue. With GLB privacy notices in particular, we led people to the privacy question, and they chose not to choose.

Thus, the FIPs model has fundamental limitations. Because considering the choice imposes costs apparently in excess of the benefits for many consumers, applying the model would simply reflect inertia, rather than revealing what consumers want. Moreover, legislation codifying the principles runs the risk of unnecessarily hobbling development of the many benefits that an information-based economy could offer consumers.[18] It is hard to describe in advance technology or beneficial information uses that have not been invented or even considered.

If Fair Information Practices is not the answer to consumer concerns about privacy, what is? In contrast to the one size fits all approach in FIPS, our current approach balances the benefits of information sharing with protection of consumers from the misuse of that

---

[18] Implementing Fair Information Practices can itself require difficult distinctions. In our recent Information Flows workshop, a Senior Vice President of an international hotel company stated that a caller in Germany who wishes to make a reservation for a hotel in Washington, D.C., would probably call a reservation center in Amsterdam, which would use a computer data center in Georgia to make the reservation. The company might be pulling data from other countries as well. He noted that under the European opt-in privacy model, his company must go to great lengths to disclose to consumers that their reservation information will be transferred overseas to be processed by a computer in Atlanta. He stated that this is very costly in the aggregate, even if it only adds 5 to 10 seconds to each call. Moreover, consumers do not find this information helpful and may even find it confusing or annoying. Of course, a sensible application of FIPs leads to the conclusion that notice and choice are unnecessary in this context. But if we make an exception here, why not elsewhere? This example, and many others like it, illustrate the difficulty of making reasonable distinctions when applying FIPs in practice. The workshop transcript is available at <http://www.ftc.gov/bcp/workshops/infoflows/infoflowstranscript.pdf>.

information.[19]

Focus on Misuse of Consumer Information

Consumers benefit from legitimate uses of information; such uses do not cause their privacy concerns. They are concerned, however, that information, once collected, may be misused to harm them or disrupt their daily lives. It is these adverse consequences that drive consumer concerns about privacy. These include physical harm: certainly, parents do not want information on the whereabouts of their kids to be freely available. The misuse of information also can cause economic harm. Such harm includes denial of credit – or even a job – based on inaccurate or incomplete information. In extreme cases, the misuse of information also can lead to identity theft, our top consumer complaint category for three years in a row. Finally, the misuse of information can cause annoying, irritating, and unwanted intrusions in daily lives. These include the unwanted phone calls that disrupt dinner or the spam that clogs our computers.

Explicit Recognition of Trade-Offs

Our approach to targeting practices that involve misuse of consumer information reflects the reality that any regulation designed to protect consumer privacy involves trade-offs. Privacy is not, nor can it ever be, an absolute right. Every day, consumers make practical compromises between privacy and other desirable goals – like having our briefcase or backpack inspected at the airport or before entering a building or a sports arena. These trade-offs exist in the commercial sphere as well – where information-sharing poses risks, but also offers benefits. Our privacy agenda seeks both strong protection of privacy *and* preservation of the important

---

[19] Remarks of Timothy J. Muris, "Protecting Consumers' Privacy: 2002 and Beyond" (Oct. 4, 2001), available at www.ftc.gov/speeches/muris/privisp1002.htm.

benefits of our information economy.

Focus on Online as well as Offline

Finally, the FTC's previous efforts were primarily focused on addressing consumers' concerns about *online* data collection. If the concern is reducing the adverse consequences that can occur when information is misused, then it does not matter whether information is originally collected online or offline.[20] It simply matters if it is misused. The risk of identity theft, for example, is no less real and the consequences no different if a thief steals your credit card number from a Website or from the mailbox in front of your house. Equal treatment of information collected online or off provides better protection for consumers. Moreover, a level playing field for online and offline businesses is less likely to impede the continuing growth and development of Internet commerce.

FTC Privacy Program

For two years, we have implemented these principles through a variety of privacy initiatives – from our National Do Not Call Registry enabling consumers to stop unwanted telemarketing sales calls,[21] to our efforts to combat deceptive spam, to our enforcement and

---

[20] For example, the Commission has brought cases challenging misrepresentations about the uses of information collected in surveys of students conducted in class. *See Educational Research Center of America, Inc.*, Dkt. No. C- 4079 (May 6, 2003); *The National Research Center for College & University Admissions*, Dkt. Nos. C-4071 & C-4072 (Jan. 28, 2003).

[21] Telemarketing Sales Rule, 16 C.F.R. Part 310 (as amended December 2002).

education efforts involving financial[22] and children's privacy.[23] To achieve our goals, in each of the past two fiscal years, we have increased significantly the agency resources devoted to privacy. In Fiscal Year 2002, we increased the resources devoted to privacy issues by 60 percent. Compared to 2001, the FTC now spends several times more resources on protecting consumer privacy.

Information Security and Identity Theft

As we crafted the framework, it became clear that a key to protecting consumer privacy is protecting the security of consumer information. A great many "breaches of privacy" are actually security lapses rather than conscious decisions to share information.[24] Poor information security practices put consumer information at risk of misuse. And much of the misuse results from theft, in circumstances where no one would deliberately provide the information to the thief.

Take, for example, the relationship between identity theft, one of the most serious forms of misuse, and security. Identity theft is more widespread and pernicious than previously realized. In September, the FTC released a survey showing that, in the year preceding the

---

[22] The Commission enforces the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*, the Fair Debt Collection Practices Act, 15 U.S.C. § 1601 *et seq.*, and the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*

[23] The FTC has brought eight cases alleging violations of its Rule under the Children's Online Privacy Protection Act and obtained a total of $360,000 in civil penalties.

[24] During our initial review, our staff presented numerous press reports detailing breaches of privacy where personal information was revealed improperly. As we examined these reports, the vast majority of them appeared to be the result of erroneous or unauthorized access, rather than deliberate sharing of information. Although as discussed below, not all of these incidents are law violations, our information security program seeks to prevent misuse in circumstances where notice and choice would be ineffective.

survey, 3.23 million people – or 1.5 percent of the adult population – were victims of identity theft, with new accounts opened or other frauds committed in their name.[25] An additional 6.7 million people – or 3.19% of the adult population – were victims of account theft, in which thieves placed charges on existing accounts, usually credit cards.[26] These numbers translate to an estimated $48 billion in losses to businesses, nearly $5 billion in losses to victims, and almost 300 million hours spent trying to resolve the problem.[27] Other consequences also can be severe. Of those victims who had new accounts or other frauds in their name, 14% were the subject of a criminal investigation, 14% were named in a civil suit, and 35% were harassed by debt collectors as a result of the theft.

---

[25] The Commission's Identity Theft report, released on September 3, 2003, is available at www.ftc.gov/opa/2003/09/idtheft.htm. The FTC commissioned the survey to get a better picture of the incidence of identity theft and the impact of the crime on its victims as part of the Commission's ongoing Identity Theft program. The FTC's primary role in combating identity theft derives from the 1998 Identity Theft Assumption and Deterrence Act ("the Identity Theft Act" or "the Act"). Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified at 18 U.S.C. § 1028). The Act directed the Commission to establish the federal government's central repository for identity theft complaints, to provide victim assistance and consumer education, and to provide our identity theft complaints to law enforcement. The Commission also works extensively with industry to help victims, including providing direct advice and assistance when information has been compromised. The FTC has committed significant resources to assisting law enforcement. Investigation and prosecution not only stop the offender from corrupting another person's financial well being, but also can deter would-be identity thieves from committing the crime.

[26] Account theft is a form of identity theft because credit card numbers or other account numbers are considered a "means of identification" under the federal identity theft criminal statute. Nonetheless, it differs substantially from other forms of identity theft as used in the text. Despite its greater frequency, account theft is discovered more quickly: 40% of account theft incidents were discovered in less than one week's time compared to 17% for other forms of identity theft. In addition, account theft results in smaller losses to business ($14.7 billion compared to $32.9 billion) and to consumers ($1.2 billion compared to $3.8 billion), and less time is needed to recover per incident (60 hours compared to 15 hours).

[27] These figures are for identity theft and account theft combined.

Although a great many identity theft victims – 42%– had no idea how the thief obtained their personal information, 20 percent said the information was acquired by theft.[28] Some of this theft occurs the old fashioned way. Information stolen from mail boxes accounted for 7% of victims, and lost or stolen wallets accounted for 8%.

Other information thieves are more innovative, getting personal information directly from consumers using high-tech trickery. One such example we are combating is the practice of "phishing" for consumers' sensitive financial information.[29] In this scam, identity thieves send

---

[28] These results are based on all people who were identity theft victims in the past five years. Another 11% reported that their information was stolen during a commercial transaction, such as when a consumer rented a car.

[29] The Commission brought its first "phising" case in July 2003. *FTC v. Unnamed Party, a minor*, No. 03-5275 GHK (C.D. Cal. filed July 25, 2003). In this case, the Commission alleged that the defendant, posing as America Online, sent consumers email messages claiming that there had been a problem with the billing of their AOL account. The email falsely represented to consumers that if they did not update their billing information, they risked losing their AOL accounts and Internet access. The message directed consumers to click on a hyperlink in the body of the email to connect to the "AOL Billing Center." When consumers clicked on the link they landed on a site that contained AOL's logo, AOL's type style, AOL's colors, and links to real AOL Web pages. It appeared to be AOL's Billing Center, but in fact, the Commission alleged, the defendant had hijacked AOL's identity to steal consumers' identities. The defendant's AOL look-alike Web page directed consumers to enter the numbers from the credit card they had used to charge their AOL account. It then asked consumers to enter numbers from a new card to correct the problem. It also asked for consumers' names, mothers' maiden names, billing addresses, Social Security numbers, bank routing numbers, credit limits, personal identification numbers, and AOL screen names and passwords - the kind of data that would help the defendant plunder consumers' credit and debit card accounts and assume their identity online.
According to the Commission's complaint, the defendant used the information to charge online purchases and open accounts with PayPal. In addition, he allegedly used consumers' names and passwords to log on to AOL in their names and send more spam. Finally, the Commission alleged that he recruited others to participate in the scheme by convincing them to receive fraudulently obtained merchandise he had ordered for himself. The Commission's complaint alleged that the defendant's emails to consumers were deceptive; that defendant "pretexted" consumers' personal information in violation of the Gramm-Leach-Bliley Act's prohibition on pretexting; and that defendant's billing of consumers' accounts constituted an unfair practice in

spam that appears to originate from a company with whom the consumer already has an established relationship – such as the victim's ISP or bank. The spam message warns the consumer to update his or her "billing information," and contains links to "look-alike" Websites that are loaded with actual trademarked images so that they look like a real company's website. The scammers ask for credit card numbers, passwords, Social Security numbers, and other information, and use it to order goods or services or to obtain credit. These scammers initially seemed to target customers of large ISPs, online auction companies, and online payment providers. However, in the last six to nine months, a number of financial institutions have been targeted as well. Scammers have engaged in "phishing" by posing as entities such as Discover, Citibank, Bank of America, and Best Buy.[30] Any institution with a large number of consumer accounts is probably vulnerable to the "phishermen."

Other identity thieves exploit insider access or simply resort to garden-variety breaking and entering. Consider the widely reported TriWest[31] and TCI[32] incidents. TriWest, a health insurance provider for Department of Defense employees, experienced a burglary at its Phoenix, Arizona offices during which laptops and computer hard drives were stolen. These computers contained the names, addresses, dates of birth, and Social Security numbers (and in some cases

---

violation of Section 5 the FTC Act. The Commission obtained a stipulated permanent injunction prohibiting the defendant from engaging in these fraudulent practices.

[30] In response to the Best Buy "phishing" incident reported in June 2003, the Commission issued a consumer alert, available at www.ftc.gov/opa/2003/06/bestbuyscam.htm.

[31] Adam Clymer, *Officials Say Troops Risk Identity Theft After Burglary*, N.Y. TIMES, Jan. 12, 2003, § 1 (Late Edition), at 12.

[32] Kathy M. Kristof & John J. Goldman, *3 Charged in Identity Theft Case*, LA TIMES, Nov. 6, 2002, Main News, Part 1 (Home Edition), at 1.

credit card numbers and sensitive medical information) of about 562,000 health insurance beneficiaries.[33] In the TCI breach, 30,000 consumer credit reports were stolen when a former employee of TCI improperly used passwords and subscriber codes of TCI's corporate clients to download credit reports from credit reporting agencies' database.[34] The perpetrator of this fraud was indicted on charges of fraud and conspiracy. According to the indictment, consumer victims reported that tens of thousands of dollars in existing accounts had been depleted; new accounts had been opened without their knowledge or authorization; credit cards held in their names had been used without authorization; and their addresses had been changed at various financial institutions without their knowledge or consent.[35]

---

[33] These beneficiaries were all members of the armed services, retirees or their dependents. The breach occurred on December 14, 2002.

[34] The ex-employee, Philip Cummings, worked as a Help Desk representative at TCI, and was arrested November 2002. TCI provides software and computer equipment to credit grantors that enables them to obtain credit reports from the credit bureaus. The credit bureaus assign a unique "subscriber access code" to the credit grantors that is used, together with TCI's software or computer equipment, to obtain the credit reports. According to the U.S. Attorney's complaint, from 2000 until he was arrested in 2002, Cummings allegedly worked with others to illegally obtain the credit reports of consumers. The complaint alleges that members of the identity theft ring supplied him with Social Security numbers, and he pulled the credit reports by using passwords and subscriber codes of TCI's clients' to gain access to the credit bureaus' databases.

[35] *United States v. Philip Cummings*, No. SI 03 Cr. 109 (GBD)(S.D.N.Y. Nov. 22, 2002)(criminal complaint available at http://news.findlaw.com/hdocs/docs/crim/uscummings112202cmp.pdf Most identity theft cases are best addressed through criminal prosecution. The FTC itself has no direct criminal law enforcement authority. Under its civil law enforcement authority provided by Section 5 of the FTC Act, the Commission may, in appropriate cases, bring actions to stop practices that involve or facilitate identity theft. *See, e.g., FTC v. Assail, Inc.*, W03 CA 007 (W.D. Tex. Feb. 4, 2003) (order granting preliminary injunction) (defendants alleged to have debited consumers' bank accounts without authorization for "upsells" related to bogus credit card package) and *FTC v. Corporate Marketing Solutions, Inc.*, CIV-02 1256 PHX RCB (D. Ariz Feb. 3, 2003) (final order) (defendants "pretexted" personal information from consumers and engaged in unauthorized billing of consumers' credit cards). In addition, the FTC brought six complaints

The survey data, "phishing" scams, and the large-scale incidents of breaches put identity theft and information security in sharper focus for law enforcement, policy makers, consumers, and the media. They highlight both the value and vulnerability of personal information to determined thieves and the necessity for all participants to follow good information security practices, be they a multi-national corporation securing its network or a consumer installing a firewall on a home computer. Notwithstanding good security practices, we understand that some security breaches will occur. When they do, vigorous criminal prosecution of the information thieves and internet scammers is important. But when the breach occurs because companies failed to take reasonable steps to protect their customers' information, law enforcement action against the company may also be appropriate, and in fact, the FTC has brought a series of cases challenging such practices.

FTC Law Enforcement and Information Security

General Principles

The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce are declared unlawful."[36] The statute defines "unfair" practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[37]

---

against marketers for purporting to sell international driver's permits that could be used to facilitate identity theft. *See* www.ftc.gov/opa/2003/01/idpfinal.htm.

[36] 15 U.S.C. § 45(a)(1).

[37] 15 U.S.C. § 45(n)

Most FTC actions are based on deception, however, which the Commission and the courts have defined as a representation or omission that is likely to mislead consumers acting reasonably in the circumstances about a material issue.[38]

In addition, the Commission enforces a variety of specific consumer protection statutes that prohibit specifically-defined trade practices and generally specify that violations are to be treated as if they were "unfair or deceptive" acts or practices under Section 5(a).[39] The Commission enforces the substantive requirements of consumer protection law through both administrative and judicial processes.[40]

To date, the Commission's security cases have been based on deception.[41] Companies

---

[38] Letter from FTC to Hon. John D. Dingell, Chairman, Subcommittee on Oversight and Investigations (Oct. 14, 1983), reprinted in appendix to *Cliffdale Associates, Inc.*, 103 F.T.C. 110, 174 (1984) (setting forth the Commission's Deception Policy Statement).

[39] *E.g.*, the Equal Credit Opportunity Act, 15 U.S.C. § 1691, *et seq.*, the Truth-in-Lending Act, 15 U.S.C. § 1601, *et seq.*, the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.*, and the Cigarette Labeling Act, 15 U.S.C. § 1331, *et seq*.

[40] For routine fraud cases, such as the Internet fraud cases discussed *supra*, the Commission proceeds under Section 13(b) of the FTC Act which authorizes the Commission, through its own attorneys, to bring actions in federal district court to seek injunctive relief against defendants' business practices. Trans-Alaska Pipeline Authorization Act, Pub. L. No. 93-153, § 408(f), 87 Stat. 576 (1973) (codified as amended at 15 U.S.C.§ 53(b) (1997)). The statute provides that this authority may be used "whenever the Commission has reason to believe that any person, partnership, or corporation is violating, or is about to violate, any provision of law enforced by the FTC." For an overview of the Commission's fraud program, see Remarks of Timothy J. Muris, "The Federal Trade Commission and the Future Development of U.S. Consumer Protection Policy" (Aug. 19, 2003), available at http://www.ftc.gov/speeches/muris/030819aspen.htm.

In contrast, this section discusses the Commission's security enforcement actions against sellers who normally do not make deceptive claims and whose products normally are reputable. For those claims, the Commission chose its administrative process.

[41] Even when there is no claim regarding information security, the Commission's unfairness authority could be used to attack unreasonable security practices. When the injury or

have made explicit or implicit promises that they would take appropriate steps to protect sensitive information obtained from consumers. When security measures are inadequate, those promises are deceptive.

Security Procedures Must Be Appropriate In The Circumstances

Security can go awry even in large, sophisticated companies with harmful consequences for consumers. The most obvious problem occurs when a company inadvertently releases sensitive personal information due to inadequate security procedures. The Commission's first security case, *Eli Lilly*,[42] involved such an inadvertent [43]disclosure despite promises to maintain security. Specifically, in sending an email to subscribers of its Prozac website, Lilly put all of the subscribers' email addresses in the "To" line of the email, thereby disclosing to each subscriber the email addresses of every other Prozac website subscriber.

Given the sensitivity of the information involved, this was a serious breach. At first glance, it would be easy to say it was just a mistake and one that, given the ensuing publicity,

---

likelihood of injury from a breach is significant, there is substantial injury. For instance, if a breach exposed sensitive financial information which was then used to perpetrate identity theft, we would examine the security measures in place. If our examination revealed inadequate measures that could be remedied easily at a low cost, the injury would outweigh the countervailing benefits of avoiding the costs of precautions. Moreover, consumers could not reasonably avoid the injury that stems from the theft of information that they have entrusted to others. Thus, the Commission could consider unfairness an appropriate theory of liability. On the other hand, many, perhaps most, breaches would not cause substantial injury and/or occur even when all cost effective security measures are in place. There should not be strict liability for security breaches.

[42] The Commission's final decision and order against Eli Lilly is available at www.ftc.gov/os/2002/05/elilillydo.htm. The complaint is available at www.ftc.gov/os/2002/05/elilillycmp.htm.

[43] Lilly offered an email reminder service to its Website subscribers. Although the reminders themselves included only the recipient's email address in the "To" line, Lilly's message terminating the service included the addresses of all 669 subscribers.

was unlikely to reoccur. But, the more appropriate analysis is to ask *why* the breach occurred. Had the company followed reasonable procedures in light of the sensitivity of the information to prevent such breaches from occurring in the first place?

In this case, the FTC alleged that the answer was "no." And in answering the question, the Commission, through its complaint and order, set forth the general principles that guide our information security program.

First, the Commission construed Lilly's privacy policy as a promise to take steps "appropriate under the circumstances" to protect personal information.[44] It did not see a claim of absolute protection, and it did not hold Lilly to such an impossible standard. Rather, it set forth an analysis that makes the reasonableness of the company's efforts the central question in assessing whether there is a violation. Thus, the complaint alleged that the breach resulted from Eli Lilly's "failure to maintain or implement internal measures appropriate under the circumstances to protect sensitive consumer information."[45]

Second, our analysis of what constitutes reasonable and appropriate procedures is linked directly to the sensitivity of the information collected by the company. Not all personal

---

[44] For example, the Lilly privacy policy stated that "Eli Lilly and Company respects the privacy of visitors to its websites, and we feel it is important to maintain our guests' privacy as they take advantage of this resource." *Eli Lilly Complaint*, paragraph 4(A) and (B). The policy also informed consumers that the company's Websites "have security measures in place, including the use of industry standard secure socket layer encryption (SSL), to protect the confidentiality of any of Your information that you volunteer. . . These security measures also help us to honor your choices for the use of Your Information." *Id.*

[45] *Eli Lilly Complaint*, paragraph 7. The complaint described various deficiencies in Lilly's security program, including failing to provide appropriate training for its employees regarding consumer privacy and information security; failing to provide appropriate oversight and assistance for the employee who sent out the email; and failing to implement appropriate checks and controls on the process, such as reviewing the computer program with experienced personnel and pretesting the program internally before sending out the email. *See id.*

information is the same – some facts, such as use of antidepressant drugs, are more sensitive than others. Such sensitive information is deserving of greater protection, precisely because the potential consequences to the consumer of disclosure are greater.

Not All Breaches Are Violations of FTC Law

It is important to note that the Commission is not simply saying "gotcha" for security breaches. Although a breach may indicate a problem with a company's security, breaches can happen even when a company has taken every reasonable precaution. In such instances, the breach will not violate the laws that the FTC enforces. Instead, the Commission recognizes that security is an ongoing process of using reasonable and appropriate measures in light of the circumstances. When breaches occur, our staff reviews available information to determine whether the incident warrants further examination. If it does, we gather information to enable us to assess the reasonableness and appropriateness of the procedures in place in light of the circumstances and whether the breach resulted from the failure to have such procedures. Using this analysis, in dozens of instances, we have concluded that FTC action is not warranted. When we find a failure to implement reasonable procedures, however, we act.

Law Violations Without a Known Breach

Because appropriate information security practices are necessary to protect consumers' privacy, companies cannot simply wait for a breach to occur. Particularly when they promise security, companies have a legal obligation to take reasonable steps to guard against reasonably anticipated vulnerabilities. Just because no breaches have yet occurred does not mean that the company had in place – and followed – reasonable procedures.

Our case against Microsoft, which focused on its Passport online authentication service,

establishes this principle.[46] Like Eli Lilly, Microsoft promised consumers that it would keep their information secure.[47] Unlike Lilly, there were no specific security breaches that triggered the case. Nevertheless, we alleged that there were significant security problems that, left uncorrected, could jeopardize the privacy of millions of consumers. In particular, we alleged that Microsoft did not employ "sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information obtained through Passport and Passport Wallet."[48] Specifically, the Commission alleged that Microsoft failed to have systems in place to prevent unauthorized access; detect unauthorized access; monitor for potential vulnerabilities; and record and retain system information sufficient to perform security audits and investigations.[49] Again, sensitive information was at issue – in this case, financial information including credit card numbers.

---

[46] Passport is an Internet sign-on service that allows consumers to sign in at multiple Websites with a single username and password. Passport Wallet and Kids Passport are add-on services that facilitate online purchasing and parental consent. At the time of our case, Passport contained 200 million accounts.

[47] Microsoft's privacy policy represented that the Passport system "achieve a high level of Web Security by using technologies and systems designed to prevent unauthorized access to your personal information" and further promised that Passport "is protected by powerful online security technology and a strict privacy policy." *Microsoft Complaint*, paragraphs 3 and 4. As in *Lilly*, the Commission construed the policy as a promise to provide "security measures that were reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information" obtained from Passport and Passport Wallet consumers. *Microsoft Complaint*, paragraph 6.

[48] *Microsoft Complaint*, paragraph 7.

[49] *Id.* Besides failing to deliver on its security promises, the Microsoft complaint alleged other privacy violations. The complaint alleged that Microsoft's collection of consumers' sign-in history was not disclosed. The complaint further alleged that Microsoft misrepresented to parents that they could control information collected about their children for Kids Passport service.

Good Security is an Ongoing Process of Assessing Risks and Vulnerabilities

One clear feature of information security is that the risks companies confront will change over time. Hackers and thieves will adapt to whatever measures are put in place, and new technologies likely will have new vulnerabilities waiting to be discovered. As a result, companies need to assess the risks they face on an ongoing basis and make these adjustments that are necessary to reduce these risks. The Commission's third security case, against Guess?, Inc. ("Guess"), highlights this crucial aspect of information security, in Web-based applications and the databases associated with them. Databases frequently house sensitive data such as credit card numbers, and Web-based applications are often the "front door" to these databases. It is critical that online companies take reasonable steps to secure these aspects of their systems, especially when they have made promises about the security they provide for consumer information.[50]

In *Guess*, the Commission alleged that the company broke such a promise concerning sensitive consumer information collected through its Website, www.guess.com. According to the Commission's complaint, by conducting a relatively basic "Web-based application" attack on the Guess Website, an attacker gained access to a database containing 191,000 credit card numbers. This particular kind of attack was well known in the industry and has appeared on a

---

[50] Guess promised that its Website "has security measures in place to protect the loss, misuse and alternation of the information under control." *Guess complaint*, paragraph 6. The company further stated that "[a]ll of your personal information including your credit card information and sign-in password are stored in an unreadable, encrypted format at all times. This Website and more importantly all user information is further protected by a multi-layer firewall based security system." *Id.* In addition to attacking the claim that all personal information is stored in an unreadable, encrypted format at all times, the Commission also construed the company's statements as claims that "they implemented reasonable and appropriate measures to protect the personal information they obtained from consumers through www.guess.com against loss, misuse, or alteration." *Id*. at paragraph 14.

variety of lists of known vulnerabilities.[51] According to the complaint, Guess did not: (1) employ commonly known, relatively low-cost methods to block Web-based application attacks; (2) adopt policies and procedures to identify these and other vulnerabilities; or (3) test its Website and databases for known application vulnerabilities, which would have alerted it that the Website and associated databases were at risk of attack.[52] Essentially, the company allegedly had no system in place to test for known application vulnerabilities, or to detect or to block attacks once they occurred. Even if the system was state of the art when it was put in place, companies that promise security have an obligation to monitor that system, and make reasonable changes to monitor and address new threats.[53]

As in prior cases, the emphasis on Guess is on reasonableness. When the information is sensitive, the vulnerabilities well known, and the fixes are cheap and relatively easy to implement, it is unreasonable simply to ignore the problem.

Remedies

Perfect security is not possible in any reasonable sense. There will always be thieves among us, and occasionally they will succeed. Just as we have not expected perfection in

---

[51] The industry press began to cover Web-based application vulnerabilities and solutions long before Guess' vulnerability to Web-based application attacks was exploited. *See e.g., Application Security: Taming the Wide Open Web*, Business Security Advisor, Feb. 2001; *Web apps are Trojan horses for hackers*, InfoWorld, April 5, 2001; and *Developers play vital role in web app security*, InfoWorld, April 5, 2001.

[52] In addition, the complaint alleged, Guess misrepresented that the personal information it obtained from consumers through www.guess.com was stored in an unreadable, encrypted format at all times; but in fact, after launching the attack, the attacker could read the personal information, including credit card numbers, in clear, unencrypted text.

[53] The *Guess* complaint focused on vulnerabilities that should have been known by at least 1998. The case challenged the reasonableness of steps taken since that time, not the adequacy of the system when it was first developed.

assessing whether a Section 5 violation exists, our orders do not require companies to achieve perfection. The most important relief we obtain is to require a comprehensive security program that takes into account the sensitivity of the information collected and includes an ongoing assessment of reasonably foreseeable risks and threats to information the company collects. We modeled the order provision requirements on the requirements of the FTC Safeguard Rule under the Gramm-Leach-Bliley Act.[54] The Rule became effective on May 23 of this year, and I expect that it will quickly become an important tool to ensure greater security for consumers' sensitive financial information. Whereas our Section 5 cases, to date, have derived from misstatements particular companies make about security, the Rule requires a wide variety of financial institutions to implement comprehensive protections for customer information – many of them for the first time. Each institution must develop a written plan[55] that takes into account its particular circumstances – its size and complexity, the nature and scope of its activities, and the

---

[54] In May 2002, the Commission finalized its Gramm-Leach-Bliley Safeguards Rule which implements the security requirements of the Gramm-Leach-Bliley Financial Modernization Act of 1999. 15 U.S.C. § 6801(b). The Rule requires financial institutions under the FTC's jurisdiction to develop and implement appropriate physical, technical, and procedural safeguards to protect customer information.

[55] As part of its plan, each financial institution must: (1) designate one or more employees to coordinate the safeguards; (2) identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks; (3) design and implement a safeguards program, and regularly monitor and test it; (4) hire appropriate service providers and contract with them to implement safeguards; and (5) evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards. The Safeguards Rule requires businesses to consider all areas of their operation, but identifies three areas that are particularly important to information security: employee management and training; information systems; and management of system failures.

sensitivity of the customer information it handles.[56] The Rule could go a long way to reduce risks to this information, including the risk that it will be used to facilitate identity theft.

The Rule's flexible performance standard found its origins in the Commission's previous research in this area. In May 2000, the Commission's Advisory Committee on Online Access and Security issued its final report.[57] Although the Report addressed security only in the online context, the Commission determined that many of its conclusions applied to information security practices generally and adopted them when promulgating the Safeguards Rule. For example, the Report recognized that security is a process, requiring continuous monitoring and adjustment to address new hazards as they emerge. Thus, no one static standard can assure adequate security. As a result, the Report recommended that each Website maintain a security program that is "appropriate to the circumstances."

The recognition that effective security is an ongoing process has also guided the nature of

---

[56] The Commission has issued guidance to businesses covered by the Safeguards Rule to help them understand the Rule's requirements. *See Financial Institutions and Customer Data: Complying with the Safeguards Rule, available at* http://www.ftc.gov/bcp/conline/pubs/buspubs/safeguards.htm. Commission staff have met with a variety of trade associations and companies to learn about industry's experience in coming into compliance with the Rule, to discuss areas in which additional FTC guidance might be appropriate, and to gain a better understanding of how the Rule is affecting particular industry segments. Since the Rule's effective date, the staff also held two training sessions for the public, and over 400 people attended. Now that the Rule is effective, we are conducting sweeps to assess compliance within various covered industry segments.

[57] Advisory Committee Report at 19. The Report is available at http://www.ftc.gov/acoas/papers/finalreport.htm. The FTC appointed forty members to the Advisory Committee who represented varied viewpoints on implementing access and security online. Members included representatives from online businesses, trade associations, computer security firms, database management companies, privacy and consumer groups, as well as academics, experts in interactive technology, and attorneys. The Advisory Committee held four public meetings, and in addition, members worked in subgroups to address specific topics in more depth.

remedies we have adopted in individual cases. In each case, the key relief is a requirement that the company establish an information security program, modeled after the requirements of our Safeguards Rule.[58] Core elements of that program have included putting appropriate personnel in charge of the program; conducting a comprehensive risk assessment in all relevant areas of the business; designing appropriate safeguards to control these risks and regularly monitoring their effectiveness; adjusting the program as needed; and documenting all elements of the program in writing.

One area where our orders have differed is requirements for outside audits. Monitoring security systems and the environment to identify new and emerging threats and vulnerabilities is a crucial element of any sound security program. Much of that monitoring will be internal to the company. External monitoring through an audit offers a more independent perspective, and can be very useful to us in assessing order compliance. By its nature, however, it is more of a snapshot of a security program at a particular point in time.

In Lilly, the order requires an annual written review by "qualified persons" – that is, persons qualified to perform the audit whether within the company or from outside. In Microsoft, however, we required an external audit every 2 years. In our view, the enormous complexity of the security problems that Microsoft is likely to confront, and the difficulties we

---

[58] The *Lilly* order is typical, requiring the company to "establish and maintain an information security program for the protection of personally identifiable information collected from or about consumers." *See, e.g., Eli Lilly Decision and Order*, paragraph II. The program shall consist of (A) designating appropriate personnel to coordinate and oversee the program; (B) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information, including any such risks posed by lack of training, and addressing these risks in each relevant area of its operations, whether performed by employees or agents, including (i) management and training of personnel; (ii) information systems for the processing, storage, transmission, or disposal of personal information; and (iii) prevention and response to attacks, intrusions, unauthorized access, or other information systems failures.

would likely confront in assessing their compliance from outside the company, necessitated a requirement for external audits. Similarly, in Guess, the order required an external audit every two years; however, unlike the Lilly and Microsoft orders, it also listed the type of information expected in the auditor's report.[59] We added this new provision to provide additional guidance to the company and its auditors, and we think it will be helpful to everyone in ensuring and assessing compliance.

A flexible information security program as required by our Safeguards Rule and individual orders is a sound approach to the security problem. It protects consumer information without imposing rigid, technologically-specific standards as a remedy. To do otherwise would likely engender a false sense of security and send a misleading message to industry. We could easily identify desirable technologies, such as intrusion detection or particular network architectures, but there is no magic bullet that will provide the appropriate level of security for all systems. If a company believes a particular technology or product solves all of its security problems, then it is likely not conducting a comprehensive risk assessment or taking other necessary steps to ensure that its systems are truly secure. Moreover, to specify a magic bullet neglects the obvious and rapid change of both technology and threats to those technological systems. As noted earlier, security is an ongoing process, and companies need to conduct periodic risk assessments and adjust their programs in light of what they find. For that reason, although our complaints have described the problems we have found, we have not charged that

---

[59] For example, the order requires that the audit report set forth "the specific administrative, technical, and physical safeguards that Respondents have implemented and maintained during the report period." *Guess Order*, paragraph III(A). The order also mandates that the audit report explains how such safeguards are appropriate to company's size and complexity, the nature and scope of the company's activities, and the sensitivity of the personal information collected form or about consumers. *Id.* at paragraph III(B).

the failure to adopt a particular technology constitutes a violation, and we have not imposed such requirements in our orders.

Notice in Cases of Security Breaches

Another potential remedy for information breaches is notice to affected parties.[60] Determining when notice is warranted and to whom notice should be given should be done on a case-by-case basis. Thus, when breaches occur, notice may not be appropriate in all circumstances.

Notice to consumers whose information may have been compromised is potentially attractive because it enables these consumers to take steps to protect themselves. The value of notice depends on the likelihood that the information will be misused, and on whether there are additional reasonable steps that consumers can take to reduce the risk of loss. If the circumstances of the breach indicate that information is in fact being used for identity theft, or that such misuse is highly likely, notice is likely to be extremely valuable.[61] Depending on the type of information compromised, consumers can take appropriate steps such as closing accounts, placing a fraud alert on their credit report to prevent new fraudulent accounts from

---

[60] For example, the recently-passed California law requires notice in certain circumstances where a breach has occurred exposing consumer information. *See* 2003 Cal ALS 241; 2003 Cal SB 1; Stats 2003 ch 241.

[61] Our identity theft survey found that victims who quickly discovered that their information was being misused were less likely to incur out-of-pocket expenses and resolved their problems more quickly. No out-of-pocket expenses were incurred by 67% of those who discovered the misuse less than 6 months after the misuse began. Only 40% of victims who took 6 months or longer to discover the misuse were able to avoid incurring some such expenses. 76% of consumers who discovered that their information was being misused less than a month after the misuse began spent less than 10 hours resolving their problems. Where the misuse was discovered 1 to 5 months after the misuse began, 59% of victims spent less than 10 hours resolving their problems. Where it took 6 or more months to discover the misuse, only 20% of victims were able to resolve their problems in this amount of time.

being opened, or examining their report to clear up any fraudulent information that may be affecting their creditworthiness.[62]

There may be some situations where, in addition to consumers, or even in lieu of direct notification to consumers by the compromised business, other parties should receive notice (*e.g.* credit reporting bureaus, credit card issuers). Because some consumers will inevitably fail to receive, act upon, or perhaps, understand the notice sent to them, or because the costs of notice may outweigh the benefits to consumers, it could be useful for a business that suffers a breach to notify other relevant parties. For example, if only credit card numbers were compromised, notifying the credit card issuers so that they can monitor and close affected accounts may be an alternate solution to blanket notification of consumers. Because the credit card companies bear financial risk of unauthorized transactions, they have incentives to be vigilant and have mechanisms already in place to contact consumers about questionable transactions. Furthermore, consumers' options for self-help are no different from what the credit card companies would do: monitor and close affected accounts. Thus, the cost of notice to consumers might outweigh any benefits given the ability of the credit card companies to identify and stop injury.

---

[62] The credit reporting agencies will place a fraud alert on a consumer's reports in order to alert users of the reports to be aware of the possibility of fraud before they open accounts in the name of the consumer. Fraud alerts are most useful when the type of information that has been compromised could be used to open new accounts such as SSNs, driver's licenses, addresses and birth dates. The major credit reporting agencies also will block information in a consumer's files resulting from identity theft if the consumer provides them with a police report. Although these programs are currently voluntary on nationwide basis (they are mandatory in a few states), the Commission has recommended that Congress codify them as part of the Fair Credit Reporting Act. *See* Commission Testimony before the U.S. Senate Committee on Banking, Housing and Urban Affairs, July 10, 2003, available at http://www.ftc.gov/os/2003/07/030710fcratestsenate.htm.

In other cases, however, notice to consumers or other parties may have little or no value. When a database has been compromised, it may be discovered that the perpetrator was only be trying to prove that the system could be breached, as in the Guess case, or it may be difficult to determine exactly which information has been stolen, or even whether any information was stolen. Individualized notices to consumers in such an instance would raise concerns for no particular reason. Moreover, if consumers did react to the warning by, for example, placing a fraud alert, the value of the fraud alert as a signal of a real risk of fraud might be reduced as creditors spend time and money checking for fraud where it doesn't exist.

Experience has shown us that there is no one-size-fits-all approach to notification. Instead, notice to consumers and others, should hinge upon the likelihood that the information compromise will result in actual injury. This determination itself hinges upon numerous factors including the type of information compromise, the nature of the compromise or the intent of the perpetrator, if known. Still, I think we have developed practical advice for businesses to consider when they are the source of an information breach. Notice is, of course, just the beginning of the education process for businesses and consumers.

Education

Our education efforts focus on prevention of harms by making sure businesses and consumers are paying attention to the steps they can take to minimize the risks to personal information and the harms that result from misuse of personal information. Through our fraud enforcement work, we know that the hazards resulting from poor information security practices are not unique to the Internet and that an educated business *and* consumer often present the best defense against the seemingly endless parade of scams, whether tech-based or not.

In September 2002, we launched an extensive and ongoing education campaign featuring Dewie, the e-Turtle, focusing on steps businesses and consumers can take to secure sensitive information.[62] Most recently, the Commission has published alerts addressing risks to computer systems[63] and the risks associated with file-sharing.[64]

The FTC has taken the lead in coordinating with other government agencies and organizations in the development and dissemination of comprehensive consumer education materials for victims of identity theft and those concerned with preventing this crime. The FTC's extensive consumer and business education campaign includes print materials, media mailings, and radio and television interviews. The FTC also maintains the identity theft website, which includes the publications and links to testimony, reports, press releases, identity theft-related state laws, and other resources.[65]

We held workshops to explore emerging technologies and their impact on information security practices. As head of the U.S. delegation to the OECD Experts Group for Review of the 1992 OECD Guidelines for the Security of Information Systems, FTC Commissioner Orson Swindle, led efforts to revise the Guidelines, which were finalized in August 2002.[66] In all of these efforts, our central message is that commercial security practices are simply one aspect of a

---

[62] *See* <http://www.ftc.gov/bcp/conline/edcams/infosecurity/index.html>.

[63] *Security Check: Reducing Risks to Your Computer* Systems, available at <http://www.ftc.gov/bcp/conline/pubs/buspubs/security.htm>.

[64] *File-Sharing: A Fair Share? Maybe Not*, available at <http://www.ftc.gov/bcp/conline/pubs/alerts/sharealrt.htm>.

[65] <http://www.consumer.gov/idtheft>.

[66] *See* <http://www.ftc.gov/opa/2002/08/oecdsecurity.htm>.

much larger and more comprehensive “culture of security” that must be developed across all sectors of our economy if we are to protect our vital national information infrastructure.

Conclusion

One key lesson of our privacy agenda is that, of course, principles matter. An institution that merely reacts to circumstances and does not work from a coherent philosophy will ultimately fail to achieve lasting success. Our cases demonstrate these principles in action. Secondly, our extensive experience in consumer privacy issues has taught us that maintaining good privacy practices is an important part of reducing cybercrime of all types that puts consumer information at risk – from online hacks to low-tech dumpster dives. Whether the information thief is an insider or a remote hacker, the critical lesson in this information-based economy is that government, private industry, and consumers must all take appropriate steps to protect personal information and the systems that house it.