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.

[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.

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 agencieTJ-pllafirg454.s4(n-0hem)opent aor natiosuate. Joly

---

[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.)

14

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

[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]

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.

[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*

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.

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

[34]

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

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/elililly do.htm. The complaint is available at www.ftc.gov/os/2002/05/elililly cmp.htm.

[43]

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,

[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

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.

[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

56

[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.

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 si

In September 2002, we launched an extensive and ongoing education campaign featuring

---

[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>.