Order Code RS22082
March 16, 2005

CRS Report for Congress
Received through the CRS Web

Identity Theft: The Internet Connection

Marcia S. Smith
Specialist in Aerospace and Telecommunications Policy
Resources, Science, and Industry Division

Summary

Concern is growing about identity theft — where one person assumes the identity of another by stealing personally identifiable information (PII), such as credit card or Social Security numbers. High profile incidents disclosed in early 2005 involving ChoicePoint, Bank of America, and LexisNexis, where the PII of more than a million Americans may have been compromised, have refocused congressional attention on this issue. Many associate the rise in identity theft cases with the Internet, but surveys indicate that comparatively few victims cite the Internet as the source of their stolen PII. Still, the Internet may play a role, particularly through a practice known as "phishing." Congress already has passed several laws to address identity theft, and continues to debate whether additional action is needed. This report will not be updated; for information on pending bills and current legislative action, see CRS Report RL31408.

Introduction

The growth in the number of cases of "identity theft," where one individual assumes the identity of another to commit fraud, is alarming to many consumers, including many Members of Congress. Despite widespread public perception that the Internet is a major contributor to the rise in identity theft, surveys indicate that comparatively few individuals who know how a thief acquired their personally identifiable information (PII) cite the Internet. Some attribute the rise in identity theft instead to carelessness by businesses in handling PII, and by credit issuers that grant credit without proper checks. Identity theft can be separated into "low-tech" crimes by thieves who acquire PII through traditional means such as lost or stolen wallets or "dumpster diving," and "high-tech" crimes by thieves who compromise computer databases or use the Internet. A survey released in January 2005 (discussed below) found that computer crime accounted for 11.6% of identity theft cases in 2004, compared with 68% from paper sources.

Computer crimes do not necessarily involve the Internet; they may be caused by data security or computer security lapses (such as insider theft). Still, the Internet can be used to acquire an individual's PII, particularly through a practice known as "phishing." The Internet also could enable hackers to access computer databases if the databases are connected to the Internet. Also, PII may be inadvertently placed on the Internet through

human error.[1] The networked nature of the Internet age, coupled with steadily increasing computer power, not only allows the linking of enormous databases to facilitate information access, but also makes that information more vulnerable to misuse. The ease, speed, and relative anonymity of online transactions may further exacerbate harm to the consumer when identity theft occurs.

Identity Theft: Definition, Prevalence, and How It Occurs

The Federal Trade Commission (FTC) defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[2] The FTC commissioned Synovate to conduct an identity theft survey in 2003 [http://www.ftc.gov/os/2003/09/synovatereport.pdf]. An FTC press release summarizing the survey [http://www.ftc.gov/opa/2003/09/idtheft.htm] reported that 27.3 million Americans had been victims of identity theft in the previous five years.[3] Losses to businesses and financial institutions totaled nearly $48 billion, and, to consumer victims, $5 billion in out-of-pocket expenses. The survey found (pp. 30-31) that 51% of the identity theft victims in their survey knew how their PII was stolen, including 14% who said it was obtained from lost or stolen wallets, checkbooks, or credit cards; 13% who said it was obtained during a transaction; 4% who cited stolen mail; and 14% who said the thief used "other" means, for example, the information was misused by someone who had access to it, such as a family member or workplace associate.

More recent detailed statistics have not been published by the FTC, but a February 7, 2005 FTC press release states that identity theft affects approximately 10 million Americans each year [http://www.ftc.gov/opa/2005/02/ncpw05.htm]. Meanwhile, the Council of Better Business Bureaus and Javelin Strategy & Research released a survey in January 2005.[4] The report states that it is based on data collected in 2004 by Synovate using questions that closely mirrored those in the 2003 FTC survey, plus several new questions. The survey found that computer crime accounted for 11.6% of identity theft cases in 2004, compared with 68% from paper sources. It further found that the average loss for online identity theft was $551 compared to $4,543 from paper sources. In cases where the perpetrator could be identified, family members were responsible for 32% of cases; complete strangers outside the workplace for 24%; friends, neighbors, and in-home employees for 18%; someone at a company with access to personal information for 13%;

---

[1] For example, in October 2004, a University of California network exposed the personal data (including names, addresses, phone numbers, SSNs, and birthdays) of 1.4 million people participating in a state in-home care program. See Rachel Konrad. Hackers May Have Stolen Californians' Data. Associated Press, February 16, 2005, 10:18 (via Factiva).

[2] 69 FR at 63933.

[3] The Synovate report explains that 12.7% of respondents to its survey reported they were victims of identity theft in the past five years, which "implies that approximately 27 million American adults have been victims in this period." (p. 12)

[4] The 2005 Identity Fraud Survey. An abbreviated "complimentary" version of the report is available at [http://www.javelinstrategy.com/reports/2005IdentityFraudSurveyReport.html]. A Better Business Bureau press release is at [http://www.bbb.org/alerts/article.asp?ID=565]. The survey was sponsored by Checkfree, Visa, and Wells Fargo & Company, but the report emphasizes that although those companies were invited to comment on the content of the questionnaire, they were not involved in the tabulation, analysis, or reporting of final results.

someone at the victim's workplace for 4%; or "someone else" for 8%. The study concluded that, contrary to popular perception, identity theft is not getting worse. For example, it reported that the number of victims declined from 10.1 million in 2003 to 9.3 million in 2004, and the annual dollar volume, adjusted for inflation, is "highly similar" ($52.6 billion) to the 2003 survey.

Tips on Preventing Identity Theft and Where to Go For Help

The 1998 Identity Theft and Assumption Deterrence Act (P.L. 105-318) directed the FTC to establish a central repository for identity theft complaints, and provide victim assistance and consumer education. The FTC's identity theft website is at [http://www.consumer.gov/idtheft/]. Tips on avoiding identity theft are available at [http://www.consumer.gov/idtheft/protect_againstidt.html#5]. The lengthy list includes the following that relate to the Internet and computers:

- Do not give out personal information over the Internet unless you have initiated the contact or are certain you know who you are dealing with; and
- If you store PII such as Social Security Numbers (SSNs), financial records, tax returns, birth dates, or bank account numbers on your computer:
  - — Use virus protection software and update it regularly;
  - — Do not open files sent to you by strangers or click on hyperlinks or download programs from people you do not know, and be careful about using file-sharing programs;
  - — Use a firewall program;
  - — Use a secure browser (software that encrypts information you send over the Internet);
  - — Try not to store financial information on your laptop;
  - — Delete all personal information on a computer before disposing of it; and
  - — Look for website privacy policies, and if you do not see one, or cannot understand it, consider doing business elsewhere.

Consumers also are advised to check their credit reports regularly, which are maintained by the three nationwide credit bureaus: TransUnion, Equifax, and Experian. Under the 2003 Fair and Accurate Credit Transactions Act (discussed below), those credit bureaus and other consumer reporting agencies (CRAs) must provide consumers one free copy of their credit reports each 12 month period, upon request. Consumers in Western and Midwestern states already have access to free reports. Consumers in Southern states can order them beginning on June 1, 2005, and, in Eastern states, beginning September 1, 2005. (Some states also have laws requiring such agencies to provide free copies of these reports). The credit reports can be ordered at [http://www.annualcreditreport.com], or consumers may phone or write a central location. Consumers may not contact the credit bureaus or other CRAs directly to obtain these free reports. For further information, see [http://www.consumer.gov/idtheft/recovering_idt.html#9].

For consumers who are victims of identity theft, the FTC has a toll free number (877-ID-THEFT) to call for help. (See also CRS Report RL31919 for remedies for victims of identity theft.) The FTC's identity theft website also lists steps that victims should take

as soon as they discover their information has been compromised. The non-profit Identity Theft Resource Center [http://www.idtheftcenter.org] also offers advice and information.

ChoicePoint and Other High Profile Incidents in 2005

Three high profile incidents that became public in 2005, where the security of consumer PII was compromised, reinforced existing fears about identity theft. Congressional hearings are underway on whether new legislation is needed to regulate companies that collect and sell PII (called data brokers, data warehousers, or information brokers), and other businesses that store PII in computer databases. Breaches of consumer data privacy have become disturbingly commonplace. These three incidents were chosen as examples because they are of current congressional interest. Officials from these companies testified to Congress on March 15, 2005 about the incidents — to the Senate Committee on Banking, Housing, and Urban Affairs on March 15, 2005 (ChoicePoint and Bank of America); and the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection (ChoicePoint and LexisNexis). Their testimony is available on the committees' websites: [http://banking.senate.gov], and [http://energycommerce.house.gov].

In February 2005, data broker **ChoicePoint** revealed it had sold data on at least 145,000 Americans to criminals posing as officials in legitimate businesses.[5] Contrary to initial press reports, ChoicePoint's computers were not hacked. Instead, the criminals opened about 50 accounts with the company and accessed the data as customers. The disclosure came as ChoicePoint complied with a California law that requires companies with corporate computer networks that do business with state residents to notify individuals if their unencrypted personal information is acquired by an unauthorized person. According to testimony to the House Energy and Commerce subcommittee by ChoicePoint's Chairman and CEO, Derek Smith, a ChoicePoint employee became suspicious in September 2004 during the credentialing process for a prospective small business customer in Los Angeles. According to Mr. Smith, the Los Angeles Police Department was brought in, and at least one individual was arrested and convicted. Thereafter, ChoicePoint discovered that those involved previously had opened accounts by presenting fraudulently obtained California business licenses and fraudulent documents. After the public disclosure of this data security breach, it became known that a similar incident occurred at ChoicePoint five years earlier.[6]

Also in February 2005, **Bank of America** publicly announced that it lost five backup computer data tapes in December 2004.[7] The tapes contain personal information on 1.2 million federal employees who use a federal government charge card program (SmartPay), including some members of the Senate and their staffs. The tapes were being transported

---

[5] Evan Perez. Identity Theft Puts Pressure on Data Sellers. Wall Street Journal, February 18, 2005, B1 (via Factiva). According to that article, although ChoicePoint cites 145,000 individuals, investigators on the case believe the number may be as high as 400,000.

[6] David Colker and Joseph Menn. ChoicePoint Had Earlier Data Leak. Los Angeles Times, March 2, 2005, C-1 (via Factiva).

[7] Eileen Sullivan. Lost Data Prompts Bank of America to Tighten Handling of Federal Accounts. FederalTimes.com, March 7, 2005 [http://federaltimes.com/index2.php?S=705180].

by airplane to a storage facility. At the House Energy and Commerce subcommittee hearing, a Bank of America official stated that there is no evidence to date of unauthorized use of the data.

In March 2005, information broker **LexisNexis** (a division of Reed Elsevier) disclosed that it had identified a number of incidents of potential fraudulent access to information about 32,000 U.S. individuals. At the House Energy and Commerce subcommittee hearing, a LexisNexis official reported that criminals compromised the IDs and passwords of legitimate customers and used them to access certain databases at Seisint, a company that recently had been acquired by LexisNexis.

At this time, it appears that the Internet played no role in the Bank of America case. ChoicePoint used the Internet as a communications medium to provide data to the criminals, but it apparently otherwise was not a factor. The extent to which the Internet may have been involved in the LexisNexis incident is unclear.

"Phishing"

As noted earlier, the Internet can play a role in identity theft. Today, attention is focused on a relatively new scam called "phishing." Phishing refers to a practice where someone misrepresents their identity or authority in order to induce another person to provide PII over the Internet. Some common phishing scams involve e-mails that purport to be from a financial institution, Internet Service Provider, or other trusted company claiming that a person's record has been lost. The e-mail directs the person to a website that mimics the legitimate business' website and asks the person to enter a credit card number and other PII so the record can be restored. In fact, the e-mail or website is controlled by a third party who is attempting to extract information that will be used in identity theft or other crimes. The FTC issued a consumer alert on phishing in June 2004.[8] An "Anti-Phishing Working Group" industry association has been established to work collectively on solutions to phishing. The group encourages consumers to report phishing incidents via its website [http://www.antiphishing.org/] and provides phishing statistics. In January 2005, it reported there were 2,560 active phishing websites, and the average monthly growth rate between July 2004 and January 2005 was 28% [http://antiphishing.org/APWG_Phishing_Activity_Report-January2005.pdf].

Existing Laws

The FTC enforces three federal laws that restrict disclosure of consumer information and require companies to ensure the security and integrity of the data in certain contexts — Section 5 of the Federal Trade Commission Act, the Fair Credit Reporting Act (FCRA), and Title V of the Gramm-Leach-Bliley Act. FTC Chairwoman Deborah Platt Majoras summarized these laws as they pertain to identity theft at a March 10, 2005 Senate Banking Committee hearing [http://banking.senate.gov/_files/majoras.pdf]. She identified two other laws that are not enforced by the FTC, but which also restrict the disclosure of certain types of information: the Driver's Privacy Protection Act, and the Health Insurance Portability and Accountability Act. Congress also has passed laws

---

[8] FTC. How Not to Get Hooked by a 'Phishing" Scam. June 2004. [http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.pdf]

specifically regarding identity theft: the 1998 Identity Theft and Assumption Deterrence Act; the 2003 Fair and Accurate Credit Transactions (FACT) Act; and the 2004 Identity Theft Penalty Enhancement Act. Those laws are summarized in CRS Report RL31919.

The FACT Act, which amended FCRA, contains perhaps the most comprehensive provisions in federal law directed at identity theft. In addition to allowing consumers to obtain free copies of their credit reports (discussed earlier), the act further regulates consumer reporting agencies (CRAs), enhances penalties for identity theft, and provides assistance for victims.[9] Among other things, the FACT Act requires CRAs to follow certain procedures concerning when to place, and what to do in response to, fraud alerts on consumers' credit files; requires credit card issuers to follow certain procedures if additional cards are requested within 30 days of a change of address notification; requires the truncation of credit card numbers on electronically printed receipts; and extends the statute of limitations for when identity theft cases can be brought.

As noted, some states, such as California, have their own identity theft laws (see CRS Report RL31919), and others are considering such legislation.

Continuing Congressional Issues

At a March 10, 2005 Senate Banking Committee hearing, FTC Chairwoman Majoras emphasized that a "complicated maze" of laws governs consumer data based on the type of company or institution involved, the type of data collected or sold, and the purpose for which it will be used. She conceded that it is not clear if data brokers like ChoicePoint come under the FTC's jurisdiction, and concluded that additional legislation may be necessary, particularly regarding notice and security. A witness from the Secret Service also testified about his agency's jurisdiction over identity theft crimes.[10]

Many bills have been introduced in the 109th Congress (see CRS Report RL31408). Legislative approaches include strengthening penalties for identity theft or for the misuse of SSNs[11]; increasing regulation of information brokers, such as by requiring them to notify individuals whose PII has been breached, or to obtain a consumer's consent before selling PII; limiting the use of SSNs or allowing individuals to choose an identifier other than their SSN for Medicare purposes, for example; or making phishing a crime. The only legislative action to date in the 109th Congress is markup of a bill (H.R. 29) that contains an anti-phishing provision. The bill was ordered reported from the House Energy and Commerce Committee on March 9, 2005. As discussed already, the Senate Banking Committee held hearings on identity theft on March 10 and March 15, 2005. A House Energy and Commerce subcommittee held a hearing on March 15, 2005. Additional hearings are expected.

---

[9] Implementation of the act is discussed in CRS Report RL32535, Implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003, by Angie A. Welborn and Grace Chu.

[10] The hearing can be viewed on the committee's website at [http://banking.senate.gov/index.cfm?Fuseaction=Hearings.Detail&HearingID=142].

[11] For more on Social Security numbers, see CRS Report RL30318, The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality, by Kathleen S. Swendiman.