IDENTITY THEFT & TERRORISM

Democratic Staff of the
Homeland Security Committee
Prepared for
Rep. Melissa Bean, Member – House Financial Services Committee
Bennie G. Thompson, Ranking Member, House Committee on Homeland Security
Rep. Edward Markey, Member, House Committee on Homeland Security

July 1, 2005

INTRODUCTION

High profile security breaches that have been reported over the past five months involving consumer database companies ChoicePoint and LexisNexis — as well as several large banks — have compromised the personally identifiable information of millions of individuals.[1] There have been numerous other data breaches reported by companies, universities, and even Federal government agencies such as the Department of Justice and the Federal Deposit Insurance Corporation.[2] In many instances, criminals stole the consumers' identity information to get new credit cards or empty existing financial accounts. For example, so far 750 of the 145,000 ChoicePoint victims have reported their identities stolen.[3] These breaches highlight the continuing evolution of identity theft and demonstrate the vulnerability of our citizens' personal information to criminal attacks.

The breaches also raise troubling questions about the possibility that terrorists are using identity theft and related techniques to further their efforts to harm the United States. Stolen identities provide criminals, including terrorists, with access to critical infrastructure such as airports and nuclear facilities. Terrorists also use stolen identities to get cash or credit necessary to finance their operations. Democratic members of the House Committee on Homeland Security have voiced their concerns because of possible ties between identity theft and terrorism. **"**We are concerned that ChoicePoint and similar entities are not securing their databases in ways that prevent terrorists from stealing personal records. Little exists to prevent Al Qaeda from breaking into these databases. This security gap must be fixed so that terrorists cannot steal American identities to enter the United States and hide among us once here," noted Congressman Bennie G. Thompson, Ranking Member of the House Homeland Security Committee.[4]

In an age where information is treated as a valuable commodity,[5] identity theft has become one of the fastest-growing and most profitable criminal enterprises in the world. The statistics are frightening:

- the 2003 Federal Trade Commission (FTC) indicated that 27.3 million Americans were victims of identity theft over the past five years;[6]
- a more recent report issued in 2005 stated that in the last 12 months approximately 9.3 million Americans were victims of identity theft; and[7]
- in 2004 identity theft cost the United States $52.6 billion.[8]

---

[1] Marcia Smith, "Identity Theft: The Internet Connection," March 16, 2005. Washington, D.C.: Congressional Research Service, 2005 (RS22082), 1.
[2] Jonathan Krim, "FDIC Alerts Employees of Data Breach," *Washington Post*, June 16, 2005.
[3]Sarah Scalet, "The Five Most Shocking Things About the ChoicePoint Debacle," *CSO online*, May, 2005, found at http://www.csoonline.com/read/050105/choicepoint.html.
[4] Democratic Staff of the Committee on Homeland Security, United States House of Representatives, "Prominent Democrats Ask for Investigation into Terrorism Risk Created by the Theft of Personal Records from ChoicePoint and Other Information Brokers," *Democratic Staff press release*, March 3, 2005.
[5] Evan Hendricks, "When Your Identity is Their Commodity," *Washington Post*, March 6, 2005.
[6] Federal Trade Commission , "Identity Theft Survey Report," September 2003.
[7] Better Business Bureau and Javelin Strategy & Research, "2005 Identity Theft Survey Report," January 2005
[8] Id.

The use of several methods for conducting electronic commerce, such as electronic fund transfers, credit and debit cards, and online banking has also created a vast new industry for fraudsters.[9] One e-mail scam currently targeting innocent computer users is called "phishing," which occurs when criminals send fraudulent e-mails that appear to be from legitimate companies—but are not—to trick customers into revealing personal information. Between July 2004 and April 2005, phishing sites grew at an average rate of 15 percent per month.[10]

There are numerous dangers posed by phishing. According to Avivah Litan, a research director with Gartner, "There's a high correlation between victims of phishing attacks and victims of identity theft." She further commented, "A majority of those who remember giving away sensitive information to phishers also reported being victimised [sic] by identity theft."[11]

The economic impact of phishing is also tremendous. In a report released last year, Gartner estimated that 57 million people had received online phishing attacks – three percent of whom had provided information to "phishers," costing banks and credit card users $1.2 billion in 2003 alone.[12] Litan also stated that phishing has the potential to severely harm e-commerce because it erodes consumer confidence in the security of online purchases. Unless phishing is remedied, Litan estimated that the growth of e-commerce would slow to 10 percent by 2007.[13]

Despite the growing number of reported identity and data thefts, consumers still have few, if any, proactive tools for preventing identity theft. Most remedies for consumers are only available after the first incident of identity theft occurs. For example, once a consumer suspects he or she is a victim of identity theft, temporary fraud alerts can be placed on his or her credit file. If negative information is put in a consumer's credit file because of identity theft, the consumer can block the information– but the consumer must say the fraud has occurred.[14]

Another problem consumers face is that they have little or no control over their private personal information once they give it to an entity. A U.S. Secret Service agent testified earlier this year before the Senate Banking Committee that:

> [C]onsumers routinely provide personal and financial identifiers to companies engaged in business on the Internet. They may not realize that the information they provide in credit card applications, loan applications, or with merchants they patronize is a valuable commodity in this new age of information trading.

---

[9] Federal Trade Commission, Consumer Alert, "How Not to Get Hooked by a Phishing Scam," found at http://www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

[10] Anti-Phishing Working Group, "Phishing Activity Trends Report, April 2005," found at www.antiphishing.org/APWG_Phishing_Activity_Report_April_2005.pdf.

[11] Avivah Litan, "Phishing Attack Victims Likely Targets For Identity Theft," *Gartner, Inc., publication FT-22-8873*, found at http://www4.gartner.com/resources/120800/120804/phishing_attack.pdf.

[12] Gregg Keizer, "Phishing Attacks Surge: Gartner," *ChannelWeb Network*, May 7, 2004, found at http://www.crn.com.au/story.aspx?CIID=15057.

[13] Id.

[14] Angie Welborn, et al, "Remedies Available to Victims of Identity Theft," April 19, 2005. Washington, D.C.: Congressional Research Service, 2005 (RL31919), 4.

Consumers may be even less aware of the illegitimate uses to which this information can be put.[15]

DATA BROKERS
Thefts from Data Brokers Present Threats to Consumer Privacy

The commercial data broker market consists of approximately 20 "data aggregator" companies including ChoicePoint, LexisNexis, Axciom, and Experian. These companies collect, manage, buy, and sell personal information they collect from public records, credit applications, and other sources of information.[16] For example, data brokers collect information such as social security numbers, dates of birth, addresses, criminal records, property records, and even DNA information. Data brokers also purchase "credit header" information, which generally includes an individual's name, date of birth, address, phone number and social security number, from credit reporting agencies. The brokers sell this information to an even larger variety of clients that include marketers, landlords, prospective employers, and the Federal government. While Federal law regulates the information credit reporting agencies can release from a consumer's credit file, the purchase and sale of this information remains unregulated.

ChoicePoint

ChoicePoint is one of the largest data brokers holding more than 19 billion data files and accumulating almost 40,000 new records a day.[17] In the fall of 2004, a group of criminals obtained valid California business licenses that were used to open accounts with ChoicePoint. The criminals then used these legitimate accounts to obtain credit information about thousands of private citizens. In February 2005, ChoicePoint was forced by California law to reveal that personal data for 145,000 individuals had been compromised by this crime ring.[18] In November 2002, ChoicePoint had experienced a similar incident of fraud when a group of suspects allegedly orchestrated the theft of 7,000 individuals' identities.[19] As a result, ChoicePoint has been called a "gold mine" for criminals seeking to steal identities.[20]

LexisNexis

Consumers' personal information was stolen from another large data broker, LexisNexis– widely known as a research engine. Last summer, the owner of LexisNexis purchased data broker company Seisint and made it a unit of LexisNexis.[21] Months after

---

[15] See Larry Johnson, Special Agent in Charge - Criminal Investigative Division, United States Secret Service, in testimony before the Senate Banking Committee, hearing on Identity Theft: Recent Developments Involving the Security of Sensitive Consumer Information, March 10, 2005.
[16] Nathan Brooks, "Data Brokers: Background and Overview," May 5, 2005. Washington, D.C.: Congressional Research Service, 2005 (RS22137), 2.
[17] Duane D. Stanford, "All our lives are on file for sale," *Atlanta Journal-Constitution*, Mar. 20, 2004.
[18] Bill Husted, "Consumers wait for ID-theft news," *Atlanta Journal-Constitution*, February 18, 2005.
[19] AP, "Report: Scam Targeted ChoicePoint in 2002," March 2, 2005, found at http://www.foxnews.com/story/0,2933,149169,00.html.
[20] Harry R. Weber, "Personal Info Breach Puts Data Warehouser in Hot Seat," *USA Today*, February 18, 2005.
[21] Nathan Brooks, "Data Brokers: Background and Overview," May 5, 2005. Washington, D.C.: Congressional Research Service, 2005 (RS22137), 4.

the purchase, LexisNexis announced that criminals had illegally accessed consumer data by assuming the identities and passwords of legitimate customers to download the names, addresses, social security and driver's license numbers of approximately 300,000 individuals.[22]

Threats Posed by Data Brokers

There are several significant threats posed by data brokers. One of the biggest threats is the frequency with which incorrect information gets into consumer databases causing extremely negative results for consumers, including the loss of basic constitutional rights. For example, ChoicePoint Vice President Martin Fagan admitted that in the state of Texas that at least 8,000 names had been incorrectly listed as felons in their database. This may have caused them to lose their ability to vote in the 2000 Presidential election. ChoicePoint Vice President Fagan described the error as a "*minor glitch.*" At the time, ChoicePoint's policy was to avoid verifying the accuracy of its data arguing that it was the user's responsibility to verify accuracy.[23]

Several cases demonstrate how inaccuracies in a consumer's credit file can have devastating effects, including the ability to earn a living. For instance:

> A Maryland woman was wrongly arrested for a burglary that was not cleared from the state's criminal databases. Her name and social security number were transferred to a Baltimore County database relating to child protective services cases. She was fired from her job as a substitute teacher, and only after she could establish that the information was erroneous was she rehired. After she left that job to run a day care center for the U.S. military, she was subject to questioning about the erroneous arrest. Later on, when employed as a child care director at a YMCA, she was terminated when her arrest record surfaced in a background clearance check. Since she could not have the error expunged in sufficient time, the job was given to another person. Only after several years was the error finally cleared from public records.[24]

These databases also pose a potential threat to consumers' civil and privacy rights because several Federal agencies regularly use these databases to gather information. The Privacy Act of 1974 strongly limited the Federal government's ability to gather information about consumers from credit reporting agencies. With the advent of data aggregator companies such as LexisNexis, however, the government can actually contract with these companies to receive information that would otherwise be prohibited.[25]

---

[22] Id.
[23] "ChoicePoint," *Wikipedia* (last modified May 23, 2005), found at http://en.wikipedia.org/wiki/ChoicePoint.
[24] Eugene Meyer, "Md. Woman Caught in Wrong Net; Data Errors Link Her to Probes, Cost 3 Jobs," *Washington Post*, December 15, 1997.
[25] Center for American Progress, "Protecting Privacy in the Digital Age: American Progress Recommendations on Government's Use of Commercial Databases," May 4, 2005.

The breadth of the data thefts seems to grow with each incident, as well as the means used to steal the data. Bank of America, the second-largest bank in the United States, shipped unencrypted data tapes containing financial information of approximately 1.2 million Federal workers, including U.S. Senators. According to news reports, baggage handlers were the prime suspects.[26] At DSW Shoe Warehouse, 103 of the company's 175 U.S. stores had credit card information and other purchase data stolen.[27] Another scheme involved collection agencies and law firms specializing in collection cases purchasing the personal data of 676,000 customers from New Jersey-based employees of Bank of America, Wachovia, PNC Bank, and Commerce Bank.[28] The operation allegedly lasted four years and netted its ringleader at least $2 million.[29] According to security analysts, "The incident reveals a disturbing vulnerability in the banking system… [The incident's] impact reaches far beyond the Delaware River. Now, the leadership at virtually every bank in the country has to wonder whether its employees or outsourcing partners are involved in such a scheme."[30]

CardSystems Solutions, Inc.

On June 17, 2005 CardSystems Solutions, Inc., of Atlanta belatedly announced that it had identified "a potential security incident" almost one month earlier—on May 22. The company, which processes credit card transactions for all of the major credit card companies doing business in the United States, had been compromised by a computer hacker. The incident gave the perpetrator(s) access to consumer records including names, account numbers and verification codes that could be used to carryout a fraud scheme.

In a press release, CardSystems Solutions said it had contacted the Federal Bureau of Investigation (FBI) on May 23 and also notified the VISA and MasterCard Card Associations. Although CardSystems Solutions says it "immediately began a remediation process to ensure all systems were secure" and hired a third party to confirm its systems' security, it also admitted in press reports that it should not have retained the information in the first place.[31] The records were generated when CardSystems processed swiped cards to confirm credit card transactions. The information should have been destroyed after the transactions were completed.

The incident came to light when MasterCard International Inc. disclosed the security breach and indicated that as many as 13.9 million of its cards had been compromised. The

---

[26] Associated Press, "Bank of America Loses Customer Data," March 1, 2005, found at http://www.msnbc.msn.com/id/7032779/.
[27] Associated Press, "Credit Information Stolen from DSW Shoe Stores," March 8, 2005, found at http://www.ohio.com/mld/centredaily/business/11083172.htm.
[28] Todd R. Weiss, "Scope of Bank Data Theft Grows to 676,000 Customers," *Computerworld.com*, May 20, 2005, found at http://www.computerworld.com/databasetopics/data/story/0,10801,101903,00.html.
[29] Jonathan Krim, "Banks Alert Customers of Data Theft," *Washington Post*, May 26, 2005.
[30] Ivan Schneider, "Protecting Bank Data Requires Internal Security Measures," *Security Pipeline*, May 3, 2005, found at http://www.securitypipeline.com/showArticle.jhtml?articleID=162100977.
[31] Eric Dash, "Lost Credit Data Improperly Kept, Company Admits," *The New York Times*, June 20, 2005, found at http://www.nytimes.com/2005/06/20/technology/20credit.html?adxnnl=1&oref=login&adxnnlx=1119543522-kWvypraZ8alA9q0xdou8sA.

breach is estimated to have compromised the consumer records of roughly 40 million U.S. cardholders.

Federal Deposit Insurance Corporation (FDIC)

In June 2005, the FDIC informed approximately 6,000 of its employees that their personal information may have been compromised as much as 18 months earlier. The data potentially compromised included social security numbers, names, birth dates and salary information of employees hired as of July 2002. The agency said in a "small number of cases" the information had been used to apply for and receive fraudulent loans from an unidentified credit union. The FDIC did not say when it had learned of the security breach or why it waited to tell employees about it.[32]

Other Cases

In one extraordinary case of identity theft, the perpetrator charged more than $100,000 of credit card debt, obtained "a federal home loan, and bought homes, motorcycles, and handguns" – all in the victim's name.[33] The convict also called his victim to taunt him—"saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time."[34] He subsequently filed for bankruptcy in the victim's name. The victim spent more than four years and $15,000 to restore their credit while the perpetrator served a brief sentence for making a false statement to obtain a firearm.[35] The perpetrator made no restitution to his victim for any of the harm he had caused.[36]

In another case of identity theft, Ms. Mari Frank testified before the United States Senate Committee on Commerce, Science, and Transportation that she was a victim of identity theft in 1996. In her testimony, she stated that:

> While wrecking my credit, she also destroyed my sense of security and peace of mind. My impersonator obtained over $50,000 using my name, purchased a red convertible Mustang, and even caused me to be threatened with a lawsuit by a rental car company for the auto that she damaged in an accident. It took me almost a year and over 500 hours to clear my records and regain my credit and my life. I accumulated five banker boxes of correspondence, and lived in fear of how else this invisible person might harm me and my children.[37]

---

[32] Jonathan Krim, "FDIC Alerts Employees of Data Breach; Intrusion Occurred in 2004," *Washington Post,* June 16, 2005.
[33] Department of Justice, Identity Theft and Fraud," (last modified: June 5, 2000), *at* http://www.usdoj.gov/criminal/fraud/idtheft.html.
[34] Id.
[35] Id.
[36] Id.
[37] See Ms. Mari Frank, testimony before the United States Senate Committee on Commerce, Science, and Transportation, hearing on Identity Theft and Data Broker Services, May 10, 2005.

Data Security Standards

The various methods used to steal consumers' private data from data brokers, as well as other companies that maintain consumer files containing private information, demonstrate that there is little regulation over how these institutions protect the storage and transfer of this valuable information. With little regulation, there is little incentive for data brokers to use due diligence in determining that their customers are who they say they are.

In fact, data brokers have almost no accountability for how they collect the information and to whom they sell it because there are currently no Federal standards regulating the commercial data broker industry.[38] The Electronic Privacy Information Center (EPIC) is a data privacy advocate that sent a letter to the Federal Trade Commission urging it to regulate data brokers. In a December 16, 2004 letter, Associate Director Chris Hoofnagle observed:

> Under the self-regulatory scheme erected by the now defunct Individual Reference Services Group, commercial data brokers choose who is eligible to buy personal information. This is a subtle but important deviation from the Fair Credit Reporting Act's approach, which tends to approve record disclosure based on the use of the information, rather than the identity of the purchaser … As a result, ChoicePoint and other information brokers can create ties with marginal businesses ...ChoicePoint's customers can pull information on almost anyone without having to declare their legal justification or entitlement to the data.[39]

The Case for Notification

Currently, most victims find out about their identity theft because they have experienced its consequences. Notification about information breaches can give consumers an opportunity to monitor their credit files more closely in the event criminals use the stolen information. Continued monitoring is important because criminals sometimes wait six to twelve months (well past the "fraud alert" period) before using the stolen information.[40] A notification requirement would give consumers a powerful preventative tool and it could also motivate businesses to strengthen their security practices. Businesses which experience a data breach now would receive even greater public scrutiny since their customer base would be more aware of their security practices.

Currently, there are approximately 20 states that have enacted or are in the process of enacting notification provisions, but there is no Federal notification law.[41] It was only because of the enactment of California's notification law that the ChoicePoint breach came to light.

---

[38] Angie Welborn, "Information Brokers: Federal and State Laws," May 17, 2005. Washington, D.C.: Congressional Research Service, (RS22087), 1.
[39] Electronic Privacy Information Center, EPIC Letter to the FTC, found at http://www.epic.org/privacy/choicepoint/fcraltr12.16.04.html.
[40] Jonathan Krim, "FDIC Alerts Employees of Data Breach," *Washington Post*, June 16, 2005.
[41] Angie Welborn, "Information Brokers: Federal and State Laws," May 17, 2005. Washington, D.C.: Congressional Research Service, (RS22087), 2.

Subsequently, Attorneys General from 38 other states demanded that ChoicePoint "do for their states' residents what they did for Californians."[42]

STOLEN IDENTITIES AS WEAPONS

Information breaches and identity theft incidents are particularly troublesome because they show the ease with which terrorists could use these strategies. Terrorists can access an individual's private information with little effort. To prove this point, activist Betty (BJ) Ostergren created a website on which she posts prominent individuals' social security numbers, or links to them. House Majority Leader Tom DeLay's (R-TX) social security number can be found on the Internet because of a tax lien filed against him in 1980.[43]

For terrorists, access to such information is important because it allows them to assume another person's identity. According to the National Commission on Terrorist Attacks Upon the United States, identity fraud is one method by which terrorists evade detection.[44] Most businesses and government entities require individuals to present a social security number and a photo identification to conduct most daily activities from renting apartments or opening bank accounts to potentially dangerous activities such as purchasing firearms. In the past, criminals often stole legitimate identification documents and passed them off as their own or created counterfeit documents. Today, criminals are using off-the-shelf technology to manufacture more realistic counterfeit IDs that are hard to differentiate from the numerous legitimate versions of documents issued by governmental agencies.

From September 2002 through May 2003, the GAO conducted several undercover investigations using counterfeit "breeder" documents and driver's licenses to determine whether counterfeit documents could be used to enter the country or access federal buildings.[45] A breeder document is one that would allow access to other forms of legitimate identification for establishing a false identity. For example, if a green card or social security card were fraudulently obtained under a false identity it could then be used to get a driver's license in some states. These counterfeit documents were used to enter through ports of entry around the country. The GAO found its undercover operations were 100 percent successful.[46] More recently, U.S. Immigration and Customs Enforcement investigators arrested two men in Mississippi for attempting to sell fraudulent IDs to a source posing as an individual with terrorist connections. The documents had been created by the men in a hotel room using store-bought technology, including computers and printers.[47]

---

[42] Associated Press, "38 AGs Send Open Letter to ChoicePoint," February 18, 2005.
[43] Jonathan Krim, "A Matter of Public Record," *Washington Post*, May 25, 2005.
[44] The National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report," August 2004, 384.
[45] U.S. General Accounting Office, *Security: Counterfeit Identification and Identification Fraud Raise Security Concerns*, GAO-03-1147T (Washington, D.C.: U.S. General Accounting Office, September 9, 2003), 7.
[46] Id at 2.
[47] Department of Homeland Security, U.S. Immigration and Customs Enforcement press release, "Two New Orleans Men Admit Offering to Sell False Identities to Assist Members of Terrorist Organization," February 28, 2005.

FUNDING FOR TERRORIST OPERATIONS

Terrorists also steal identity information to gain access to credit or cash that can be used to finance their operations. As Dennis Lormel, Chief of the Terrorist Financial Review Group at the Federal Bureau of Investigation (FBI), noted during a Senate hearing:

> Terrorists and terrorist groups require funding to perpetrate their terrorist agendas. The methods used to finance terrorism range from the highly sophisticated to the most basic. There is virtually no financing method that has not at some level been exploited by these groups. Identity theft is a key catalyst fueling many of these methods.[48]

For example, several of the 9/11 hijackers used a variety of methods to steal credit card information, such as "counterfeit trademarked goods, consumer coupon fraud, drug trafficking, insider trading, support from Gulf-area governments, and conflict diamonds."[49]

In 2002, terrorist Imam Samudra organized a series of bombings in Bali nightclubs that killed 202 people. Most of those killed were foreign visitors. Samudra partially financed the operation through online credit card fraud, according to the Indonesian police.[50] After his conviction, Samudra wrote a book from prison that included a chapter with instructions on how to commit credit card fraud.[51] According to reports, suspected terrorist cells operating North America and Europe have used many different "scams to steal millions from credit card companies."[52] The groups then use these funds to support their activities and to send money to Middle Eastern terrorist groups.[53]

The FBI also reports that al Qaeda terrorist cells hiding in Spain used stolen credit cards to make numerous purchases, being careful to keep their spending below levels at which identification would be needed. False passports and travel documents were used extensively to open bank accounts for routing money through Pakistan and Afghanistan for the mujahideen movement.[54]

---

[48] See Dennis M. Lormel, Chief, Terrorist Financial Review Group, FBI, testimony before the Senate Judiciary Committee, Subcommittee on Technology, Terrorism and Government Information, hearing on S. 2541, "The Identity Theft Penalty Enhancement Act," July 9, 2002.
[49] John Roth, Douglas Greenburg, and Serena Wille, "National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission," August 21, 2004, 19.
[50] Alan Sipress, "An Indonesian's Prison Memoir Takes Holy War into Cyberspace," *Washington Post Foreign Service*, December 14, 2004.
[51] Id.
[52] Todd Lighty, "Fraud, ID Theft Finance Terror," *Chicago Tribune*, November 4, 2001.
[53] Id.
[54] See Dennis M. Lormel, Chief, Financial Crimes Section, FBI, testimony before the House Committee on Financial Services, Subcommittee on Oversight and Investigations, hearing on the PATRIOT Act oversight, Investigating Patterns of Terrorist Financing, February 12, 2002.

SUMMARY

The high-profile data security breaches addressed in this report undermine public confidence in the data security practices of many U.S. companies and heighten consumers' concerns about becoming potential victims of fraud and identity theft. The public is appropriately concerned about the increasing number of identity thefts[55] since millions of consumer files held by data brokers have been stolen or otherwise compromised though the use of a wide and inventive array of tactics. These problems illustrate the data broker industry's shocking lack of security standards and practices and it is clear the American people want the Federal government to take concrete steps to enhance data security and help consumers better protect their private information.

Consumers need stronger federal protections against improper collection and sale of sensitive consumer information and advanced warning when their personal information has been put at risk. That is why Congress should enact legislation that addresses the following data security gaps:

Regulation of Data Brokers: Expand the Fair Credit Reporting Act (FCRA) to cover data brokers, such as ChoicePoint and LexisNexis, requiring them to operate by the same information sharing standards and consumer protections as consumer reporting agencies;

New Data Security Standards: Require similar data security obligations and standards for data brokers and credit reporting agencies as those required of regulated financial institutions in the Gramm-Leach-Bliley Act;

Uniform Data Breach Notification: Establish uniform requirements for data brokers, consumer reporting agencies and financial institutions to notify consumers following a breach in any data system in which sensitive consumer information has been obtained by an unauthorized party and is likely to be misused; and

Notification by Merchants: Place a greater level of responsibility on retail merchants to protect their customers' account payment information by requiring that any business that routinely collects and maintains customer credit card, checking or other payment information must notify customers or their financial institutions when financial account information has been obtained and is likely to be misused by unauthorized parties.

[55] Cyber Security Industry Alliance, "Internet Security Voter Survey: A Call for Coordinated Action," June, 2005, 6.