CORPORATE AMERICA AND CONSUMER PRIVACY: THE PRICE OF GREATNESS IS RESPONSIBILITY

VICKI M. LUOMA*
PENNY HERICKHOFF**

I. INTRODUCTION

It has almost become a cliché to speak of how the Internet has posed serious threats regarding identity theft. While most of the discussion has centered on securing individual transactions that take place every day online, the greatest vulnerability for the widespread threat of identity theft is the reluctance of the credit and finance industry to change their way of doing business in light of the technological advances in recent years. This paper examines widespread identity theft by computer hackers breaching the security of information warehouses and stealing consumers' private credit card and social security information. Various approaches to self-regulation by the industry are reviewed, as well as federal and state legislative approaches to the threat of identity theft. The conclusion proposes a combination of available legislation and existing technology as a solution to this problem.

II. THE PROBLEM

The Federal Trade Commission reports that identity theft has been the number one consumer complaint for the last five years. Identity theft costs businesses $55 billion a year, which ultimately costs the consumer in increased prices for goods and services. According to the FTC, complaints of Internet-related identity theft in 2005 tripled to 1,000. While that accounts for only a fraction of the 160,000 reports of identity theft nationwide, that growth rate is still alarming. On average, Internet-related identity theft costs victims about $800 and 175 hours to clean up.[754] According to a survey by Price Waterhouse, nearly one half of the fastest growing companies in the United States have suffered a breach of data security in the past few years. Other statistics show that there are 7.8 severe attacks per every 10,000 security events (Financial Service Industry). Clearly, this problem is serious and it is getting worse.[755]

The primary villains are *hackers*, the term used for people who gain unauthorized access to another's computer or electronic data for the purpose of stealing or corrupting the data. In the early days of computing, the biggest problem may have been bored teenagers, but now it is truly a high-tech crime of epic proportions. This problem is not simply a few criminals perpetrating a few crimes, but criminals who hold themselves out for hire. If one wants the database of a particular company, one need only place an order for it. Hackers have even been known to operate out of a

* J.D., Assistant Professor, Minnesota State University, Mankato.
** J.D., L.L.M., Professor, Minnesota State University, Mankato.
[754] Federal Trade Commission Home Page, http://www.ftc.gov (last visited Feb. 27, 2006).
[755] *Id.*

foreign country, steal data from companies, and then blackmail those same companies by merely threatening to steal their data.

The real victims in this situation are the consumers. One of the biggest problems for consumers is that they are powerless to control the widespread dissemination of their private data. Financial institutions are legally allowed to transmit consumer information to third party information brokers without the knowledge of or the consent of consumers. Not only do the consumers' banks, credit institutions, schools, employers and the government have consumer data, but there are over 1,000 information brokers that collect personal data.[756] Some of the larger brokers include ChoicePoint, Intelius, ZabaSearch, and Acxiom. These information brokers are virtually unknown to consumers and virtually unregulated. One information broker alone, ChoicePoint, has data on at least four out of five consumers.[757] There is a substantial incentive for companies not to inform consumers when a breach occurs. If the public were made fully aware of how often consumers' information was breached, consumers would lose confidence in financial institutions and their government's ability to protect their interests.

The list of the companies that have suffered security breaches in the past year alone is too lengthy to discuss in this paper, but some incidents are worthy of note. In February 2005, eight million credit card numbers were accessed by hackers attacking DPI, a payment processing company that handles transactions for VISA, MasterCard, Discover and American Express.[758] In May 2005, one of the worst data security breaches occurred when computer hackers accessed more than 10 million Visa, MasterCard and American Express credit card account numbers from the computer system of CardSystems, a third-party payment company. CardSystems, contrary to its contractual obligation with MasterCard, VISA and American Express, stored data on individual card users. The data stored included names, addresses, purchases, and card numbers. CardSystems not only stored the data on 40 million credit cards, but also did not encrypt it. Consumers were not notified of the breach. Most consumers were not even aware that their information was being processed by a third-party company, let alone being stored by one.

Another serious breach of data security accomplished by social engineering involved ChoicePoint, another third-party information broker. ChoicePoint, a NYSE company, is a spin-off of Equifax. ChoicePoint was approached by what it believed to be a Nigerian credit bureau seeking to purchase credit data. In fact, ChoicePoint had been approached by an individual whose sole intent was to defraud the individuals whose data he would acquire. That data security breach came to the public's attention only because of the California law that required notification of consumers.[759]

It seems that no company is immune from these debilitating breaches of information security. In December 2005, Guidance Software, one of the leading security companies that creates anti-hacking software and the developer of EnCase computer forensics software, had its electronic records hacked. Hackers were able to compromise 3,800 customers' credit cards as well as other financial and personal data. Guidance Software's customers include law enforcement agencies and personnel as well as network security professionals. Once again, this case became public knowledge only because of the California law requiring public disclosure and notification of a serious breach of security.[760]

Clearly, identity theft arising from information security breaches facilitated via the Internet has become too widespread for comfort. It is no longer an isolated and rare occurrence. The most serious of these breaches have involved third-party data brokers who appear to hackers to have a

[756] Sandra Lysecki, *Privacy Commissioner Calls on Compliance*, 21 COMPUTER DEALER NEWS 15, 15-17 (2005).
[757] Kenneth Reed, *Data Protection Disaster Looms for Thousands*, 25 ACCOUNTANCY AGE 21, 21-27 (2005).
[758] *Id.*
[759] Pam Greenberg, *No Easy Fix for Identity Theft Problem*, 31 STATE LEGISLATURE, 29-30 (2005).
[760] Nikki Swartz, *Viruses on Rise, but Are Companies Liable?* 38 INFORMATION MANAGEMENT JOURNAL 3 (2004).

plethora of data that can fuel identity thieves. While there are no perfect solutions in the world of information security, the targets of these hackers could do much more to protect consumers' private information than they are now doing. The industry prefers self-regulation to regulation by Congress or the states. Before examining the state of both federal and state law, the matter of self-regulation of this industry will be considered.

III. SELF-REGULATION

Some of the third-party corporations in the credit card information industry have taken action to self-regulate. In June 2005 a data security standard for all merchants handling credit data sponsored by MasterCard, Inc. and Visa, Inc. was mandated for all companies accepting those credit cards. This standard was established by several credit card associations and was a combination of two other standards in place–the Visa Cardholder Information Security Program and the MasterCard Site Data Protection Program. Both of these programs require all companies that accept those credit cards to comply with twelve security mandates, including data encryption. Failure to comply with these standards could result in fines of up to $500,000 per incident if the credit card data is breached.[761] The problem with this tough-sounding mandate is that most merchants are left to self-assess their systems. Only the largest companies processing over $6 million of MasterCard and Visa transactions per year should submit to an outside audit. Although this requirement is a step in the right direction, the standards are more for show than compliance. Unless enforcement is audited by an independent security expert, the standards are only as good as the merchant that self-assesses them. More importantly, even if all merchants comply with these twelve security steps, as soon as a third-party processor who is not bound by these standards becomes involved, that third party becomes the weakest link in the chain; and hence, the third party becomes the prime target of the hackers.[762]

Some companies' answers to the hacking problem are to require customers to waive their rights to sue for negligence. American Airlines and Verizon both require consumers to sign waivers of any lawsuits or damages due to their data being hacked. Often these waivers are on lengthy click-on contracts that consumers rarely read or understand. The policies are contrary to the public interest and contrary to good corporate ethical policy. Requiring the public to waive its rights to sue for the companies' wrongdoing before doing business with the consumer is simply unconscionable. Unfortunately, the self-regulation standard appears to be little more an effort to hold off tough legislation and simply a public relations diversion. Self-policing rarely works in most industries; and in this industry in particular, it has been a failure so far. Accordingly, the best answer for the consumer appears to be legislation.

IV. THE STATE OF THE LAW

A. FEDERAL LAW

Congress has not been derelict in passing legislation addressing the problems posed by these serious information security breaches. There are several federal laws that attempt to solve this problem, including the Identity Theft and Assumption Deterrence Act of 1998 (S1408), the Computer Fraud and Abuse Act (1984), the National Information Infrastructure Protection Act, the Gramm-Leach-Biley Acts, the U.S. Patriot Act, HIPAA, Sarbanes-Oxley, the Federal Information

[761] Nikki Swartz, *Markey Seeks Protection for Outsourced Data*. 39 INFORMATION MANAGEMENT JOURNAL 6, 6-7 (2005).
[762] John McPartlin, *Hackers Find Backers*, 22 CFO 75, 75-77. (2006).

Security Management Act of 2002, and the Electronic Communication Privacy Act, among others.[763]

First, the Identity Theft and Assumption Deterrence Act of 1998 makes identity theft a federal crime with penalties of up to fifteen years' imprisonment and a maximum fine of $250,000. This act does make the person whose identity was stolen a victim who can seek restitution if a conviction is secured.[764]

Second, the Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) requires the Department of Health and Human Services (HHS) to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also covered security and privacy of health data.[765]

Third, in response to continual threats from computer hackers Congress passed the Computer Fraud and Abuse Act in 1984. The act was passed to protect federal interests and to protect the federal government's computers and financial information as well as information on computers of financial institutions. As more hacking issues presented themselves, and as the issues presented by terrorism surfaced, the act was amended and rewritten. In one amendment, subsection (g) was added to assist private companies in pursuing computer hackers. This section was a significant addition and expanded the scope of the law substantially. Subsection (g) reads as follows:

> (g) Any person who suffers damage or loss by reason of a violation of the section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. Damages for violations involving damage as defined in subsection (e) (8) (A) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage.

In spite of the broad powers conferred by this statute, companies have failed to use this act to pursue hackers. Essentially, corporations have determined this law does not provide a cost-effective basis for pursuing hackers, nor does it paint them in a flattering light if they do take action against hackers. Either action would require companies to reveal too much information. Specifically, they would likely have to reveal how much information they pass on to third parties and how serious of a breach of their systems they suffered. It is also unlikely that any individual hacker would have a deep pocket that might justify litigation. Most companies still fail to report break-ins or cooperate with the law enforcement agencies for fear of losing customers or their reputation.[766]

The federal government thought it had solved the problem of companies refusing to cooperate with the passage of Section (g) of the Computer Fraud and Abuse Act that permits them to pursue hackers. Instead of pursuing hackers, companies have used this Act to pursue their own employees for unauthorized access to company computers. They have yet to pursue a hacker. None of the present or proposed laws makes it a crime for any company to fail to notify the police of computer security breaches or require any company to cooperate with legal investigations of such breaches.[767]

[763] Financial Services Modernization Act, 15 U.S.C. § 6801.
[764] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
[765] HIPPA, Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320.
[766] The Affordable Transaction Account Act: Hearing on HR 4490, the First Accounts Act of 2000 And HR 4584, before the Committee on Banking and Financial Services, Honorable James Leach, Chairman (June 27, 2000) (testimony by Edmund Mierzwinski, Consumer Program Director, U.S. PIRG).
[767] Computer Fraud and Abuse Act, 18 U.S.C. § 1030.

Fourth, Sarbanes-Oxley was passed in response to the Enron and Arthur Andersen debacles. In addition to the highly touted provisions regarding CEO and CFO responsibilities, it also requires corporations to take punitive action in response to threats to data security.

Fifth, the National Information Infrastructure Protection Act makes it unlawful to intentionally access a protected computer or to intentionally transmit a program, code or command without authorization.[768]

Sixth and finally, the Financial Services Modernization Act requires financial institutions to protect the security of customers' non-public personal information. The law further requires financial institutions to protect their customers against any unauthorized breach.[769]

The U.S. Patriot Act extends the authority of the law enforcement investigatory tools and authorizes the Attorney General to establish a regional computer security lab.[770]

The Federal Information Security Management Act of 2002, or FISMA, requires federal agencies to implement information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized use. This applies to access, use, disclosure, disruption, modification or disclosure of information used by federal agencies or contractors. The act requires agencies to provide training, conduct periodic tests of policies and procedures as well.[771]

The Electronic Communication Privacy Act (1986) prevents the use of pin registers or traps and trace devices without court orders.[772]

While the current set of federal statutes has provided a broad framework of law and has empowered both the federal government and private corporations and individuals with the tools needed to seek redress in court from hackers, very little action has been taken in that regard. With this situation in mind, and in response to recent significant security breaches of third-party information brokers, Congress is currently considering additional legislation.

B. PROPOSED FEDERAL LEGISLATION

In addition to the foregoing statutes, the following legislation is under consideration as a response to the most recent information security breaches, particularly the one suffered by ChoicePoint. On November 3, 2005, the Data Accountability and Trust Act (hereinafter referred to as DATA) passed by a 13-8 vote along party lines in the Senate Judiciary Committee. DATA would override state mandates such as the Breach Notification Law. The main problem with DATA is that corporations would have to notify consumers of the breach only if they think the customer is at risk of identity theft after their information is breached. In addition to the notification requirement, the proposed bill would require companies to notify the Federal Trade Commission of their plans to safeguard information. DATA is not likely to be effective unless it also empowers the FTC to evaluate corporations' standards of review and to shut down data brokers' operations in the event of an egregious violation. Fines alone are not enough to ensure enforceability. The proposed DATA bill applies only to companies with data on 10,000 Americans or more. It does not allow consumers access to or to correct inaccurate data. The problem with this legislation and most of the proposed legislation is that consumers should have the right to determine how significant the risk is to them without having to rely on third parties whose interests are not the same as theirs. Although some proposals under consideration set the definition of *high risk* at a 50% likelihood of having an identity stolen, the latest version does not attempt to define *high risk*. The Senate Judiciary Committee will likely have to compromise its DATA bill with other committees' proposals, including the Senate Committee on Commerce, Science and

[768] Sarbanes-Oxley Act, 15 U.S.C. § 7241.
[769] Financial Services Modernization Act, 15 U.S.C. § 6801.
[770] U.S.A. Patriot Act, 18 U.S.C. § 1801.
[771] Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541.
[772] Electronic Communication Privacy Act, 18 U.S.C. § 2701.

Transportation's proposed law, the Identity Theft Protection Act, and the Banking, Housing and Urban Affairs Committee's presently unnamed and unfinished proposed act.[773]

C. STATE LAW

State law is far ahead of the federal law in corporate self-regulation efforts. California was the first state to enact a law requiring notification of California consumers when a serious breach in data security has occurred. California's Notice of Security Breach law 1386 passed in 2003 requires notification only to California residents of a breach of security. This statute, codified as Section 1798.82 of the California Civil Code, requires any person or business conducting business in California to provide notice in the event of a security breach of computerized data containing unencrypted "personal information." "Personal information" means an individual's first name or initial and last name in combination with one or more of the following, if any of these data elements are unencrypted: (a) Social Security number, (b) driver's license number or California identification card number, or (c) account number or credit or debit card number, along with any required security code, access code, or password that provides access to that account. If the security of this data is breached, the company is required to provide written notice to every California resident whose personal information may have been accessed.

This law also requires companies to have a reporting and monitoring system to detect breaches. Banks cannot share information with affiliated companies unless they ask consumers' permission and give consumers the right to refuse to share personal data. Further, the company cannot share information with third-party companies unless the consumer agrees. As of November 2005, twenty-one states have passed legislation requiring companies to notify consumers or customers when their sensitive personal information has been acquired by an unauthorized person. Approximately a dozen states have followed California's lead in passing a notice of breach law. [774]

While the state laws do require consumer protection in the event of an information security breach, several problems do exist. First, the state laws cover only notification of residents in their own state. Processing companies handle information for people in all states of the union, so notifying people within a particular state affords protection only to a small percentage of all persons affected by the breach. In addition, many state laws require notification only when the company itself feels there is a significant risk to the consumer of having their identity stolen. By deferring to the data broker the determination of whether a breach poses a significant risk to the public, the statute loses most of its potential effectiveness.

In addition, the California law has been and is still being challenged through the appellate process. One argument against the statute is that the California law violates the Fair and Accurate Credit Transaction Act of 2004, which allows banks to share information with their affiliates. A U.S. District Court upheld the California Statute, but this decision is being appealed.[775]

If a federal law is eventually passed, it would supersede the power of all of the state laws because of the Interstate Commerce Clause of the U.S. Constitution. Since the current federal proposals require companies to notify consumers only when the company determines the consumers' information to be in jeopardy, state law should be allowed to require stricter notification to be effective in protecting the consumer.

V. IMPEDIMENTS TO CONSUMER PROTECTION LEGISLATION

The greatest impediments to federal legislation designed to protect consumers from the threat of identity theft as a result of an information security breach perpetrated against one of the third-party

[773] U.S.A. Patriot Act, 18 U.S.C. §1801.
[774] David Bender and Kevin Barnard, *How to Keep Your Customers After a Data Breach,* 171 AMERICAN BANKER 17, 17 (2006).
[775] Allison Enright, *As Identity Theft Grows, Penalties Reexamined* 39 MARKETING JOURNAL 20, 15-16 (2005).

data brokers are lobbying efforts. The resistance to federal regulation is fierce, and the most powerful lobbyists in Washington have been recruited. For example, ChoicePoint paid lobbyists Akin, Gump, Strauss, Hauer, & Feld (hereinafter referred to as Akin Gump) approximately $320,000 in 2004 and 2005 and $280,000 in 2002 and 2003 to influence lawmakers on this issue. The firm advertises:

> When an industry is threatened or legislative and political reform warrant strategic positioning, we help shape the issues and structure a rational approach. Akin Gump lawyers understand how decisions are made, which arguments will work, how to assemble coalitions, how to advocate legislative action–and when to litigate.[776]

Akin Gump is just one of many law firms that have been retained to influence the legislation in Congress in this area. Information brokers have "an enormous number of [lobbyists] canvassing the Hill with inside connections and massive campaign contributions," says Ed Mierzwinski, Consumer Program Director for the U.S. Public Interest Research Group."[777]

A. The Industry Arguments and Their Counterpoints

The information brokering industry has staunchly resisted regulation at any level and continues to insist that self-regulation is sufficient to allay any concerns that the public may have about information security breaches. The industry has fought the legislative attempts–both state and federal–through a combination of lobbying, persuasion and litigation. The industry puts forth several arguments in support of its position.

First, the industry claims that governmental regulation would end up costing the consumer much more than the proposed benefits by having the industry comply with computer security regulations. In spite of this position on the part of the industry, at the present time, the consumer is already covering all the costs of hacking. Some of that cost is passed on in general to all consumers and some is borne by the individual victim.

Second, the industry has argued that if it were required to cooperate with the government in criminal and civil litigation, the government would have access to sensitive consumer data. This argument is hypocritical since the industry sells the consumer data and shares it without consumers' knowledge anyway. If a government agency offered to purchase the information, the industry would not refuse that revenue.

Third, the industry argues that notification requirements will induce litigious consumers to sue the industry, causing the industry to incur prohibitively high defense costs. In the end, all consumers will suffer as a result when those costs are passed on to the public. What the industry is quick to overlook, however, is that in the absence of statutorily mandated damages, any plaintiff must prove damages in order to prevail in any lawsuit. If a consumer can prove monetary damages as a result of a security breach, why should the consumer not prevail on a negligence claim?

Fourth, the industry claims that notification would be too expensive to comply with and that ultimately the costs would be borne by the consumer. However, consumers will not be fully protected until such time as the industry views the costs of an information security breach to be higher than the costs of implementing more appropriate security policies to prevent hacking.

Fifth, the industry argues that if it had to notify consumers every time there was a security breach, it would overly alarm consumers, causing stress or panic when nothing is likely to happen. The flaw in this reasoning is that the consumer has a right to know everything that affects them. In an incident involving Wells Fargo, consumers were notified that their information was breached and that it was unlikely that their data would be compromised. Wells Fargo offered a new credit

[776] Elliot Freeman, *Disclosure of Information Theft: The ChoicePoint Security*, 14 Information Systems Security 6, 6-10 (2006).
[777] *Id.*

card for anyone who wanted it. Only about one third of the credit card holders requested a new credit card. The industry's real fear is that if the consumers knew the true story, there would be a reason for the consumer to panic.[778]

Sixth, according to an ID Analytics Corp study, only 0.0098 of breached data or 98 out of 100,000 people whose information was breached actually had their identities stolen. MasterCard's spokesperson stated that approximately 1,000 customers out of 40 million had data stolen from CardSystems Solution, Inc. that resulted in identity theft. The problem with this argument is that even if these statistics are correct, it is devastating to the victims whose identities are stolen. Further, if this criminal conduct is not stopped, the numbers will continue to grow. By the way, MasterCard made only a general press release when its data were compromised, but made no individual notifications to consumers. MasterCard announced that it felt that the press release was sufficient notification to consumers.[779]

Seventh, another argument offered by the industry is that the so much information is obtained in each breach that it would take 40 years for one person to use it all. Thus, it is only a remote possibility that a particular consumer's information would be stolen.[780] If this is accurate, the industry would have limited damage exposure if sued by the consumers victimized by negligent security efforts.[781]

Eighth, the final argument propounded by the credit industry is that consumers' family members and friends are a larger risk than industry negligence for identity theft. Even though this statement is true, the existence of another potential threat to consumer identity does not excuse or justify the credit industry's lack of security and the resulting threat to consumer identities. The threat posed by friends and family is not universal to every cardholder, but the credit industry's failure to prevent hacking is a universal threat to all consumers.[782]

Although the industry opposes legislation, it prefers federal legislation to state legislation. The basis for this position is the need for uniformity. Current proposals in Congress are not strong enough to provide effective consumer protection. Unless and until there is a change of sentiment on the part of federal legislators, state laws are more likely to offer significant protection to consumers.

B. A Proposed Solution

Any effective solution to the identity theft problem should protect the interests of the industry and the consumers. Both Congress and the credit industry should work collaboratively to eradicate this problem. Both need to act ethically and not just legally in this action.

Congress should pass legislation more like that of the European Union's (hereinafter referred to as EU) tough privacy laws. In the EU, consumer data can be collected only for a specific purpose and can be kept only so long as absolutely necessary for that purpose. EU law does not allow transfer of private data to a third party without consumer agreement. Congress would undoubtedly receive a significant amount of resistance to this legislation because data brokers in the United States are a multi-billion dollar business.

The EU has not considered United States systems secure. The EU requires creation of government data protection agencies, registration of databases with those agencies, and, in some instances, prior approval before personal data processing may begin The Department of Commerce negotiated with the EU to establish safe harbor laws. The European Commission's Directive on

[778] Bruce Schneier, *Risks of Third-Party Data*, 48 Communications of the ACM 136, 136-8 (2005).
[779] Jaikumar Vijayan, *Credit Reporting Firm Hit by Theft of Confidential Data*, 39 Computerworld, 12-17 (2005).
[780] Andrew Miller, *Lost Data Doesn't Necessarily Lead to Crimes*, http://www.idanalytics.com/pdf/BankInfoSecurityLostDataDoesntNecessarilyLeadtoCrimes011006.pdf. (last visited Feb. 22, 2006).
[781] Kevin Reed, *Data Protection Disaster Looms for Thousands*, 3 Accountancy Age 3 (2005).
[782] *Data Protection Challenge Is Not Ever Going Away*, 26 New Orleans City Business 21 (2005).

Data Protection went into effect in October 1998, and prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection.[783]

Under the Safe Harbor Law, the United States is required to provide notice, disclosure, choice, and access to customer information. There are also other more restrictive provisions for financial institutions. All companies dealing with such data should certify that they are in compliance with provisions of the Safe Harbor Law. Specifically, the Safe Harbor Law requires the following:

> Notice: Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.
> Choice: Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.[784]
> Onward Transfer (Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent(1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
> Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
> Security: Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
> Data integrity: Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.
> Enforcement: In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.[785]

[783] Stephanie Godof, *What Is an Employer's Exposure When Doing Business in Europe?* 31 EMPLOYEE RELATIONS LAW JOURNAL 3 (2005).

[784] Michele Mullins and Luke Mullins, *Data Bill Gets Partisan OK; Panel Vows Privacy Next* 170 AMERICAN BANKER 1, 1-3 (2005).

Under the Federal Trade Commission Act, for example, a company's failure to abide by commitments to implement the safe harbor principles might be considered to be deceptive and actionable by the Federal Trade Commission. Companies that are not in compliance will lose their rights to data flow to Europe. If the companies can comply with data safeguards with European companies and consumers, then they can certainly make the same safeguards for United States consumers. In fact, the federal government should take these safeguards a step further and negotiate with Europe and the rest of the world to set up extradition and prosecution treaties when companies have been discovered to have violated these provisions.

Congress needs to pass stricter privacy laws that are not tied to technology but are simply privacy-oriented. Consumer privacy should be protected regardless of the form and consumers should at least have the right to consent to the dissemination of their private data. Congress needs to pass laws that allow consumers to place security freezes on their credit data. A security freeze would allow a consumer, especially one who has had his or her identity compromised, to freeze access to his or her credit report. No one, including the consumer, could receive instant credit. Credit could be obtained only after the consumer provides additional information. Credit companies are fighting this effort because they argue that it is inconvenient for consumers. The industry also asserts that consumers' ability to tag their credit file with fraud alerts is sufficient protection. The problem with fraud alerts is that creditors can choose to ignore them and give credit anyway.

Consumers should be notified if there is a breach of information and allowed to determine for themselves the extent of their liability, exposure, and risk. As further protection for consumers and as an incentive to the industry, a company affected by such a breach should be responsible for any costs in repairing the damaged credit and should be required to provide free credit monitoring services to the consumer for three years. Companies should not be allowed to require customers to sign or click away their legal rights in case of security breaches. Companies should always be responsible for their negligence as an incentive to correct their problems. It should be unconscionable not to do so.

The industry should be required to report all breaches to the FBI and fully cooperate in the investigation and prosecution of all criminals. Companies that do not comply should be subject both to criminal and civil penalties that include large fines and punitive damages. The costs of failing to comply should be high enough to dissuade companies from considering that option viable. Individual executives within the company also should be personally liable for failure to notify legal authorities. Data and information brokers should be included in all legal consequences including criminal and civil penalties. They should be under the same regulations as financial institutions. In addition, any company using data and information brokers that suffers a consumer information breach should be held civilly liable under the theory of agency and should face criminal charges.

Companies should set aside assets to find, detect and pursue hackers. As an act of corporate civil responsibility, the industry players should notify and cooperate with federal authorities regarding breached data and cooperate with prosecutors, even if the law does not require it. They should pursue hackers under the CFFA even if it is not cost-effective in the short term. They need to make examples of the hackers to deter other potential hackers in the future. A good example of this approach is how the music industry pursued people of all ages for pirating music through

[785] *Id*.

Napster. They required each defendant to pay a settlement of at least $1,000 before dismissing their suits. The settlement undoubtedly did not cover the cost of investigation, pursuit and prosecution, but the individual settlements were enough to put an end to Napster's problem by setting examples for those who saw the consequences of their actions. The same approach could make examples of hackers for other potential hackers.

Another key element of the solution to this problem is encryption. If all sensitive data were encrypted, hackers would be faced with a much more difficult problem after breaching security. Encryption is the translation of data into a code. To read the data, the reader must have the proper decryption key. Multiple layers of encryption could relatively easily make the problem insurmountable for hackers. Unfortunately, most companies fail to encrypt data. Only 16% of North American companies implement data-at-rest encryption for company databases and only 48% use encryption for data in motion encryption.[786]

Another problem is that companies are often inconsistent in the data that are encrypted. Many companies encrypt credit card numbers but do not encrypt social security numbers. There is no current law requiring the encryption of social security numbers so even in the cases where credit card data are encrypted, social security numbers are not. A law requiring all data to be encrypted would dramatically increase the level of safety and protection of the data. Whether or not there is a law, companies should encrypt all data and companies should properly manage encryption keys. There should also be regular security audits by outside security experts.

Another technique that could enhance the security of the data with or without encryption is data masking. Data masking, the process whereby information in a database is de-identified, creates realistic databases without the risk of exposing sensitive information to unauthorized users. Data masking allows organizations to avoid the costly consequences and penalties associated with data breaches. Additionally, data masking has unique benefits including providing data protection, ensuring compliance with privacy legislation, and maintaining client confidence.

Finally, a key component of the long-term solution of securing credit transactions is the use of biometrics. Biometrics involves the use of unique measurable biological characteristics of each individual. While there are many biometric characteristics that can be measured and used, including fingerprints and retinal patterns, perhaps one of the most promising biometric characteristics is iris patterns. Each individual's irises have unique and complex patterns that do not change with age. These patterns can be encoded and verified each time a transaction occurs. Such an approach would render a lone credit card number useless without the biometric measurement provided at each transaction. Online transactions would require a biometric scanner to be available to the consumer. For that reason, biometrics is more likely to be part of a long-term solution than a short-term solution.

VI. CONCLUSION

It is clear that the two most important vulnerabilities in our information system infrastructure resulting in a significant threat of identity theft on a wide scale are the lack of appropriate information security on the part of information brokers and the lack of emphasis on privacy rights of consumers in how that information is handled. Before the Internet became the force that it is, the existing system of processing credit transactions did not pose the risk that it does today. With the advent of the Internet, old ways of doing business should be revised.

The industry asserts that it can adequately counter the threat of widespread identity theft through self-regulation in lieu of legislative regulation. Thus far, however, self-regulation has been ineffective largely because third party information brokers are not held to strict standards for security. Further, existing federal legislation has not had the anticipated effect on the problem.

[786] Rebecca Herold, *Movie Goddess Encryption Lessons*, 2 COMPUTER SECURITY INFORMATION 4, 4-8 (2006).

The most effective legislation has been enacted by various states, most notably California, but its positive impact is limited exclusively to California residents.

The most promising approach to legislation would be to enact a European Union style of statutory protection based on individual privacy rights at the federal level. This legislative approach focuses on privacy rather than technology. The credit and finance industry can retain information regarding financial transactions only so long as it is absolutely necessary and cannot warehouse the information as is commonly done in the United States. Further, any breaches of information security should be disclosed to the individuals who may be affected.[787]

Coupling this legislative approach with some technological improvements such as data masking and encryption for data at rest and for data in motion and introducing biometric protections would virtually eliminate the threat of widespread identity theft.

The greatest impediments to implementing both the legislative and technological fixes to this problem are the lobbying efforts of the industry. Their priorities do not lie with the interests of the consumers in spite of the fact that without the consumer they would have no reason to exist. It is time that the credit and finance industry recognize that the price of greatness is responsibility to consuming public.

[787] Allen Sheikh, *The Data Protection (Amendment) Act*, 22 EUROPEAN JOURNAL OF HEALTH LAW 4, 4-8 (2005).