



YOUR GROWING EXPOSURE FOR IDENTITY THEFT RISKS

By Kirk J. Nahra¹

Identity theft has become a problem of enormous proportions in the United States. According to the Federal Trade Commission, nearly 10 million people fall victim to identity theft annually, costing consumers \$5 billion in out-of-pocket losses and businesses \$48 billion. For these individuals, the problems range from loss of credit to problems with medical history records and even potential wrongful exposure to criminal prosecution. The FTC's most recent study found that identity theft victims cumulatively spent almost 300 million hours – or an average of 30 hours per person – correcting their records and “reclaiming their good names.”

Identity theft is not only an issue affecting individual consumers. As awareness of identity theft grows, companies across the country, in virtually all industries, are facing significant regulatory and liability risks related to identity theft because the behavior of companies in protecting information entrusted to them is perceived as a major cause of identity theft risks. As the Federal Trade Commission has stated,

These days, it is almost impossible to be in business and not collect or hold personally identifying information — names and addresses, Social Security numbers, credit card numbers, or other account numbers — about your customers, employees, business partners, students, or patients. If this information falls into the wrong hands, it could put these individuals at risk for identity theft.

Accordingly, **for any company that maintains information on employees or customers – information that could provide the basis for identity theft – it is critical to understand the problem of identity theft and to begin to take steps to reduce these risks now, as much as possible.**

¹ Kirk J. Nahra is a partner with **Wiley Rein & Fielding LLP in Washington, D.C.**, where he **specializes in privacy and information security litigation and counseling for companies facing compliance obligations in these areas.** He is the Chair of the firm's Privacy Practice. He serves on the Board of Directors of the International Association of Privacy Professionals, and edits IAPP's monthly newsletter, *Privacy Officers Advisor*. He is a Certified Information Privacy Professional, and is the Chair of the ABA Health Law Section's Interest Group on eHealth, Privacy & Security.



I. WHY ALL THE WORRY ABOUT IDENTITY THEFT?

The environment surrounding the protection of personal information and risks from identity theft has changed enormously in just the past year. Almost every week, we now see extensive publicity surrounding substantial security breaches – in all kinds of industries.

In just the past few months, we've seen the following headlines:

- Hackers Breach Northwestern computers (Chicago Tribune)
- 84% of the North American Enterprises Suffered a Security Breach in the Last 12 Months (Sarbanes-Oxley Compliance Journal)
- Security Breach: 26,000 USDA employees' IDs at risk (Federal Times)
- Data Theft at Nuclear Agency Went Unreported for 9 Months (New York Times)
- Data Theft Affected Most in Military (The Washington Post)

These headlines follow some of the most egregious cases in recent years, including the following highly publicized incidents:

- The ChoicePoint incident

ChoicePoint Inc. revealed that it had sold the personal information, including Social Security numbers, of 145,000 individuals to a criminal ring posing as small businesses. The theft and the FTC's subsequent action against ChoicePoint made front page news (including ChoicePoint's agreement to pay a \$10 million fine and to establish a \$5 million fund for victims of identity theft, while instituting new security measures designed to protect personal information in the future).

- LexisNexis

Intruders accessed personal information for more than 310,000 consumers in a database owned by LexisNexis. The hackers compromised the log-ins and passwords of a handful of legitimate customers to gain access to the database.

- Laptop Problems



The University of California at Berkeley reported the theft of a laptop computer containing the names and Social Security numbers of 98,000 graduate students and applicants. None of the information was encrypted.

- Employee risks

A contract employee illegally downloaded the names and Social Security numbers of 27,000 former and current Blue Cross and Blue Shield of Florida employees to his home computer.

- Lost Data

CitiFinancial notified 3.9 million of its customers that computer tapes containing their account information, payment histories, and Social Security numbers had been lost. The tapes had been shipped via UPS to a credit bureau facility, but were lost in transit. CitiFinancial assured customers that the tapes would be difficult to decode without special equipment and software.

- Human Error

- An employee of Montclair State University accidentally stored the Social Security numbers and declared majors of 9,100 MSU students on the university's web server, thinking that it was inaccessible to the public. The human error allowed the information to be searched and indexed by search engines, exposing it to the world.
- A firm under contract with the Farm Service Agency's Kansas City Administrative Office accidentally released the Social Security numbers of 350,000 participants in the tobacco buyout program to eight Freedom of Information Act requesters.
- Discarded bank and credit card account information for 240,000 subscribers of The Boston Globe was accidentally recycled into paper used to print routing slips. More than 9,000 individual routing slots used to label bundles of a sister newspaper were distributed with the personal information displayed.

These problems cross industry lines – and virtually no industry is immune, whether commercial, government or non-profit. The theft at the Department of Veterans Affairs - involving sensitive data of more than 26 million veterans - is probably the biggest single breach in history. There have been widespread recent reports about a security breach involving the American Red Cross, where an employee gained unauthorized access to Social Security numbers and other personally identifying information from blood donors, and allegedly used this information to obtain credit cards and other accounts. Similarly,



the YMCA of Greater Providence announced that a laptop computer was stolen containing personal information (including Social Security numbers and credit card numbers) for more than 65,000 members. We also have seen cases involving employee theft of personal data and, in one bizarre case, criminal charges against an employer, a former Northern California restaurant owner, who was indicted for stealing her employees' and relatives' identities in order to open dozens of bank and credit card accounts in a \$1.13 million fraud scheme.

There are also a growing number of situations where identity theft has caused a far broader range of problems for its victims. For example, medical identity theft is becoming a significant concern, with risks of fraudulent charges, falsified medical history and loss of insurance coverage resulting. There are documented problems involving criminals, who take on another person's identity and leave the victim exposed to wrongful criminal prosecution. Money may be removed from financial accounts. Debt collectors may be sent after an identity theft victim, based on false charges from the criminal perpetrator. These risks – extending far beyond mere “credit” problems – create enormous risks and practical problems for identity theft victims.

II. THE LEGAL ENVIRONMENT FOR IDENTITY THEFT

In connection with these breaches, and literally hundreds of other highly publicized incidents, two major legal developments have made security breaches and identity theft relevant to every corporation: the legal requirement for reasonable security practices and state laws across the country requiring notification to individuals in the event of a security breach.

A. The need for reasonable security practices

1. The BJ's Wholesale case requires reasonable security practices

The Federal Trade Commission's recent settlement with BJ's Wholesale Club makes an effective security program a national requirement for any company that holds personal information, regardless of industry or specific statutory or regulatory requirements. To the FTC, a failure to develop and implement an effective information security program constitutes an unfair trade practice, independent of any specific statutory or regulatory requirements.

In the BJ's Wholesale case, the FTC took enforcement action despite the fact that BJ's apparently made no representations whatsoever to its customers concerning security protections. Instead, the FTC alleged that BJ's Wholesale's information security practices, taken together, did not provide “reasonable security for sensitive customer information.” Specifically, the FTC alleged that BJ's Wholesale violated the FTC Act because it:



- Failed to encrypt consumer information when it was transmitted or stored on computers in BJ's Wholesale stores;
- Created unnecessary risks to the information by storing it for up to 30 days, in violation of bank security rules, even when it no longer needed the information;
- Stored the information in files that could be accessed using commonly known default user IDs and passwords;
- Failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and
- Failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations.

These problematic practices apparently came to light because of a large number of false or fraudulent charges posted to BJ Wholesale customer accounts, which the FTC determined to have been derived from “hacker” access to this poorly secured information (including through in-store wireless networks).

2. What is a “reasonable” security program?

As a result of these security failures, BJ Wholesale settled the FTC allegations, without admitting any wrongdoing. This settlement includes not only a requirement to implement “a comprehensive information security program that is reasonably designed to protect the security, confidentiality and integrity of personal information collected from or about consumers,” but also requires the company to have an independent third party assessment of this program, every other year for the next 20 years, subject to ongoing FTC oversight.

The reasonable security program, as mandated by the FTC, must include the following components:

- (1) The designation of an employee (or employees) to coordinate and be accountable for the information security program;
- (2) The identification of “material internal and external” risks to the security of this personal information (with this risk assessment to include employee training on the prevention, detection and response to attacks, intrusions or other system failures);



- (3) The design and implementation of reasonable safeguards to control the risks identified in this risk assessment; and
- (4) the evaluation and adjustment of the program in light of the results of testing and ongoing monitoring of the program, material changes to the company's operations or business arrangements or "any other" circumstances that may have a material impact on the effectiveness of the security program.²

The elements of this BJ's Wholesale settlement have become the minimum "standard" for a reasonable and effective security program – across all industries.

B. Security breach notification laws

Next, largely as a result of numerous security breaches, more than 35 states now have passed laws requiring notification of individuals in certain situations where a security breach presents a reasonable risk of identity theft. With the exception of a groundbreaking California statute from 2003, every law on this topic has been passed since January 2005.

These security breach laws typically apply to any industry, and protect the resident of the state in which the law was passed (so companies need to be aware of where their customers and employees reside, regardless of where the business is located). The laws vary somewhat by state. In general, most of the laws require:

- Notice to individuals when there has been the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business.
- Some states require notice only where illegal use of the personal information has occurred or is reasonably likely to occur, or creates a material risk of consumer harm.

Not all data leads to mandatory reporting requirements. For example, these laws typically apply when there has been a breach involving the following data elements:

² For information about how a small business can develop effective security practices, you may wish to review a recent publication (from the Better Business Bureau) that is designed to be a "toolkit" on security practices for small businesses. This document is available at: <http://www.bbb.org/securityandprivacy/download.asp>.



An individual's first name or first initial and last name in combination with any one of the following data elements, when either the name or the elements are not encrypted or redacted:

- I. social security number
 - ii. Drivers license number
 - iii. Account number, credit/debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account.
- Once there has been a security breach triggering these notice requirements, notice must be provided promptly (sometimes within specific statutory timeframes), with fines and potential privacy causes of action for a failure to meet the notice statutes.
 - Some states require reporting to the state attorney general as well.

These laws, taken together, have created what is essentially a national standard for the reporting of security breaches to a wide range of individuals. While states consider additional laws (in the few remaining states without a law), Congress also is expected to pass a nationwide security breach notification law either in 2006 or 2007.

C. What other laws are out there?

The obligations for reasonable security policies and notification to individuals are broad, and apply to virtually every company, regardless of industry. Beyond these requirements, there is a wide variety of other laws that create additional obligations in connection with information security and the protection of personal data. Among the most prominent laws:

1. FACTA

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) was one of Congress' first steps to deal with the growing problem of identity theft. The FACTA law, amending the Fair Credit Reporting Act, created a series of steps for business and consumer reporting agencies in connection with identity theft risks. For example, under FACTA,

- Individuals are entitled to free credit reports;
- Identity theft victims are entitled to place fraud alerts on their accounts;



- Businesses must “truncate” credit card and debit card numbers on receipts;
- A business that provides credit or products and services to someone who fraudulently uses your identity must give you copies of documents such as applications for credit or transaction records; and
- Financial institutions and creditors must adopt procedures designed to detect the warning signs of fraud and prevent identity theft from occurring.

In addition, FACTA (and the FTC “Disposal Rule”) requires any business that uses consumer reports and information derived from these reports - such as background reports obtained about job applicants - to develop and maintain appropriate procedures to dispose of this information. Several state laws contain similar provisions.

2. HIPAA

The HIPAA privacy and security rules create substantial obligations for companies in the health care industry, not only for the hospitals, doctors and health insurers covered directly by these rules, but also for the tens of thousands of “business associates” – companies providing services to companies in the health care industry. These rules cover a wide range of topics, from privacy notices to specific individual rights to obligations to mitigate any potential harm from privacy and security breaches. These rules focus on harm from the mis-use of medical and health care information – some of which can lead to identify theft, but also bringing with it a wide range of other risks, ranging from embarrassment to job loss to mistaken identity and medical errors.

The HIPAA rules also impose privacy and security obligations on virtually any employer that provides health care benefits to its employees, to ensure that the medical information is protected appropriately and is not mis-used by the employer to make employment decisions about individuals.

3. G-L-B

The Gramm-Leach-Bliley Act governs financial institutions – a broad term that encompasses not only banks and brokerage firms, but also:

- Mortgage companies (lender or broker)
- Insurance companies
- Tax preparers
- Debt collectors



- Credit counseling service and other financial advisors
- Financial or investment advisory services including tax planning, tax preparation, and instruction on individual financial management; and even
- Auto dealers that lease and/or finance automobiles.

Like the HIPAA rules, G-L-B encompasses both privacy and security obligations. These rules impose significant obligations on financial institutions to protect the security and privacy of personal financial information, with government oversight from a wide range of agencies at both the state and federal level. The G-L-B rules also impose substantial contractual obligations on “service providers” to the financial services industry.

III. WHAT KINDS OF LEGAL EXPOSURE ARE THERE?

For businesses that collect and maintain personal information, what kinds of exposure do companies face?

A. Government Enforcement

A wide range of government agencies have either formal or informal authority to pursue civil enforcement for privacy and security violations. These agencies range from specific designated agencies with authority under specific statutes (e.g., the Department of Health and Human Services’ Office of Civil Rights for the HIPAA Privacy Rule) to the most general enforcement authority – encompassing both the Federal Trade Commission (with its authority to pursue unfair and deceptive trade practices) to state attorney generals across the country, who have broad authority to investigate and pursue various practices involving privacy and security. The Federal Trade Commission – the most active and visible enforcer in security breach and identity theft cases – recently has created a new Division of Privacy and Identity Protection to focus on aggressive enforcement in identity theft cases.

Government sanctions in recent cases have involved:

- A \$15 million fine by the FTC against ChoicePoint related to its security breach;
- Numerous criminal sanctions for individuals involved in identity theft activity, often involving years in jail; and
- Numerous multi-year injunctions (from the FTC and others) against problematic behavior, including up to 20 years of independent annual third party audits of security practices.



B. Privacy and Security Litigation

In addition, while many privacy statutes do not contain private causes of action, many privacy and security statutes do authorize private suits against those who are responsible for privacy and security breaches. In addition, with increasing creativity, plaintiffs' attorneys have been pursuing litigation involving privacy breaches and responsibility for identity theft and security breaches. For example, in recent months,

- A class action lawsuit has been filed against Ohio University, based on; alleged failures to protect sensitive personal information
- B.J.'s Wholesale has faced a series of lawsuits, not only from consumers allegedly injured by the security breach, but also from a wide range of corporate entities forced to bear costs related to the identity theft;
- Veterans groups teamed up to file a class action lawsuit against the Department of Veteran's Affairs, seeking redress for millions of veterans whose personal information was breached in an incident made public by the VA.
- Wells Fargo settled a class action for \$9.6 million, relating to wrongly disclosed private consumer information to third parties.

We also have seen substantial class actions (often multiples cases) filed against ChoicePoint, Card Systems Solutions, and others who have been involved in security breaches, with more to come.

IV. WHAT CAN COMPANIES BE DOING?

A. Reasonable security steps

The first step in protecting your company against these risks is to develop and implement an appropriate security policy. The FTC guidelines in the BJ's Wholesale case and the Better Business Bureau guide are excellent places to start. These security programs do not have to be perfect – the standard is one of reasonableness. An effective and reasonable program will go a long way towards reducing the risk of government enforcement action – even in the event that the security policy doesn't work in a particular situation, and there is a security breach.

B. Educate your work force

Some security steps are implemented across a company and are virtually invisible to the average employee – for example, installing an effective firewall to keep hackers out of your computer system. Other steps are very individual, and require training of your



employees to engage in concrete steps that can reduce the risks of security breaches and identity theft. These steps not only can reduce actual risks – but can also go a long way towards ensuring that your overall security practices are both reasonable and are being followed. **Remember**, a “reasonable” security program on paper isn’t really “reasonable” if your employees don’t know about it and don’t follow it.

A few hints on employee training. Tell employees to:

- Properly erase data from obsolete office equipment (hard drives, floppies);
- Shred documents that have sensitive information when no longer needed;
- Remove sensitive information from e-mails wherever possible before you reply or forward over the Internet;
- Don’t share your identification or access passwords;
- Don’t use obvious passwords or write down passwords in a readily accessible place; and
- Don’t store sensitive information on your laptop unless necessary – and remove it when the task is finished.

C. **Be prepared – Create a mitigation plan**

Because of the focus on “appropriate” risk levels and “reasonable” security measures, there is the obvious possibility that security breaches will occur no matter what precautions are taken. Accordingly, it is critical that companies have an effective mitigation plan in the event of a security breach. This plan should involve not only how to correct the particular situation - but also an assessment of how to revise existing policies to prevent recurrences. This mitigation plan is very important, because this plan kicks in when the rubber meets the road - you have had a security or privacy breach and need to "fix it" immediately in the eyes of your customers, regulators and management.

This plan needs to have two critical components. First, you need to identify and fix the problem. This should involve a series of questions designed to deal with four main problems: (1) how do I stop or control the breach? (2) how do I determine what happened and what information was subject to the potential for improper use or disclosure; (3) how do I repair any injury from the breach (including recovering lost data for internal purposes) and (4) what do I need to do to make sure this doesn’t happen again? Companies in all industries need to recognize that the biggest litigation risk today involving privacy and security relates to credible threats of identity theft and costs related to identity theft prevention. An effective mitigation plan often will reduce or eliminate these realistic threats.



Second, companies need to have a quick and effective approach to the question of whether and through what means to notify individuals of a security breach. This involves several questions – do I have to notify anyone? If so, who must I notify and through what means? If I don't "have to" notify, should I notify anyway? Is there anyone else I need to notify (clients, regulators, etc)?

Because the state laws are complicated and not fully consistent, it is important to have an understanding of the legal requirements in developing a policy – and it may be too late to do this once a breach happens. In addition, keep in mind that the congressional debate about breach notification is ongoing, with passage of a federal standard (that may or may not preempt state law) likely in 2006 or 2007. Because of the tensions and pressures created when a security breach takes place, these reporting decisions typically are made under intense business pressure and (perhaps) public scrutiny. Reporting is neither required nor appropriate with every security breach (and Congress and the FTC both are concerned about the risk of "overnotification," with the concern that consumers will become numbed by constant security breach notifications), but it should be considered by senior management in any circumstance where there is any realistic likelihood of customer impact.

D. Keep re-assessing your security program

Security programs cannot be stagnant – they must be re-evaluated almost constantly. This involves not only technological developments, but also developments in your business and in the external environment. Make sure that your risk management and security team pay attention to news developments and other reports concerning security breaches – if there are lots of reports about stolen laptops; make sure that you have taken steps to reduce your risks from a stolen laptop (e.g., encryption of laptops, increased password strength, reduction of information contained on laptops, etc.). This "update" component also is critical to ensuring that your security program stays reasonable.

E. Re-evaluate your data practices

Companies should pay close attention to how they collect, use, store and disclose personal information. Reducing the information that you collect and distribute can have a substantial impact on your exposure to identity theft risks.

For example, many companies routinely collect and distribute Social Security numbers, for employees and customers. In many cases, this is simply the result of longstanding practices. However, it is now clear that the Social Security number is the single most sensitive piece of personal data – and is the gateway too many identify theft schemes. Companies should rigorously analyze every situation in which it collects SSNs – if you don't absolutely need it, don't get it. And, don't share it with others – even trusted vendors – unless they absolutely need it also.



F. Pay attention to your vendors

Aside from worrying about your own employees, companies also need to evaluate how they will select, contract with and monitor the activities of their vendors. Vendors consistently receive large quantities of data about individuals – and many of the largest data breaches have involved vendors rather than principles. So, companies must be cognizant of vendor practices, must take steps to reduce as much as reasonably possible the sensitive data provided to vendors, and must develop a means – through both strong contracts and reasonable oversight practices – of keeping an eye on what vendors are doing with your data.

G. Protections for your employees and customers

As part of your mitigation plan, you should be considering what kinds of steps you can take to protect your employees and customers, if they face identity theft risks. Some of these risks involve credit; other risks affect individuals more broadly, and can extend to wrongful arrests, medical mistakes and other potential problems. These problems may take both time and legal assistance, for individuals to recover their good name and restore all the ramifications of an "unstolen" identity.

H. Credit monitoring isn't enough

Companies also need to recognize that the latest identity theft "solution of the day" – credit monitoring – likely will be insufficient in many circumstances. First, credit monitoring – which has become commonplace in many security breach circumstances – only helps when an individual already has a problem; it may help to fix the problem, but it doesn't prevent it from occurring.

Moreover, credit monitoring does not assist with many other potential results from identity theft – against risk such as wrongful prosecution, medical errors, aggressive debt collection efforts or mis-use of a Social Security Number. So, companies and individuals evaluating identity theft risks need to think beyond credit risks – to the broader range of potential identity theft problems.

V. CONCLUSION

In the past year, the law of identity theft has changed dramatically – and we can expect these changes to continue and expand. Security risks will remain – because volumes of personal data that are collected, used and disclosed on a daily basis will remain substantial. Companies – in all industries – need to be aware of the increasing legal obligations arising from security practices and identity theft risks, and must be exploring all reasonable means of meeting these obligations and reducing risks from these areas as much as possible.