
SHERRARD
GERMAN & KELLY, P.C.
ATTORNEYS AT LAW

28th Floor, Two PNC Plaza, Pittsburgh, PA 15222
Phone: 412-355-0200 • Fax: 412-261-6221 • www.sgkpc.com

REPORT FROM COUNSEL

SUMMER 2005 ISSUE

THE WAR ON IDENTITY THEFT

By Edward G. Rice, Esquire

Hardly a day goes by without a story appearing in the press or over the airwaves about another compromise of a large consumer information database or some other horror story concerning consumer information security. Few topics have garnered as much attention, and rightfully so. Indeed, the technological advancements of the electronic age have also ushered in a seedy underbelly of data theft and black-market profiteering in such information (thieves can fetch up to \$100 for each element of stolen data). In the past year alone, millions of consumers have had their data stolen in a number of high-profile cases, involving "blue-chip" companies not known for lapses of the type occurring:

- * Lexis-Nexis--310,000 stolen social security and driver's license numbers;
- * Choice Point--at least 145,000 stolen name, address and social security numbers (some estimate this figure could be 10 times greater);
- * Bank of America--"lost" back-up computer tapes containing the credit card information of 1.2 million government employees, most from D.O.D., and including many U.S. Senators;

* Time-Warner--"lost" a container of computer tapes containing the personal information of over 600,000 current and former employees;

* DSW Shoe Warehouse--1.4 million stolen credit and debit card numbers and driver's license information.

The consequence of this increase in data theft has been a more pro-active regulatory response. Most of this response, on a federal level, has been directed towards financial institutions and related business entities. On one level, this makes sense in that the typical use to which a data thief puts stolen consumer data is in the financial world, most notably involving credit theft. The thief, using stolen identities, obtains goods on credit. The victim, of course, suffers great harm to his or her credit rating, affecting his or her ability to obtain credit for legitimate purchases of goods and services and housing. The ripple effect of this identity theft is staggering in monetary costs on the economy, as well as the emotional cost on the victims who historically have had a very difficult time repairing damaged credit reputations. This Article will explore recent developments employed by the federal government in its "war" on identity theft.

First Response

The first significant national response to the growing problem of identity theft occurred in 1999, with the passage of the federal Gramm-Leach-Bliley Act ("GLB"). While the GLB is better known in banking circles for substantially realigning the financial services industry, Title V of the Act dealt with consumer privacy and information security matters. Section 501 of the Act specifically provided that each "financial institution" has an affirmative and continuing obligation to both respect the privacy of its customers *and* "to protect the security and confidentiality of those customers' non-public personal information."

Under the Act, the definition of "financial institution" is very broad, and encompasses not only banks and thrifts, as one would expect, but also many other types of businesses such as insurance brokerage services, mutual funds, investment advisory services, real estate settlement services, and any other business that conducts activities deemed "financial in nature" (e.g., General Motors Acceptance Corporation and the credit card operations of department stores such as Macy's are additional types of non-bank entities that are subject to GLB). In addition, the term "non-public personal information" is defined very broadly under the Act to include virtually any information about a consumer that a financial institution has in its files, obtained in connection with providing a financial product or service to the consumer. This is quite a bit of information to protect.

Section 501(b) of GLB provides that the various agencies charged with regulating financial institutions are required to establish appropriate standards relating to the administrative, technical and physical safeguards of customer records and information. As stated in the Act, these safeguards are to: (i) insure the security and confidentiality of customer records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) protect against unauthorized access to

or use of such records or information that would result in substantial harm or inconvenience to any customer.

The various agencies charged with oversight and enforcement of the GLB did issue the required standards. Leading the pack were the several banking agencies, who on February 1, 2001, published the Interagency Guidelines Establishing Standards for Safeguarding Customer Information ("Interagency Guidelines"). The Interagency Guidelines directed financial institutions to establish information security programs to: (i) identify and assess the risks that may threaten customer information; (ii) develop a written plan containing policies and procedures to manage and control such risks; (iii) implement and test the plan; and (iv) adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information and internal or external threats to information security. Recognizing that there is no "one size fits all" application to the standards, the Interagency Guidelines permitted each financial institution to adopt a security program appropriate to its size and complexity and the nature and scope of its operations.

While this first response to the growing threat of breaches in information security was a positive and necessary first step, it became abundantly clear that having information security programs alone would not stop the inevitable breach of security systems. The best systems in the world will always be subject to the new and evolving breaching techniques of data thieves. As is clear from a perusal of the Interagency Guidelines, what they did *not* cover was just as critical, if not more so, than what the standards *did* cover. Notably, the Interagency Guidelines did not address what should happen whenever there is a breach in the financial institution's information security program.

Evolution of the Legislative Response

Since the initial federal response to information security breaches was not complete, many states began exploring ways to plug the real and perceived gaps. To be sure, this is a topic that has little downside politically. Consequently, activity in this area has rapidly increased. Of course, California led the pack, enacting the first consumer notification law two years ago. Under this law, an entity conducting business in California, and that owns or licenses computerized data that includes certain personal information, is required to notify individuals of any breach of the security system where "unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Six additional states have since adopted customer notification laws - Arkansas, Georgia, Indiana, Montana, North Dakota and Washington. Further, at least 25 additional states have similar legislation pending or have recently considered such legislation.

The upshot of this is that a patch-work of state legislation may create conflicting and irreconcilable differences in the information security standards that financial institutions must follow. This could further result in an overall *decrease* in the compliance rate. The question then becomes--does a national standard make sense?

This question has been partially answered, at least with respect to bank entities that are subject to the Interagency Guidelines (i.e., financial institutions regulated by the OCC,

OTS, FRB and FDIC). On March 29, 2005, the banking agencies published a supplement to the Interagency Guidelines--dealing primarily with response programs consequent to information security breaches ("Interagency Response Guidelines"). These new Guidelines keep in place the standards of the existing Interagency Guidelines, but they add to them a response component. Under the supplemental rules, an institution is required to add a response program that contains procedures for the following:

- (a) assess the nature and scope of a security breach;
- (b) notify the institution's primary federal regulator as soon as possible after the breach;
- (c) file the appropriate reports with law enforcement authorities;
- (d) take appropriate steps to contain and control a breach in security (e.g., by monitoring, freezing or even closing affected accounts, and preserving records and other evidence); and
- (e) notifying customers when warranted.

Of course, the significant element listed above is the customer notification element. The Interagency Response Guidelines provide somewhat of a balancing test in determining when notification to the customer is warranted. The agencies do not desire notification in every instance, which could result in unnecessary customer panic or, alternatively, the "cry-wolf" syndrome of customers simply ignoring the notifications.

Under the new standard, upon becoming aware of an information security breach of "sensitive customer information" (as defined in the Guidelines), the financial institution should conduct a reasonable investigation to promptly determine the likelihood that the stolen information will be misused. If the institution determines that the sensitive customer information has been misused or that misuse is "reasonably possible," then the notification should be made. The customer notice may be delayed, however, if an appropriate law enforcement agency determines that notice will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the new Guidelines further provide that the financial institution shall notify its customers as soon as notification will no longer interfere with the investigation.

This, of course, begs the very serious question of what should the financial institution do if on the one hand, accounts need to be frozen or closed, and on the other hand, a law enforcement agency wants the financial institution to remain silent about a breach pending further investigation. For instance, how can an institution freeze or close an account without telling the customer? Not only do the new Guidelines leave this critical question unanswered, but the Guidelines also purposefully side-step the notion of "safe-harbor"--in other words, compliance with the Interagency Response Guidelines may not, in and of itself, be used as a shield against liability for the compliance actions taken. Clearly, these issues leave financial institutions in a difficult position.

Again it should be emphasized that the Interagency Response Guidelines apply to banks and thrifts, and not directly to other types of entities. As such, one should expect a great deal of continued activity on both the state and federal legislative levels.

Victim's Tactical Response

While the Interagency Guidelines, and the supplemental Interagency Response Guidelines are designed to provide the framework in which financial institutions protect their data against theft and respond in the most effective manner when a theft occurs, these Guidelines do not address the things a consumer can or should do when he or she has become a victim of identity theft. These victims typically find that their identity has been used to make fraudulent purchases on credit. It may be very difficult for the victim of identity theft to unwind the fraudulent transaction and make the necessary repairs to his or her credit rating. The federal government has also addressed this important component by the recent enactment of the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"). This new law substantially amends the federal Fair Credit Reporting Act.

FACTA does many things in its attempt to modernize and strengthen the credit reporting function that has become a critical component in the operation of the consumer credit system in the U.S. economy. A full summary of FACTA is beyond the scope of this article. Nevertheless, from an identity theft "battle-ground" perspective, FACTA includes a number of sections designed to help both financial institutions and consumers in combating identity theft. Notably, FACTA provides for:

- (i) Fraud alerts, which can be placed by the consumer on his or her file to alert creditors of a good faith suspicion that the consumer has become a victim of identity theft;
- (ii) "Red Flag" guidelines--the Act requires federal banking agencies to promulgate rules for identifying possible instances of identity theft, to be used and monitored by financial institutions;
- (iii) Card issuers (credit and debit cards) have new standards for initiating an investigation when a consumer's address changes;
- (iv) Consumer reporting agencies are now required to block the reporting of information that a consumer identifies as having resulted from an identity theft;
- (v) Banks and other financial institutions are required to establish rigorous procedures to verify the identity of a consumer, who has a fraud alert placed on his or her credit report, whenever that consumer applies for a new credit plan or an increase in credit;
- (vi) financial institutions are now required to provide to the victim (or a law enforcement agency) the business records used in a fraudulent transaction in order to allow the victim to investigate and pursue the identity thief; and

(vii) Debt collectors have new limitations placed on them in connection with collection activities of debts identified as having been originated through fraudulent means.

Conclusion

It is hard to say at this early stage whether or not these new federal laws will be effective in the government's war on identity theft. Clearly, some legislative response is warranted, and considering the national (and indeed global) scope of the economy, a federal response would appear to be a wiser approach to the problem than a quilt-patch of state laws that may be inconsistent and could ultimately inhibit the free flow of information necessary to keep the national economy running smoothly and efficiently.

Nevertheless, it should be kept in mind that identity theft is ultimately a technology problem. While legislative action on some level may be necessary to act as a catalyst in inciting industry to develop technological fixes to the problem, attempts by government, state or federal, to micromanage the problem and over-legislate may only serve to hinder more productive efforts to combat identity theft. We are not there yet, but studied restraint should be exercised.

FIRM ANNOUNCEMENTS

Joseph L. Robinson, a shareholder and director of Sherrard, German & Kelly, P.C., delivered a presentation at the Annual Meeting of the Independent Oil and Gas Association of Pennsylvania on May 17, 2005. His topic was "Negotiating a Purchase and Sale Agreement for the Acquisition of Oil and Gas Producing Properties." He discussed (1) the properties to be acquired, including leases, wells, pipelines, rights-of-way, well equipment, compressors and dehydration units and drilling permits; (2) negotiation of the representations and warranties to be included by the Seller; and (3) termination provisions of the Asset Purchase Agreement. Mr. Robinson graduated from Duquesne University School of Law in 1973 and has concentrated his legal practice in oil, gas and mineral matters throughout the Appalachian Basin. He has delivered presentations on oil, gas and coalbed methane extraction to various seminars held in Pennsylvania, West Virginia and Kentucky.

The firm is pleased to announce that **Ms. Suzanne L. DeWalt** has joined the firm as a member of the Litigation Services Group. She concentrates her practice in the areas of employment law and civil litigation.

Ms. DeWalt advises businesses and their owners and managers in a wide range of human relations and employment issues. She devotes a significant amount of her practice to defending businesses in discrimination and wrongful discharge actions, as well as representing clients in non-competition and non-solicitation matters. She assists clients in negotiating and drafting their employment and severance contracts and in creating employee handbooks, personnel policies, and other employment documents. Ms. DeWalt

also provides general advice on terminations, reductions in force, and compliance with equal employment, anti-discrimination, wage and hour and other laws and regulations affecting the work place.

Ms. DeWalt is an experienced trial attorney with a diverse civil litigation practice. In addition to employment litigation, she also represents clients in commercial litigation and construction law. She has tried numerous jury, non-jury and arbitration cases and has prepared and argued many cases on appeal. Ms. DeWalt has tried cases in federal and state courts, and before the American Arbitration Association. Ms. DeWalt received her law degree in 1984 from the University of Virginia. She earned a bachelor of arts degree summa cum laude and Phi Beta Kappa from the University of the South, Sewanee.

This firm is pleased to announce that **Ms. Jennifer R. Andrade** has joined the firm as an associate in the firm's Litigation Services Group. She currently focuses on commercial litigation matters. Prior to joining the firm, she served as a law clerk to the Honorable Ila Jeanne Sensenich of the United States District Court for the Western District of Pennsylvania for two years. Prior to and while earning her Juris Doctor, Ms. Andrade served as Vice President of Operations of a Pittsburgh-based transportation engineering firm. Ms. Andrade received her law degree in 2003 from the University of Pittsburgh School of Law, and a bachelor of arts degree cum laude in 1995 from Boston University.

Sixth Year for HEARTH Sponsorship

SGK was a Gold Sponsor for HEARTH and its 10th Annual Golf Outing on June 20th. HEARTH is a non-profit entity that runs Benedictine Place in the North Hills, a transitional housing program for homeless women and children providing a continuum of care that empowers participants to become independent and economically self-sufficient. The focus of Benedictine Place is to provide a safe place for families to live along with necessary support to enable mothers to complete educational or training programs, all while parenting their children and maintaining jobs. In the past few years, HEARTH has helped over 120 families and more than 225 children in their efforts to transition from homelessness to self-sufficiency.

SGK attorney **Eric Springer** has been on the HEARTH board for the past 6 years and has served in numerous positions including serving on its Finance, Executive, Community Housing Development, Board Development and Golf Committees. He served as the Chairman of the Golf Committee for the Event. Sponsorship for the Event doubled from last year and funds raised substantially increased thanks, in part, to help from SGK friends and contacts.

Financial Industries Network Event Sponsorship

SGK was a Gold Sponsor of the Financial Industries Network Event on June 16th. The Financial Industries Network is a non-profit organization of executives and other senior-level managers from a variety of regional companies and banking and finance-related industries, as well as accountants, investment advisors, securities brokers, tax consultants,

business consultants, attorneys and other professionals. The group meets quarterly to network and discuss issues involving corporate and personal finance. The firm has been involved with the Financial Industries Network for many years and SGK attorney Eric Springer has served as a Board Member for the past 6 years.