

A DIFFERENT TYPE OF IDENTITY CRISIS:

What Businesses Need to Know

By Peter Crane Anderson, Esq.
and William R. Terpening, Esq.

QUESTION #1: What recent social misfortune impacts at least 10 million people each year, causing each victim to suffer an average loss of nearly \$100,000? **ANSWER:** Identify Theft.

QUESTION #2: How often is identity stolen? **ANSWER:** Every 2.3 seconds, 24 hours a day, 7 days a week.

QUESTION #3: What has Congress done to address this problem? **ANSWER:** Enacting the Fair and Accurate Credit Transactions Act (FACTA), whose rules went into effect on June 1, 2005.

INTRODUCTION

Identity theft has been defined as the misuse of personal or business identifiers by an imposter for their advantage, which may be financial, non-financial, or both. Such personal identifiers ►



might include a name, date of birth, Social Security Number, and account numbers. Business identifiers include business names, federal tax identification numbers, or business account information.

Due to the recent increase in media coverage surrounding identity theft, most people are generally aware and concerned about this fast-growing crime. In turn, these trends have spawned new laws regarding both prevention and punishment. Unfortunately, most businesses remain in the dark about the potential liabilities surrounding the ever-growing corporate accumulation of personal data. As with any new law with potential hidden and harsh consequences, companies should become more aware and adjust their conduct accordingly.

A CHANGED LEGAL LANDSCAPE: “NOW, IT’S A FACTA LIFE”

The Fair and Accurate Credit Transactions Act of 2003 (FACTA) had widespread impact upon many companies in the United States. Among its various provisions, the law requires that, effective June 1, 2005, businesses must take “reasonable measures” to destroy information derived from consumer credit reports before discarding them. This article focuses on FACTA, but you should know additional federal, state, and industry-specific rules and regulations demand that businesses contend with numerous and diversely-faceted guidelines—some mandatory and some advisory—in the identity theft area.

The FACTA disposal rules apply to any business that directly or indirectly has or uses “consumer information” regardless of the size or number of employees. Given the law’s broad scope, every company needs to keep its records safe and dispose of them properly. The FTC has stated that “reasonable measures are very likely to require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training.”

Under FACTA, the liability for a business arising from identity theft includes state and federal fines, and practically unlimited civil damages. The major risks to businesses include victimization of owners, managers, employees, customers, clients and vendors; fraudulent use of the business identity or data; legal, financial, and public-relations consequences of privacy, security, and regulatory breaches. Laws aside, the public embarrassment and loss of goodwill arising from a major identity theft breach can cast a negative shadow on the company for years; companies cannot afford to ignore these risks and do nothing.

Companies need to ask themselves questions; take a “FACTA Quiz” if you will. Is your business subject to the FACTA disposal rule? Has your company developed appropriate current policies or procedures regarding record storage or disposal? Do your business policies or practices comply with

FACTA? If you hire a third-party to handle disposal of documents containing personal or business information, does that company comply with FACTA? Questions like this will keep your business out of risk and you ahead of the game.

SAMPLE CASE STUDIES

BJ’S WHOLESALE CLUB

In June 2005, the Federal Trade Commission (FTC) issued its first ruling against BJ’s Wholesale Club under FACTA for failing to provide “reasonable security” for certain sensitive customer information. More specifically, BJ’s allegedly failed to encrypt credit card numbers stored in their stores. The resulting breach caused \$13 million in charges placed upon the stolen credit card numbers.

CHOICEPOINT

The eye-opening situation with Atlanta-based consumer data services company ChoicePoint in early 2005 underscores the long-term reputational consequences for companies that do not impose sufficient identity theft protection. Criminals accessed ChoicePoint’s consumer records by opening accounts to purchase, in the guise of legitimate companies, confidential consumer information. Because of limited safeguards, ChoicePoint reportedly had difficulty even ascertaining whether consumer records had even been viewed, which was a source of strongly negative public reaction. ChoicePoint wisely elected to work with the FBI and other authorities to track down the wrongdoers, and to promptly notify even potential victims. However, by the end of the day, at least 750 identity theft case arose from the scandal, and confidential information of at least 145,000 people was compromised. ChoicePoint had outlayed at least \$11.4 million because of the episode, including \$2 million to notify victims and \$9.4 million in legal





and professional fees. Moreover, the FTC fined it \$15 million, and ChoicePoint is said to have spent millions “closing the barn door after the horses escaped” to improve safeguards after the incident. The events continue to affect share value and reputationally overshadow the company.

HOW TO MINIMIZE RISKS

- 1) Minimize the personal data your company holds. Although holding personal data is often necessary, ask whether it needs to be stored indefinitely or for more than a brief interval. Time is an important factor here.
- 2) Keeping all personal data secure is important, but not always enough. This is an area where different regulations have different requirements, and you will want to have a professional pull these requirements together (and refresh the requirements periodically to reflect revisions to the law) to be confident that you are following the current requirements. For example, if you send a Social Security Number through e-mail, it often must be encrypted. If, like the authors, you could be more technically savvy, you would not intuitively guess this encryption requirement exists. Therefore, you'd need help. This is an example of a situation where one person's definition of securing data may differ from another person's—so the regulations must be carefully and thoughtfully followed.
- 3) Make certain all employees prioritize security measures. Similarly, carefully screen and monitor your employees and third-party partners: identity fraud problems for companies often involve “moles”.
- 4) Check out your vendors, clients, and other third-party relations. Again, as in the ChoicePoint example, we all are more easily fooled by resourceful fraudsters than we would prefer to think. If your business involves selling confidential information, do you really know who you are selling to? If you outsource to partners for analysis of your clients' information, have you done your homework and investigated your partner?

5) Frequently update your policies and procedures. Remember to be proactive and impose better safeguards before the law requires you to. Again, this is an area where the risks to your reputation are as serious as your legal liability, and it is better not to be in the embarrassing position of telling your clients and authorities that you could have taken extra measures, but did not. In the same fashion, if your security is breached, or you make a mistake and fail to comply with a particular requirement, the authorities and the marketplace will be much more understanding if you can demonstrate the strenuous steps you took to develop a plan that is generally comprehensive.

6) Anticipate unforeseen consequences. Fraudsters may steal your client's information for a variety of reasons. The Securities and Exchange Commission, for instance, has started prosecuting individuals who have requisitioned investor accounts at e-Trade and several other major brokers to open fake accounts to use in “pump and dump” schemes. This exposes the companies that fraudsters have targeted to losses stemming not solely from identity theft, but from improper trading.

7) Be prepared to respond in case of a breach. Your worst-case scenario action plan needs to be written down now. When a breach occurs, your chances of mitigating your legal exposure and your reputation will be greatly impacted by how rapidly you can go to the authorities and individuals whose information was compromised with an amelioration strategy.

A FINAL NOTE

Unfortunately, the identity theft hurricane rages on with no signs for fair weather ahead. This is just another recent example of the many burgeoning compliance and regulatory areas that are coming to constitute an expanding waterfront. Until the clouds part, we continue struggling to find the right answers to our clients' early questions, while also providing adequate shelter or a safe harbor. Our goal remains to help clients sail through these storms, and to help teach lessons without harsh consequences, like a hefty civil judgment. Although every business and executive needs an experienced guide in reacting to such rough seas, the preferred course of action is still to test the sea-worthiness of the ship with proactive measures.

Remember that FACTA (and this brief overview) is not your only authority in the identity theft arena. A number of laws beyond FACTA guide corporate requirements for guarding against identity theft. For example, North Carolina professionals who counsel companies should know about the recent North Carolina Identity Theft Protection Act of 2005. Among other requirements, this law limits the type and manner of information that can be transmitted over the Internet or recorded on paper. As well, it requires prompt notification of individuals by businesses when it is reasonably likely that identifying information was compromised. **IR**