

Identity Theft and Business Solutions

by Tom Rivers

Introduction to Identity Theft

“‘Credit identity theft’ or ‘identity theft’ means the theft of a consumer’s personal identification and credit information which the thief uses to gain access to the victim’s credit and bank accounts and take over the victim’s credit identity.”

-California Department of Consumer Affairs¹

In 1998, identity theft was criminalized in the federal law through the “Identity Theft and Assumption Deterrence Act.” The act was necessary because previous legislation dealing with fraud only addressed the creation, use or transfer of identification documents, and not the theft or criminal use of the underlying personal information therein.

- The act made it a federal crime when anyone “knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under the applicable State or local law.”²

- The act applies to “any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual,” such as an individual’s name, Social Security number, date of birth, driver’s license, unique biometric data (like

fingerprints or iris images), and unique electronic identification number and telecommunication identifying information or access device (like an access code or PIN).³

- Violations of the act may be investigated by any federal investigative agency, including, but not limited to: the United States Secret Service, the Federal Bureau of Investigation, the United States Postal Inspection Service, and the Office of the Treasury Inspector General for Tax Administration. Violations are prosecuted by the Department of Justice.

- In most cases, the crime of identity theft carries a maximum term of 15 years imprisonment, a fine, and criminal forfeiture of any personal property used or intended to be used to commit the offense.⁴

- Violations of other federal, state, and local statutes must underlie the schemes to commit identity theft. Some of the federal offenses are felonies that carry substantial penalties—sometimes as high as 30 years' imprisonment, fines, and criminal forfeiture.⁵

How a Thief Obtains Victims' Information

An identity thief can obtain a victim's personal information through a variety of methods. Some of these methods are directly related to business and industry practices that put consumers at risk. Businesses should be aware of how their actions may expose themselves and consumers to the dangers of identity theft.

- *Mail theft* can be a means for an identity thief to obtain personal information for

fraudulent purposes. Pre-approved credit card offers can be stolen from a consumer's mail box, and the enclosed information can then be used to obtain credit in the consumer's name.⁶

- The practice of *dumpster diving* also provides access for a would-be thief to a consumer's personal information. If a business discards papers containing its customers' personal identification information without shredding the documents, a thief may retrieve this information from the business's dumpster (trash container).⁷

- Employees of businesses may be responsible for identity theft through more direct means. *Insider access* to information allows a dishonest employee to sell consumers' personal information or to use it for fraudulent purposes.⁸

- One specific type of business that may be responsible for identity theft is the *computerized information service*. This business sorts, packages, and sells personal information in electronic form for marketing purposes. However, such businesses may not safeguard the information adequately, or may sell it to purchasers that the business has not appropriately screened.⁹

- Businesses may also be deceived by *pretext calling*, when an information broker or identity thief calls pretending to be a customer, and may even use bits of the customer's personal information such as the Social Security Number to maintain the deception. The

information broker or thief convinces the employee to provide additional information over the phone, which can be used for fraudulent purposes.¹⁰

How the Thief Uses the Victim's Information

Once in the possession of the perpetrator, the identity thief may use stolen personal information in a variety of ways to commit fraud.

- The thief may call a credit card issuer, pretend to be the account holder, and ask to change the mailing address on the credit card account. The thief can then run up charges on the account. Because the bills are being sent to a new address, it may take some time before the problem is discovered.¹¹

- Along the same lines, the identity thief may use a victim's personal information, such as the name, date of birth, and Social Security Number to open a new credit card account. When the thief uses the credit card and does not pay the bills, the delinquent account is reported on the victim's credit report.¹²

- An identity thief may use a victim's information to commit fraud in many other ways, all under the victim's name:
 - Establish phone or wireless service
 - Open a bank account and write bad checks on that account
 - File for bankruptcy

- Counterfeit checks or debit cards and drain the victim's bank account
- Buy cars and other property by entering into loan agreements¹³

What Identity Theft Means for Businesses

Identity theft and related forms of fraud involve high costs—not only for consumers, but also for businesses:

- According to the Secret Service, incidents of identity theft and their actual costs/losses to individuals and financial institutions totaled:

- 8,806 crimes at a cost of \$442 million in 1995

- 8,686 crimes at a cost of \$450 million in 1996

- 9,455 crimes at a cost of \$745 million in 1997

- The Postal Inspection Service reports many incidents in which identity theft results in high costs for financial institutions. In 1997, the Postal Inspection Service investigated:

- a sophisticated crime ring in New York that used fraudulently obtained credit cards. Losses to the card-issuing banks were over \$1.8 million.

- a credit-card fraud ring in Florida comprised of 32 people, which was responsible for losses of at least \$1.5 million

- VISA USA, Inc. reported that in 1997, fraud losses to member banks totaled \$490

million.

- MasterCard International, Inc. reported that in 1997, fraud losses to member banks totaled \$407 million. Of this fraud, about 96% involved identity theft.
- The American Bankers Association reported that credit-card fraud losses for 10 large banks averaged about \$20 million per bank in 1996.¹⁴

What Businesses Can Do to Prevent Identity Theft

Realistically, consumers cannot totally protect themselves from identity theft. The key to prevention is for businesses to establish responsible information-handling practices and for the credit industry to adopt stricter application verification procedures, among other strategies.

There are different areas in which businesses can take steps to ensure responsible information-handling practices:

- Organizations and companies should have policies that outline their privacy practices and expectations for handling the personal information of clients, members, users, etc. These privacy policies should be communicated regularly—in employee training sessions, employee handbooks, on posters and signs, and in brochures available to their customer base.¹⁵
- It is important to maintain strict data and network security where personally identifiable

information is concerned.

- Businesses should have staff specifically assigned to data security.

- Staff members should participate in regular training programs regarding data and network security to keep up with new technical and legal issues.

- Physical access to computer operations and files containing personally identifiable information should be restricted.

- Sensitive files should be segregated into secure areas or computer systems and available only to qualified persons.

- Businesses should have audit procedures and strict penalties in place to prevent telephone fraud and theft of equipment and information.

- Employees should follow strict virus protection and password procedures, changing their passwords often. Encryption should be used to protect extremely sensitive information.¹⁶

- There are other basic security practices that can help businesses prevent identity theft.

- When providing copies of information to others, employees should make sure that nonessential information is removed and that personally identifiable information that has no relevance to the transaction is either removed or masked.

- Employees should be trained never to leave computer terminals unattended when personally identifiable information is on the screen, and password-activated screen-savers should be used.¹⁷

- Businesses should use the proper practices when retaining or disposing records.
 - Companies should have a records retention/disposal schedule for personally identifiable information, whether stored on paper or electronically.
 - When disposing of computers, diskettes, hard drives, or other electronic sources of information, all data should be erased and/or the hardware should be destroyed.
 - When disposing of paper documents, the papers should be placed in secure padlocked containers or shredded.
 - A business should also check its recycling company's disposal/destruction methods.¹⁸

- The use of **Social Security Numbers** by a business may put customers and employees at risk from identity theft if proper practices are not observed.
 - It is preferable that Social Security Numbers not be used for record keeping purposes by businesses.
 - If a business does use the Social Security Number as a record keeping number, it should offer its clients and/or employees the option of using an alternative number.
 - The business should have a strict policy prohibiting the display of Social Security Numbers on any documents that are widely seen by others (e.g. time cards, parking permits, employee rosters, mailing labels, etc.).
 - If the business requires an access code for certain transactions (ATM cards, security system codes, building access cards, passwords), it should prohibit the

use of Social Security Numbers or any portion thereof.¹⁹

• If a business maintains information on customers, and if it sells, rents, or exchanges its lists with other entities, it should take several steps to ensure fair information practices.

-The business should offer its customers an “opt-out” program, in which the customer’s name is removed; this policy should be effectively communicated to the customer.

-The business should subscribe to the Direct Marketing Association’s name removal services (the Mail Preference Service and/or the Telephone Preference Service). These services feature names that should be removed from the business’s list prior to its sale, rental, or exchange.

-Be aware of current laws and regulations regarding fair information practices.

-The business should have adequate security to prevent remote access to lists via computer.

-The business should also ensure that list recipients employ sufficient safeguards; security measures should be in place during the transfer of the list, and the secure and timely return or destruction of lists used by other entities should be ensured.

-The business may use a monitoring system to track list usage (such as the use of decoy names).

-The business should only collect those consumer data that are pertinent and necessary for the purpose at hand.

-The need for customer data should be reviewed/ revised by the business on a

regular basis.

-Businesses should disclose up-front the intended uses of the data that are collected, and data subjects should be allowed to inspect and correct the data held about them.²⁰

- Businesses should also develop privacy policies to guide employee relations.

-A business should have policies for handling the personal information of its employees; such policy statements typically concern hiring procedures, personnel records, medical records, discipline procedures, electronic mail usage and electronic monitoring.

-The business should have a policy regarding the privacy expectations of its employees concerning their e-mail and voice mail, and a policy for any third party users.

-These policies should be effectively communicated to all employees and third-party users.

-Employers may use a variety of employee monitoring practices: telephone systems that allow supervisors to listen to telephone calls, computer keystroke monitoring systems that can determine work productivity, video monitoring systems, and location detectors. If such measures are used, the business should have a policy that states the types of monitoring being conducted and the uses made of monitoring data. The policy should include procedures to safeguard sensitive personal information encountered in the process of monitoring.²¹

What Credit Issuers Can Do to Prevent Identity Theft

Credit card issuers have a heightened responsibility to help prevent identity theft—about half of the cases reported to the Federal Trade Commission involve credit card fraud. Credit issuers can reduce identity theft by taking several steps to ensure consumers' security.

- Companies should conduct better identity verification, especially when an address or birth date is reported as changed or is different from what is stated on the credit report.

- Better identity verification should be used for credit cards obtained via pre-approved offers of credit. An example would be to supplement the Social Security Number with utility bills, tax records, the address, etc.

- Companies should improve identity checking procedures for “instant” credit, which is favored by identity thieves.

- The number of pre-approved offers of credit mailed to consumers should be reduced.

- Companies should use profiling systems to detect unusual activity in credit accounts, and notify consumers of possible fraud.

- Credit issuers may:
 - put photographs on credit cards

- enable customers to place passwords on credit accounts
- check if there are existing accounts in an applicant's name
- check applicant names with the master death index.²²

Businesses and Check Fraud

Check fraud is a problem that may overlap identity theft in many cases.

- Businesses should set guidelines regarding the types of checks they will accept: personal, two-party, payroll, government, or traveler's checks.
- Checks should be examined carefully. When a personal check is presented, businesses should insist on proper identification.
- Signatures on checks should also be compared with that on the ID. Businesses should be suspicious of individuals who take extreme care and much time in signing their name and who try to be distracting while they are signing the check or while it is being examined.
- Businesses should set a policy for check cashing and review it with employees frequently. The policy may include:
 - requiring management's approval
 - verifying checks through the issuing bank
 - verifying checks through a check verification service²³

- The identification document should be examined for signs of tampering.

Pretext Calling

Financial institutions and other businesses may facilitate identity theft through their vulnerability to pretext calling. Pretext calling when an identity thief extracts personal identification information by pretending to be someone else on the telephone.

- Employees should be educated about the tactics used by pretext callers, and trained about their responsibility to safeguard customer account information.
- Businesses should develop policies that establish precisely the types of information and the circumstances under which an employee may release customer account information over the telephone.
- Employees should be trained about their responsibility to safeguard customer account information.
- Businesses should maintain strong internal controls to ensure that customer information is adequately safeguarded from improper disclosure, such as providing customers with unique authorization codes.
- Employee activities should be monitored and audited to evaluate susceptibility to

unauthorized disclosures (e.g. pretext calling tests).

- Businesses should file a Suspicious Activity Report and contact regulatory and law enforcement agencies when there is an attempt to obtain customer information under false pretenses. The customer should also be notified.²⁴

Responding to Identity Theft

If a business suspects that an illicit attempt has been made to obtain a customer's identity information, it should report the matter to the proper authorities.

- File a Suspicious Activity Report.
- Contact the Federal Trade Commission and the appropriate state or federal agencies charged with enforcing laws against identity theft.
- Directly contact the appropriate law enforcement agencies if the situation appears to require immediate attention.
- Notify identity theft victims immediately and refer them to the Federal Trade Commission.²⁵

-
1. "Credit Identity Theft: Tips to Avoid and Resolve Problems." In "State of California Department of Consumer Affairs." [www.dca.ca.gov/legal/p-3.html]. January 1999.
 2. Sexton, James. L. "Identity Theft." In "FDIC Financial Institution Letters." [www.fdic.gov/news/news/financial/1999/fi99100.html]. 29 October 1999.
 3. Ibid.
 4. Ibid.
 5. Ibid.
 6. "Credit Identity Theft: Tips to Avoid and Resolve Problems."
 7. Ibid.
 8. Ibid.
 9. Ibid.
 10. "Pretext Calling and Identity Theft." In "FDIC Fraud Alert- Spring 1999." [www.fdic.gov/regulations/resources/fraud/Pretext.html]. 28 July 1999.
 11. "ID Theft: When Bad Things Happen to Your Good Name." In "Federal Trade Commission." [www.ftc.gov/bcp/online/pubs/credit/idtheft.htm]. February 2001.
 12. Ibid.
 13. Ibid.
 14. "Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited." United States General Accounting Office. GAO/GGD-98-100BR. May 1998.
 15. "A Checklist of Responsible Information-Handling Practices." In "Privacy Rights Clearinghouse." [www.privacyrights.org/fs/fs12-ih2.htm]. August 2000.
 16. Ibid.
 17. Ibid.
 18. Ibid.
 19. Ibid.

20. Ibid.

21. Ibid.

22. “Preventing Identity Theft: Industry Practices Are the Key.” In “Privacy Rights Clearinghouse.” [www.privacyrights.org/ar/natsummit.htm]. 15 March 2000.

23. “Check Fraud Against Businesses Proliferates.” In “Better Business Bureau.” [www.bbb.org]. February 2000.

24. “Pretext Calling and Identity Theft.”

25. Sexton, James L. “Identity Theft.”

Tom Rivers was a student intern with the U.S. Attorney’s Office for the Western District of Tennessee in 2002.

