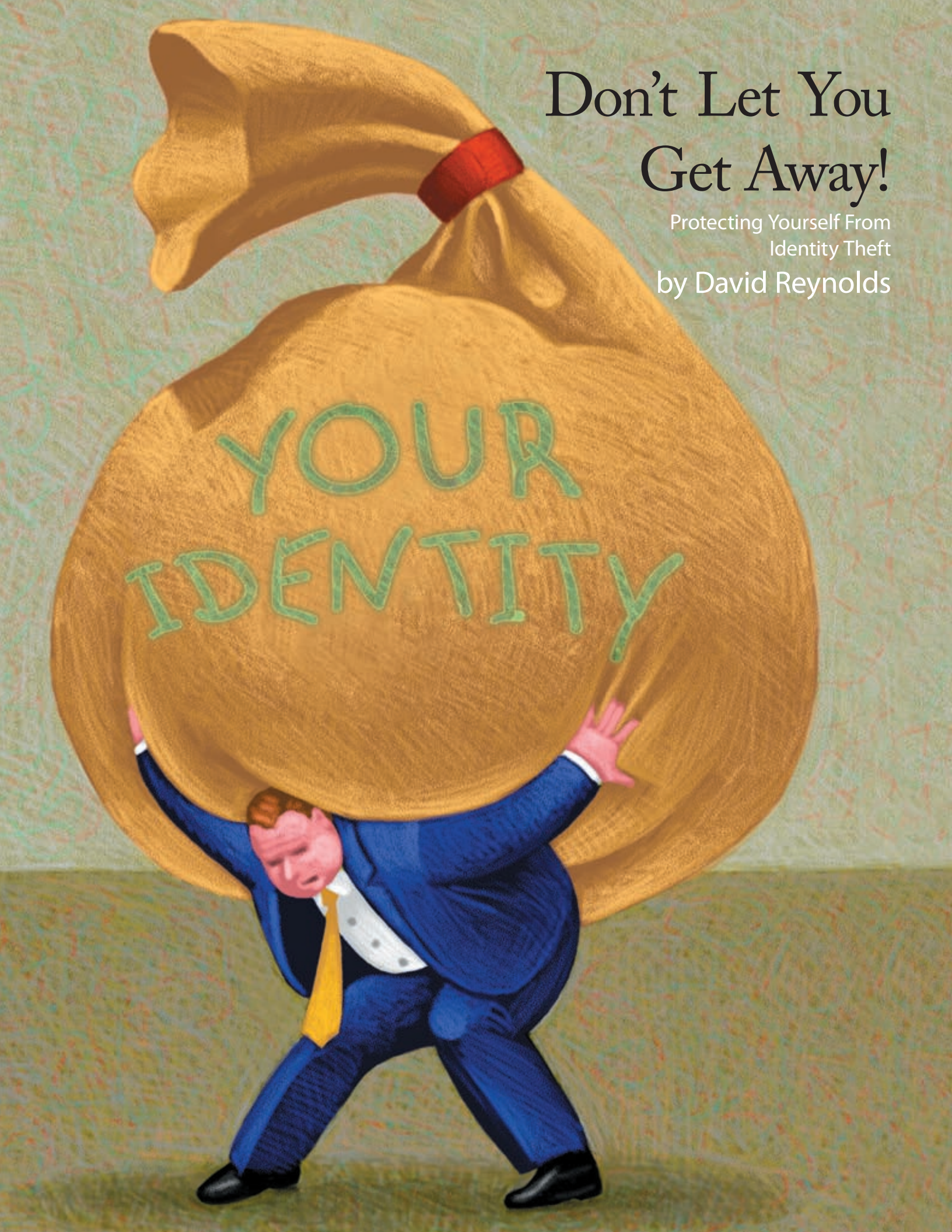
Don't Let You Get Away!

Protecting Yourself From Identity Theft

by David Reynolds



Identity theft is a growing concern among businesses and individual consumers. Information is one of the most highly valued assets a person or company can own, and people with less-than-honorable intentions have become all too aware of its value.

In its 2008 Identity Fraud Survey Report, Javelin Strategy and Research reported that 8.1 million adults in the U.S., or 3.58% of the adult population, were victims of some type of identity fraud. The total amount of losses was $45 billion, and the out-of-pocket expenses incurred by victims of identity fraud averaged $691 per person. Identity theft has proven to be a lucrative business, and law enforcement agencies have been reporting that elements of organized crime around the world are engaging heavily in the identity theft business.

Although identity theft continues to be a significant problem, incidences of identity theft have been declining in recent years. Many experts believe this decline is attributable to consumers and businesses becoming better educated and more careful about protecting their information.

What is Identity Theft?

The term "identity theft" refers to an activity where one person or group performs fraudulent activity on behalf of another person without their knowledge or authorization. The term "identity theft" is a bit misleading, because one's identity cannot truly be stolen. A better term might be "identity impersonation", because a so-called identity thief acquires personal information about another individual and uses it to convince a third party that the thief is the person whose personal information has been compromised.

How Identity Theft Occurs

Identity theft can be accomplished by any number of activities, including:

- Stealing wallets or purses that contain driver's licenses, credit cards, Social Security Cards, etc.
- Stealing mail such as bank statements, credit card statements, credit cards, etc.
- Searching through trash for items containing confidential information (commonly known as "dumpster diving").
- Fraudulently obtaining personal information such as credit reports, employment information, tax records, etc.
- Obtaining electronic information either through accidental disclosure or intentional theft and illegal monitoring of electronic information that is not properly protected.

These different forms of identity theft range from very simple theft (wallets and purses or mail) to more elaborate schemes that include using electronic deception to entice someone to inadvertently revealing confidential information (various forms of "phishing") and breaking into business computer systems and stealing confidential customer information. Accidental disclosure of confidential information can also lead to identity theft. For example, a business may give an old computer system to a charitable organization without properly clearing the system of confidential customer information.

Examples of Identity Theft

The headline-grabbing incidents of identity theft tend to revolve around the theft of electronic information. Laptop computers are stolen, backup tapes are lost, and computer databases are "hacked" (i.e. electronic information is intentionally compromised by unauthorized individuals or groups), and the media outlets are all abuzz with the news. However, most identity theft is not nearly so sophisticated or sensational. Following are a few examples of schemes that have been successfully used to accomplish identity theft:

- Newly issued credit and debit cards are stolen from unsecured mailboxes.
- Discarded offers for credit cards or other types of loans are removed from someone's trash and then used to obtain credit under the identity of the offer recipient.
- Confidential information is obtained through "social engineering" techniques (e.g. telephone calls or neighborhood door-to-door visits) where the would-be thief tricks the victim into revealing information that can then be used to obtain credit with the victim's identity or withdraw money from the victim's accounts.
- E-mail "phishing" schemes impersonate financial institutions or businesses that provide person-to-person financial transactions (e.g. eBay, PayPal). The victim receives an e-mail message informing them they need to update or verify confidential information (e.g. account number, Social Security Number, Internet banking password, etc.). The victim is asked to enter this confidential information. The information is then used by the perpetrator to obtain credit with the victim's identity or steal funds from the victim.
- One of the newer and rapidly growing forms of identity theft is the telephone-based "vishing" schemes. Under this innovative technique, the victim receives a telephone call (usually from an automated system) that appears to be from a trusted source, such as a financial institution or merchant. The victim is asked to enter their account number or other confidential information. This information is then used by the perpetrator to obtain credit with the victim's identity. Another variation of this type of identity theft is known as "smishing." Smishing uses cell phone text messaging to try to get the victim to reveal confidential information.

Website "spoofing" can be the end result of phishing schemes or more sophisticated electronic manipulation of business servers (e.g. "pharming" and "DNS poisoning"). Once the victim is at a bogus, "spoofed" Website, they are enticed to enter confidential information that is then used by the perpetrator to effect identity theft or simply to steal funds from the victim.

How to Protect Against Identity Theft

There are many steps consumers can take to avoid becoming a victim of identity theft. The Federal Trade Commission (FTC) recommends adopting a three-step program they label ***"Deter, Detect, Defend."***

Deter
Information should be safeguarded to deter identity thieves:

- Shred financial documents and all paperwork with personal information before they are discarded. This includes all junk mail and any document that contains personally identifying information.
- Consider renting a secure mailbox (e.g. a Post Office box) instead of using unsecured mailboxes.
- Pick up boxes of checks and new credit and/or debit cards from a financial institution office instead of having them mailed.
- Avoid using or revealing Social Security Numbers unless absolutely necessary.
- Keep Social Security Cards stored in a safe place; do not carry Social Security Cards in wallets or purses.
- Avoid giving out personal information over the telephone, over the Internet, or through the mail unless you are absolutely sure you can trust the party on the other end of the conversation.
- **Never** click on links sent in unsolicited e-mail.
- Use firewalls, antivirus, and anti-spyware software to protect home computers.
- Secure wireless home networks, and avoid sending any confidential information over unsecured wireless networks.
- Avoid using obvious passwords such as family names, telephone numbers, or birth dates.
- Keep personal information stored in a safe, secure place.

- Beware of any request for confidential information that appears to come from usually trusted sources (e.g. financial institutions) through unsecured e-mail. Reputable companies do not request confidential information through unsecured e-mail.
- Do not send confidential information (e.g. account numbers, Social Security Numbers, personally-identifying information) through unsecured e-mail. Consider subscribing to a secure e-mail service if a need to send this kind of information via e-mail exists.

Detect
Routinely monitor financial accounts and billing statements. Pay close attention to any of the following incidences:

- Bills that do not arrive as expected.
- Unexpected credit cards or credit card statements.
- Denials of credit for no apparent reason.
- Calls or letters concerning purchases not made.

There are three major nationwide consumer reporting companies: Equifax, Experian, and TransUnion. They are all required by law to provide consumers with a free copy of their credit report each year. The credit reports must be requested by the consumer, however. It is imperative that each person review all three credit reports each year. Each report should be checked for any of the following activities:

- Inquiries about credit from companies never contacted.
- Accounts never opened.
- Debts on existing accounts that cannot be explained.

All credit card statements and financial account statements should be carefully reviewed when they are received. It is recommended that some type of log be maintained to ensure that statements are received on a regular basis and each statement is reviewed for unauthorized activity.

Defend
Once you suspect you may be a victim of identity theft, it is important to quickly take action to minimize the effects:

- Contact the three credit bureaus and place a "fraud alert" on your credit reports. You can contact the credit bureaus at the following numbers: Equifax – 1-800-525-6285, Experian – 1-888-397-3742, TransUnion – 1-

800-680-7289.

- Close any accounts that have been tampered with or established fraudulently. Call each of the businesses where the accounts exist and inform them of the unauthorized activity on the accounts. Follow up the calls with written notice and include copies of supporting documentation. Ask for verification that the accounts have been closed and the fraudulent debts discharged. Keep copies of all documentation and correspondence!

- File a report with local law enforcement officials. This will establish an official record of the crime.

- Report the theft to the Federal Trade Commission.

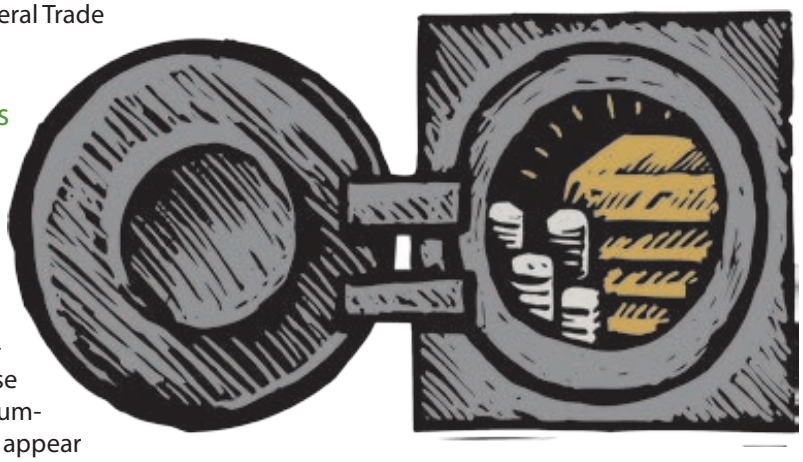
How Financial Institutions Combat Identity Theft

Financial institutions are frequently targeted by identity fraud perpetrators, because the systems they maintain contain a wealth of confidential consumer information. These threats can originate from a number of areas. External threats appear in the form of attempts to intrude into the company's systems (i.e. "hacking") and by attempting to get customers of the institution to inadvertently divulge their confidential information through "phishing" and its counterparts, "vishing" and "smishing," or other forms of social engineering. Internal threats can also appear in the form of "Bot" programs that are inadvertently downloaded from Web sites by financial institution employees through spyware, viruses or other computer "malware;" accidental disclosure by employees; and intentional disclosure by unscrupulous employees.

The potential losses suffered by a financial institution that falls prey to identity fraud can be significant. Of course, monetary losses are a concern anytime financial institution customers are victimized by identity theft, and the institutions have traditionally been willing to absorb a majority of the losses incurred through the illegitimate use of customers' information. Financial institutions also risk suffering serious reputational risk whenever identity fraud occurs as a result of security breaches. Therefore, it is in the best interest of the financial institutions to not only protect its systems, but to also take measures to educate customers about ways to prevent identity theft.

Some of the actions financials institutions are taking to combat identity theft include:

- Performing comprehensive risk assessments of customer information to identify areas where the information may be vulnerable and to establish effective controls to minimize or negate those risks.



- Implementing sophisticated intrusion detection, prevention and monitoring systems on its computer networks.

- Scanning networked systems for known vulnerabilities used by would-be intruders to gain access to systems and taking the steps necessary to counteract those vulnerabilities.

- Performing comprehensive background checks on potential employees.

- Implementing educational programs for both employees and customers to keep them aware of the latest techniques used in identity theft and ways to guard against falling prey to identity fraud.

- Enacting written policies to provide oversight by the financial institution's board of directors and to provide guidelines for management and employees to follow to a.) prevent identity fraud from occurring, and b.) provide a viable, tested plan of action to be followed in the event identity fraud does occur.

- Working with regulatory agencies to ensure that the proper controls are in place and risks are adequately mitigated.

- Utilization of "ethical hacking" techniques and penetration testing to test the controls in place in order to identify any weaknesses.

Customers of a financial institution provide confidential personal information to that institution, and trust the institution to protect that information. As a result financial institutions have an obligation to the customer to provide the protection expected.

Methods used by people who seek to steal this confidential information are continuously evolving. Through collaborative efforts with the financial services industry, financial institution customers, and regulatory agencies, the threats to data security and consumer information can be significantly minimized.

About the Author

David Reynolds serves as the First Vice President of Information Systems for InsBank. He has over 27 years experience in the banking and Information Technology fields.

He has authored and co-authored books on IT and banking for AlexInformation, and has been a regular contributor to the monthly Internet Banking Commentary Newsletter that is published by Alex Information. ◆