Identity Theft: How it Happens, How to Protect Yourself

Robert L Kardell
Michelle E. Minnich
Identity Theft
How it Happens, How to Protect Yourself

By Robert L. Kardell and Michelle E. "Micky" Minnich

The story of the couple from Philadelphia accused of looting fellow tenants in their apartment building is now well known. He was a financial analyst and she was a university student. They began living a jet-set lifestyle, which took them to some of the most intriguing places in the world. Their plans unravelled when they were charged with stealing credit cards out of neighbors’ mailboxes and making false identifications. This is just one of many stories concerning identity theft that have made front-page news.

As the crime of identity theft grows, the questions arise: How is the crime perpetrated, and how can the average person protect himself or herself from the possibility of identity theft?

Definition of Identity Theft
The term “identity theft” has been used extensively by the media in recent years to apply to a variety of circumstances. The term can encompass a number of different scenarios, but generally refers to two separate types of crime. The first type is the most invasive and difficult to correct. It is when a fraudster takes personal information and begins using the information to create a separate identity to apply for credit cards, bank accounts, driver’s licenses and possibly government benefits. It is as if a new person has been created from the unique, identifying information of another.

The second type of identity (ID) theft, and the most pervasive, is simply using another’s financial information for a limited time and for a limited purpose. An example would be the theft of an existing credit card number for a one-time transaction or several transactions for a limited duration of time. These types of theft are easier to deal with because the damage is limited in size or scope. This type of ID theft is categorized as common fraud because identification was not used to open a new account, but rather an existing account was used to perpetrate the fraud. Some studies also refer to this category as “existing account fraud.”

There are two victims of ID theft: the person whose identity was stolen and the company whose assets were stolen. In a study by the Center for Identity Management and Information Protection (CIMIP), the financial services industry was the largest victim of ID theft (37 percent) followed by individuals (34 percent).

History and Statistics
Ten years ago, Congress passed the Identity Theft and Assumption Deterrence Act of 1998, which made ID theft a federal crime. Only after the passage of the act was it possible to keep statistics. The Federal Trade Commission (FTC) began keeping statistics on ID theft in 2003. Identity theft is by far the largest reported fraud. Thirty-six percent, or 246,035, of the cases reported to the FTC are related to ID theft, while the next largest single category is only 6%. The reports of ID theft have continued to increase from year to year, although in decreasing increments.

The more frequent use of portable electronic data which can be lost or stolen can lead to ID theft. As the use of laptops, personal digital assistants (PDAs), USB thumb drives, CDs, DVDs and other removable media has risen, so has ID theft. Of the 24 largest data breaches identified by the Governmental Accounting Office (GAO), nine breaches were due to lost or stolen computer equipment.

Computers also have made the production of quality fake IDs easy to accomplish. Color scanners and digital photography equipment have made it possible to easily create a fake ID that can pass as real. Computers have helped companies manage their money and pay expenses with the use of check-writing programs. The same paper stock purchased for use by a business also can be purchased by counterfeiters to pass bogus checks. In the study by CIMIP, 192 cases, or 37 percent, involved the use of computers or technology to commit the crime.

Finally, the internet has been an incredible tool for both consumers and businesses. Consumers now shop easier and can purchase a variety of goods online. Businesses have found markets that were previously unreachable for a fraction of the marketing costs. This ease of use has led to fraudsters finding new ways to defraud businesses and consumers alike. In the study by CIMIP, 102 cases, or almost 20 percent, involved the use of the internet to commit the crime.

Reasons for Theft
In the report of the CIMIP and the report for the FTC, the reasons for ID theft were studied. The CIMIP reported fraud which was enabled through the use of ID theft was 40 percent of the...
total offenses charged. Behind fraud, ID theft lead to larceny/theft charges in 34 percent, and forgery/counterfeiting charges in 19 percent of the total offenses charged in the study.

**Methods of Theft**

Understanding the means by which ID theft is perpetrated is the key to understanding how to prevent it from happening to you. One key to understanding ID theft is to pinpoint where someone is most vulnerable to having his or her identification stolen. A CIMP study shows the points of vulnerability are businesses at 50 percent, followed by family at 16 percent, home or person at 12 percent and the mail at 9 percent.

**Businesses** - There was a famous bank robber in the '30s, '40s and '50s, Willie Sutton, who when asked by a reporter why he robbed banks replied, “Because that is where the money is.” The same sort of logic can explain why businesses have the highest percentage for ID theft. Businesses tend to make money from marketing, using consumer lists compiled from product registrations, marketing firms and credit header information.

The Association of Certified Fraud Examiners (ACFE) reports that the second leading type of internal fraud perpetrated on financial institutions involves the theft of non-cash assets. The majority of these cases, the ACFE reported, involve the theft of proprietary customer information.9

**Family** - For purposes of the study, the CIMP included friends as well as family and reported that such an individual was involved in 16 percent of the cases. This statistic is telling because the people most likely to have your identifying information besides yourself would be your family and close friends.10 No amount of privacy protection can keep close friends and family from stealing your good credit. This is one reason why you should periodically check your credit report for unauthorized use and/or access.

**Theft from Mail and Trash** - The CIMP study indicates the use of nontechnological means for theft was used in approximately 20 percent of the cases. Of these, mail theft accounted for 43 percent and dumpster diving accounted for 11 percent.11

The accused couple from Philadelphia had in their possession several keys to the mailboxes of other residents of the building. Having keys to another’s mailbox is demonstrative of where important, personal information can be retrieved and where you should start to protect yourself against ID theft. Think of the items that come via mail: credit cards offers, credit card checks, savings and checking account information, social security account information and tax information. All these items can be intercepted or just taken out of your mailbox. Any of these items would provide someone with enough information to start using your identity.

It is now a well-known law that trash left at the curbside of a residence is considered by courts to be abandoned property. Thus, anyone can sift through your trash once you have placed it at the curb. Consider all items that may be in your trash that would aid a thief — a middle name or initial, a date of birth, a credit card account number, bank statements, etc. Do not place your garbage at the end of your driveway the night before trash pick-up, and encourage your neighbors to do the same. If just a couple of people begin to place their trash at the curb on a regular basis, it will be an invitation for an ID thief to start making regular rounds.

**Network Intrusions or Data Breaches** - One example of a company that was the victim of a network intrusion which resulted in the loss of data is TJ Maxx. In that case, a database of customer information was compromised through a breach in the network security from outside the company. TJ Maxx estimated more than 47 million customer records were compromised.

Data breaches can encompass a wider definition of data loss, however, and can include employee theft of data, theft of physical equipment such as a laptop, loss of equipment or data tapes and other losses. According to a GAO report, network intrusions or data breaches accounted for 572 separate incidents and the loss of 80 million records from January 2000 through June of 2005.12

However, in the GAO report the largest 24 data breaches were studied, and of those cases only four resulted in ID
Where Does the Fraud Occur?

<table>
<thead>
<tr>
<th>Credit Card Fraud</th>
<th>Phone or Utility Fraud</th>
<th>Bank Fraud</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Accounts</td>
<td>15.2%</td>
<td>17.4%</td>
</tr>
<tr>
<td>Existing Accounts</td>
<td>10.7%</td>
<td>0.7%</td>
</tr>
<tr>
<td>Unspecified</td>
<td>0.2%</td>
<td>0.5%</td>
</tr>
<tr>
<td>Other</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

Source: Federal Trade Commission, Data Clearinghouse

you can review your credit history, report any potentially fraudulent transactions and monitor account activity. It is a smart idea to set a reminder for yourself to request a credit report once a year around an annual event such as a birthday, anniversary, tax day or the first of the year.

---

Robert L. Kardell, JD, MBA, CFE, ACE is a managing consultant and member of the Forensics & Dispute Consulting division of BKD, LLP. He is based in BKD’s Omaha, Nebraska, office.

Michelle E. “Micky” Minnich, EnCE, CCE, is a senior consultant and member of the Forensics & Dispute Consulting division of BKD, LLP. She serves as the systems administrator and computer forensic examiner in BKD’s Cincinnati office with more than 17 years of information technology experience. She is a Certified Computer Examiner (CCE), EnCase Certified Examiner (EnCE) and member of the High Technology Crime Investigation Association International and The International Society of Forensic Computer Examiners. Contact the author at mminnich@bkd.com.

---

Identity Theft Prevention Tips

- Shred everything. Invest in a good paper shredder and shred credit card offers, expired credit cards, etc.
- Carefully check credit card and bank statements for unfamiliar activity.
- Check your credit report for inaccurate information at least yearly. Consider a credit monitoring service that can notify you of inquiries and changes to your account.
- Protect your Social Security number. Don’t have it printed on checks or driver’s license.
- Put bill payments in a postal service mailbox; don’t leave in your mailbox for postal carrier.
- Limit the amount of personal information kept on portable devices, e.g., laptops, PDAs, etc. If you do need to carry personal information, consider encryption software.
- Take care not to use an unsecured wireless network to do any online financial transactions.
- Memorize passwords and PINs; don’t write down and keep them in your wallet. Use passwords that are a combination of letters, numbers and special symbols.
- Never respond to “phishing” emails. Your bank, Ebay, the IRS and Paypal will never send you an email asking for verification of personal information.