

Exploring Identity Theft

It used to be enough for financial planners to help clients minimize losses by making them aware of the risks inherent in various financial assets—even securities backed by the U.S. Treasury—and by steering them away from imprudent asset allocation and unsuitable investments.

If these seemed like challenges, they were relatively easy to defend against when compared with the potential for losses of money and credit standing which virtually anyone may face today when Social Security numbers or other personal data fall into the hands of criminals and are used for illegal gains at their owners' expense.

“Identity theft” is, to boil down the definition of the 1998 law that made it a federal criminal offense, the unauthorized transfer or use of “a means of identification of another person with the intent to commit...any...activity (which violates federal, state, or local law).”

It can result in losses of money and reputation which may not be discovered for weeks and which may require more time, at possibly significant costs, to recover, if possible at all.

Increasingly vulnerable to such dire circumstances, clients of financial planners have much to do to help themselves, of course, but would surely welcome advice from planners going beyond their traditional responsibilities when opportunities arise.

To help clients to be protected against identity theft, it is important for them to have a sense of the many ways in which it may occur.

Incidents typically involve the unauthorized use of Social Security, bank account, credit card, charge account, driver's license, and telephone calling card numbers; Personal Identification Numbers (PINs), user IDs and passwords, whether unknowingly given to the wrong people or obtained in other ways. A mother's maiden name, a favorite pet's name, or the last four Social Security digits, which are often used to verify identity, are also subject to abuse.

They may be copied from plastic cards, statements (presumably including financial planners' statements), charge slips, or other documents. They may be discerned when criminals watch people punching numbers into ATMs or public telephones, or when they eavesdrop on people giving numbers over phones. They may be retrieved from discarded checks, statements, other records—or discarded forms sent with “pre-approved” credit cards, which are activated without the recipients' knowledge.

According to a U.S. Justice Department advisory on identity theft, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or banking information. Many people respond to unsolicited e-mail that promises them some benefit, but requests identifying data.

“With enough identifying information about an individual, a criminal can take over that individual’s identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges,” says the Justice Department advisory.

Criminals’ e-mails also “lure their targets into a false sense of security by hijacking the familiar, trusted logos of established, legitimate companies,” says a Securities and Exchange Commission advisory.

Whatever the technique, illegally obtained personal information can result not only in withdrawals of money or in large debts but also in crimes that are traced to the victims. How can such incidents be minimized?

- Do not give anyone—on the phone or Internet—a Social Security or other personal number unless sure that the request is legitimate.
- Do not carry your Social Security card or number with you. If your state uses your Social Security number on your driver’s license, ask them to change it to a random number.
- Be cautious when pressing ATM or telephone buttons or dictating numbers on telephones in public.
- Retrieve sales and charge slips, safely retain them, and shred them before discarding them.
- Check statements for charge, bank, brokerage, and other accounts for unauthorized transactions, retain them, and shred them when they are no longer needed.
- Shred unneeded cancelled checks and “pre-approved” credit card offers.
- Delete unsolicited e-mails requesting information from firms you do not know, and verify—by phone, not by e-mail response—the legitimacy of those appearing to be from firms you know.
- Log out when finished with a secure Web site before going to the next.
- Consider using a lockable mailbox or a P.O. Box.
- For optimum security, a cross-cut shredder should be used (not any shredder will do).
- Contact the credit bureaus to opt out of solicitation credit offers via the mail.
- Do not offer personal information over the phone, unless you initiated the call, and the number called is from a reliable source.
- Make your computer safer. There are free programs that can do the trick. For a firewall, zonealarm (www.zonealarm.com) is free. For spyware, adaware (www.lavasoftusa.com) or spybot search and destroy (www.safer-networking.org) are both free. A firewall can keep intruders from pulling information from your hard drive. Spyware is necessary because there are spy programs that can track the Web sites you visit and track your keystrokes on those sites.
- Also, do not carry a checkbook in your wallet or purse.

If identity theft occurs, notify:

- The fraud department of one of the three major credit bureaus (Equifax, 800.525.6285; Experian, 888.397.3742, and Trans Union, 800.680.7289), the police (and obtain a copy of their report), and the Federal Trade Commission (877.438.4338).
- Postal Inspection Service, if an unauthorized change of address form has been filed to redirect mail.
- Social Security Administration (800.269.0271), if a Social Security number has been fraudulently used.
- Creditors and financial institutions, if fraudulent transactions are suspected.

The definitive source for identity theft information on the web: www.consumer.gov/idtheft/.