

## Online, Phone, U.S. Mail or In-Person: Where is Your Credit Card and Personal Identify Safest?

Identity theft is the fastest growing crime according to the Federal Trade Commission (FTC). It occurs when someone takes a piece of your personal information and uses it without your knowledge to commit fraud or theft. An all-too-common example is when an identity thief uses your personal information to open a credit card account in your name, or uses an existing credit card of yours.

Did you know that someone's identity is stolen every 20 seconds?

In a recent survey by the FTC, 12.7% of American adults, or 27 million people, reported that they had become victims of some type of identity theft in the last five years. People whose identities have been stolen can spend months or years -- and thousands of dollars -- cleaning up the mess the thieves have made of their good name and credit record.

Personal Identity Theft: Key Facts

- Victims now spend an average of 600 hours recovering from the crime of identity theft, often over a period of years. Three years ago the average was 175 hours of time, representing an increase of about 2470%.

- While victims are finding out about personal identity theft more quickly, it is taking far longer than ever before to clear their records and recover from the situation.

- Even after the thief stops using the information, victims struggle with the impact of identity theft. That might include increased insurance or credit card fees, inability to find a job, higher interest rates and battling collection agencies and issuers who refuse to clear records despite substantiating evidence of the crime. This "tail" may continue for more than 10 years after the crime was first discovered.

- Approximately 85% of victims found out about the theft of their identity due to an adverse situation - denied credit or employment, notification by police or collection agencies, receipt of credit cards or bills never ordered, etc. Only 15% found out through a positive action taken by a business group that verified a submitted application or a reported change of address.

Read Below for Key Steps to Protect Yourself!

The question remains, where is a person the most safe to make a purchase using a credit card? We compare online, phone, mail and in-person purchases to see where the most identity and credit card theft occurs. Then we provide you the key steps to keep your credit cards and personal identity safe.

Phone Theft: Talk is Not Cheap

Peter Reid, portfolio strategist for EDS Security and Privacy Services, says that "while consumers have learned not to divulge information such as their Social Security number and debit card number over the phone they are still naive and share significant amounts of information from the contents of their wallet -- putting them at greater risk for identity theft and phishing."

Over 70% of consumers freely provide personal information, such as their name, address, postal code, phone number, and account number, or give the answer to a security question, to an unsolicited call.

The price for not being aware is astonishing. For example, more than 38,000 people lost close to \$15.4 million to the operator of a sophisticated-but fraudulent-telemarketing scheme. The man convinced timeshare owners to pay \$400 for unit appraisals by relying on misrepresentations to win them over, such as promising the unit would be purchased once it was appraised. At sentencing, the judge stated that Postal Inspectors had uncovered "the most corrupt, the most extensive, and the most sophisticated mail fraud scheme this Court has ever seen." Seven others, including three of the operator's children and his son-in-law, were convicted for their roles in the scheme.

Be suspicious of marketing calls wanting to verify your address or phone number over the phone. Do not say yes at anytime during the conversation and hang up immediately!

In-Person Theft: How Much Are You Really Paying For Dinner?

Carrying and using your credit cards and other sources of personal information "in-person" appears to be by far the

leading cause of stolen identity and credit card information. "In person" may mean you are right there when the theft occurs - such as with retail purchases at stores or someone "shoulder surfing" you while you're at an ATM machine -- or you left your personal information in a location vulnerable to theft.

According to 2004 research by Javelin Group, a respected retail and business research firm, over 30% of personal identity theft occurred because of a lost or stolen wallet, checkbook or credit card.

Meanwhile, nearly 25% of personal identity theft is due to a "friend" or relative who had personal access to the information, or a corrupt employee who had access to the information.

Offline transactions account for nearly 10% of such theft. A common scenario is going out to eat at restaurant and paying with a credit card. The problem occurs when you receive your next credit card bill and see charges of several hundred dollars for things that you didn't buy! At the restaurant the likely scenario is that the employee probably ran the credit card twice, once for the meal charge and a second time on a magnetic card reader. The employee then copied the data onto a blank credit card and sold it to a third person or used it personally. This is not limited to restaurants, of course - the threat exists at any retail location where you submit your credit card.

**Garbage Theft: Your Trash is Another Person's New Identity**

Another common "live" location for theft of your identity - account for nearly 5% of such crimes according to the Javelin research - is the garbage.

If you fail to properly dispose of personal information containing account numbers, addresses, and dates of birth, you're making it easy for "dumpster divers" to obtain valuable information and steal your identity.

Such garbage diggers will often target upscale neighborhoods. They pick up garbage bags on collection day, take them home and rummage through them for "the gold." The gold can include pre-approved credit cards, discarded bills, and a host of other information containing social security numbers, credit card numbers and more. Tax season is an especially prosperous time for dumpster divers as people dispose of old receipts and financial records carelessly.

**Mail Theft: Involved in Most U.S. Identity Theft**

Identity theft is one of the most serious issues for the U.S. Postal Service, and of course for the general public.

Thieves check mailboxes looking for paid bills or credit card payments that people leave in their mailbox for the postal carrier to collect. They use information from these items to obtain credit or to purchase products and services in the victim's name.

One story involves the operator of a sweepstakes scheme in Rock Hill, South Carolina. Postal Inspectors found that respondents to the mailings were called and told they were winners, but had to mail "taxes" or "Customs fees" to collect their money. Victims either received nothing at all or items vastly inferior to what was represented, losing \$15,000 to \$102,000 apiece in the scheme. The scammer agreed in March 2003 to cease and desist his mailings and pay the Postal Service \$200,000.

Most identity theft somehow involves the U.S. mail - it crosses over to the "in person" theft described above because, beyond strangers robbing your mailbox, the friends, relatives or fellow employees who are stealing your personal information and credit cards are usually lifting it off of a piece of your U.S. mail.

The U.S. Postal Inspection Service has therefore become one of the world's lead agencies in investigating these crimes. Postal Inspectors have jurisdiction to investigate and enforce more than 200 federal statutes involving the U.S. Mail. They are allowed to arrest anyone suspected of stealing mail or filing a false change-of-address order. But don't depend on their measures for your peace of mind.

Postal Inspectors strongly advise people not to leave mail in their mailbox overnight or on weekends. Further, you should never leave your mail on your desk at work when you are not in the vicinity (or even exposed at home if you will be

having friends or relatives over that you don't trust 100%) Also, deposit outgoing mail at the post office and try to remove mail from your mailbox as soon as possible after delivery.

Online Theft: The Safest Place to Do Business is Online - If You're Smart

Despite the fears of those unused to the (relatively) "new" frontier of the Internet, online transactions account for less than 4% of identity theft! And almost all of that 4% is due to people not knowing the difference between a safe and secure website and one that may be "here today, gone tomorrow" or just plain flimsy when it comes to safety of your personal information.

The key you must remember to make your chances of online identity/credit card theft close to zero is to only make purchases through reputable and technologically secure websites like SixWise.com.

When you are making a purchase from the store of a reputable website like SixWise.com, the data you input in the checkout process is encrypted by what is known as Secure Sockets Layer (SSL) before it is sent over the Internet. This technology provides a very secure connection that keeps your data private during transmission over the Internet.

How can you tell if a website has the high-level personal encryption technology, SSL, in place for your personal information? When you are done adding products to your cart on a website and you enter the checkout process where your personal information is being requested, make sure the beginning letters in the URL (web address) at the top of your browser window have switched to "https:" instead of just "http:" If they have not, it is highly recommended you do not make a purchase from that website.

In total, computer crimes accounted for 11.6% of all known cases of identity fraud in 2004. Over half of these digitally driven crimes stem from spyware -- software the computer user unknowingly installs to make ads pop-up when the consumer is online.

SixWise.com highly recommends you read the article, [The World's #1 Internet Threat May Be Robbing Your Identity Right Now ... How to Effectively Detect, Eliminate and Avoid It](#), for tips - and a free program - to prevent identity theft by spyware.

[How to Protect Yourself from Credit Card and Personal Identity Theft](#)

Can you completely prevent identity theft from occurring? Probably not, but you can dramatically minimize your risk by managing your personal information wisely and cautiously.

Here are some tips to help protect you from credit and charge card fraud.

Do:

- Sign your cards as soon as you receive them in the mail, at a store, etc.
- Carry your cards separately from your wallet, in a zippered compartment, a business card holder, or another small pouch.
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your credit card during live transactions, and get it back as quickly as possible.
- Destroy carbon copies of your credit card bills.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Consider replacing paper bills, statements and checks with online versions. Think about moving to an electronic bill payment service, such as your bank or biller's web site, and stop sending signed paper checks through the mail. Visit the [site\(s\)](#) to monitor account activity on a regular basis.

- Sign up for automatic payroll deposits.
  - Use and regularly update firewall and anti-virus software
  - Notify card companies in advance of a change in address.
  - Examine your credit card report from each of the three major credit-reporting agencies once a year. Report any credit card fraud to them. Equifax: 800-525-6285, Experian: 888-397-3742, TransUnion: 800-680-7289
  - Shield your credit card number so that others around you can't copy it or capture it on a cell phone or other camera.
  - Before throwing out any statements containing your credit card (or social security) numbers, it is highly recommended you shred the documents
- Do NOT:
- Lend your card(s) to anyone.
  - Leave cards or receipts lying around, whether at home or at the office.
  - Sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total - this includes the space for "Tips" if you have not filled it in at restaurants.
  - Write your account number on a postcard or outside of an envelope.
  - Give out your account number over the phone unless you're making the call to a company you know is reputable. If you have questions about a company, check it out with your local consumer protection office or Better Business Bureau.
  - Discard a computer without deleting all sensitive data
  - Respond to emails that request you provide your credit card info via email - and don't ever respond to emails that ask you to go to a website to verify personal and credit card information. These are called "phishing" scams.
  - Write your PIN number on your credit card or have it anywhere near your credit card (in the event that your wallet gets stolen).

For More Information

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit [www.ftc.gov](http://www.ftc.gov) or call toll-free, 1-877-FTC-HELP (1-877-382-4357),

From the FREE SixWise.com e-newsletter, the Web's #1 most read newsletter with original articles in all 6 areas of life leading to complete wellness.