

# IDENTITY THEFT

Identity theft continues to be a growing concern. There are a wide number of ways that identity theft can occur. Please see below for a summary of some types of identity theft crimes and tips on what to do to protect yourself.

## **How Your Identity Can Be Stolen**

### Wallet or purse theft

There are three most frequent ways we have been seeing this occur in 5th Precinct;

- leaving a purse or wallet in a vehicle, usually visible
- leaving a purse (sometimes a wallet) unattended/out of view at a restaurant (especially a bar)
- leaving a purse open in a grocery cart with the wallet visible

Wallets and purses are stolen from vehicles anywhere, but especially when the owners are visiting the lakes. Oftentimes, a visitor drives to the location, then stops and leaves the valuables visible, puts them under the seat, or only then puts them in the trunk. There are sophisticated theft rings in areas like that who are watching specifically for that activity. As soon as the visitor walks away, the thief breaks the window and steals the belongings. If the valuables are put in the trunk *at* the location, they know exactly what is in there. If the valuables are put in the trunk *before* the destination, the likelihood of getting broken into drops dramatically. Another popular place where wallets/purses/etc are stolen is during shopping/food breaks at local amenities, such as at restaurants.

At restaurants and bars, some women leave their purses hanging on the back of a chair or otherwise unattended. Sometimes the woman leaves the purse at the table and goes to get another drink; sometimes she goes to the bathroom. Sometimes she is sitting there the whole time but doesn't have her purse in view. In these types of thefts, oftentimes the wallet is stolen from the purse. Sometimes the whole purse is stolen. This is even more likely in a crowded area.

The third most frequent theft targets elderly women especially. In this scheme, the woman is typically shopping at a grocery store. She will often have her purse sitting in the front of the cart, open. Someone approaches her and starts asking questions. While she is distracted, someone else will come in and steal her wallet from her purse.

### Skimming

Another type of theft to be aware of is called skimming. This often occurs at restaurants/businesses where you would feel comfortable giving your credit card over to the waiter or someone else in order to pay your bill. The waiter can then scan your card into a pocket-sized device called a "skimmer," which records all your credit card information. This can then be used to clone a new card and start charging additional purchases. If you are the victim of skimming, be sure to report it to the police. Some credit card companies track where skimming is occurring so they can identify if there is a common place of occurrence.

## Purse Snatches

There are two ways purse snatches often seem to occur in Fifth Precinct.

The first is when a woman is walking down the street or approaching her apartment building. She is often alone and it is often night, although this has occasionally occurred with a group. The suspect runs up behind her and grabs her purse and runs off. If she is approaching an apartment building, sometimes the suspect will approach her asking for something like a cigarette, or the time, or another question that will allow the suspect to get closer. Typically, the suspect is male. Usually there are no injuries aside from anything that occurs in the act of taking the purse itself. The suspect usually does not say anything other than something to potentially get closer.

The second way is closer to typical theft. In these cases, especially during the warmer months, a woman may have her purse sitting on the table at a restaurant while she sits outside. If she is close enough to the sidewalk or a main thoroughfare, the suspect may simply swipe the purse off the table as the suspect walks by and take off running.

The second type is less prevalent in Fifth Precinct but has occurred occasionally.

## Phishing

Phishing is when an identity thief tries to get personal information about you by posing as a legitimate business or institution. This can be done through email, phone, social networking sites like Facebook or MySpace, sites that contain personal information like eBay or PayPal, and so on.

Typically, the thief will have just enough information to seem legitimate. As an example, they may call posing as your bank or credit card company and have your credit card number and expiration date. They may say they're concerned that your card was stolen and they need to verify it's in your possession. They may ask for the three-digit code on the back. If you provide that, they would have all the information needed to use your card for purchases. Via email, you may receive an email from what appears to be your bank or a similar company you would trust. The email often implies or says there's some sort of suspicious activity and urges you to log onto your account. There would be a link to what looks like the website, but in fact is a clone of the site. When you put in your username and password, they are able to steal the information.

## The Most Prevalent Schemes In General

According to [spendonlife.com](http://spendonlife.com), the latest findings show that the below six methods remain the most popular ways for identity thieves to obtain your information:

1. Lost or stolen wallets
2. Card-skimming, or stealing your personal information during a transaction
3. "Friendly" theft, or identity theft by friends, family members, or other people you know
4. Mailbox raiding and dumpster diving for your personal and financial information
5. Online methods, including e-mail phishing schemes
6. Data breaches, or hacking into company systems to gain customer information

## **If Your Identity/Credit Cards Are Stolen, What Happens?**

In most cases that we have seen, if your wallet/credit cards are stolen, within an hour it is used repeatedly at big name stores and gas stations. These bills are often anywhere from a few hundred to thousands of dollars. If your credit card company/bank notices any unusual spending, they may contact you asking about it. If you are unaware that your wallet/credit cards were stolen, this may be your first indication that something happened.

Depending on the sophistication of the thief, they may attempt other scams as well. They could open new credit card accounts using your name, date of birth, and Social Security Number. When they use the credit card and don't pay the bills, it gets put on your credit report.

Being in charge of a stolen credit card, they may call the credit card issuer and ask to change the mailing address on the account. You wouldn't receive the bills and the identity thief could use the stolen or fraudulently-obtained card.

The thief could establish cell phone service in your name, open a bank account in your name and write bad checks on the account, purchase larger items like a car or house by taking out an auto loan or house loan in your name, etc.

Using a stolen debit card, they could drain your account.

## **What You Can Do: Prevention Tips/Actions to Take if Your Identity is Stolen**

### Preventing Identity Theft

- Do not leave your purse or wallet unattended or out of sight.
- Do not leave valuables visible in your car. If you must have your wallet/purse/etc but cannot bring it with you, put it in the trunk of your car *before* reaching your destination. Don't forget that laptop bags and other items are also targeted by thieves and may contain personal information.
- If you use a laptop, consider getting laptop security software installed. There is often an annual fee through a company that will track your computer if stolen. Some companies allow you to delete personal data from afar. These companies work with local law enforcement to try to return your laptop to you if stolen, and can help catch criminals.
- Minimize the number of credit cards and other identification information that you carry with you on a regular basis. Keep unused credit cards in a safe place.
- Make a photocopy of the front and back of each card and store the copies in a safe place, like a safe or other locked box. This will make it easier to know what numbers to call if a card is stolen.
- Do not carry your or others' Social Security Card with you. Keep them in a safe place.
- If you use checks, avoid carrying more blank checks than needed.
- Memorize your passwords and PIN; do not keep them in your wallet.
- Shred all mail/information that contains personal information, especially bank statements and credit card applications. Shred or cut up used/expired credit cards or ATM cards.
- Verify any requests for personal information with the originating company. Do not use the phone number, email address, or website link you are provided by the person. Call the number/directly type in the website address that you know is legit.
- Get your credit report once a year and check your billing statement every month. Ensure that all purchases are your own.

- If you notice that your credit card bill seems unusually high, check all the purchases to make sure they are yours.
- When travelling, have your mail held at the local post office or have someone stop by to pick it up.
- Take credit card and ATM receipts with you. Do not throw them away in a public trash container.
- Be careful at ATMs and using phone cards. People looking over your shoulder can obtain your PIN and access your account.
- Always keep your credit card in your sight when you give it to cashiers to swipe. If possible, walk up to pay rather than giving it to the waiter. Some restaurants use the skimmers at the table as the legitimate way to pay. Keep in mind that the information can be downloaded off those machines. Ensure that you are in a restaurant you trust and that you are taking all precautions necessary.
- Ask for the receipt even at cafes. The cashier may not be stealing your identity but could be ringing additional purchases on the card. Many places don't require a signature for purchases under \$25 but it's a good idea to ask for the receipt regardless to ensure nothing was added.
- Choose a PIN that is not based on a birthday, anniversary, address, or Social Security number. Memorize it and don't share it with anyone. Don't keep it in your wallet.
- Remove your name from the marketing lists of the three major credit reporting bureaus (Equifax, Experian, and Trans Union). This will limit the number of pre-approved offers of credit received.
- Sign up for Direct Marketing Association Mail Preference Service and the Telephone Preference Service. Your name will be added to computerized name deletion lists used by nationwide marketers.

### **If Your Card/Wallet/Purse/Mail is Stolen**

- Report stolen credit cards or ATM cards immediately.
  - Place a fraud alert on your credit reports
  - Close the accounts that have been tampered with or opened without your permission
  - Call 911 to report it to the police. Note: you can also call 311 (612-673-3000) or report it online at <http://www.ci.minneapolis.mn.us/police/e-report/>. If there is any evidence left behind at the scene or there is suspect information, call 911. 911 will direct you to 311 if necessary.
  - File a complaint with the Federal Trade Commission. This can be done online at <https://www.ftccomplaintassistant.gov/> or via the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261.
- When dealing with authorities/financial institutions, act quickly and assertively to minimize the damage; keep a log of all conversations, dates, names, and telephone numbers; and confirm conversations in writing. Send correspondence by certified mail (return receipt requested). Keep copies of all letters and documents.
- When you report the crime to the police department, obtain a copy of the police report and if it is assigned, obtain the telephone number of the investigator to provide it to creditors or others who may require verification of your case.
- There are two laws that will help protect you from fraudulent purchases but they differ between credit cards and ATM cards. More information can be found here: <http://www.spendonlife.com/guide/stolen-credit-debit-cards>
- You can place a security freeze on your account as well if you'd like. To do this, you must contact all three major credit reporting bureaus. (See their contact information below) A security freeze is an aggressive lockdown of your account, which does not allow any new activity on your account and does not allow most institutions to pull your

credit report. This can make it difficult or impossible to get loans, apartments, etc, but it is the most aggressive defense to prevent an identity thief from getting loans or credit cards with your personal information.

- If your SSN is stolen and used, call the Social Security Administration to report fraudulent use of your social security number. Order a copy of your Social Security Earnings and Benefits Statement and check it for accuracy.
- If your passport is stolen, notify the passport office in writing to be on the lookout for anyone ordering a new passport fraudulently.
- If your checks are stolen or bank accounts were set up fraudulently, report it to the check verification companies. Put stop payments on any outstanding checks you are unsure of. Cancel your checking and saving accounts and obtain new account numbers.
- If your mail is stolen or there was a falsified change of address forms, contact the local postal inspector. The local post office will have the telephone number or you can check their website at [www.usps.gov/websites/depart/inspect](http://www.usps.gov/websites/depart/inspect).

### Three Major Credit Reporting Bureaus

- [Equifax](http://www.equifax.com): www.equifax.com - 1-800-525-6285
- [Experian](http://www.experian.com): www.experian.com - 1-888-397-3742
- [TransUnion](http://www.transunion.com): www.transunion.com - 1-800-680-7289

### More Information

Find more information and tips on preventing identity theft by visiting these sites:

- Federal Trade Commission's Identity Theft  
Site: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- United States Department of Justice Identity Theft  
Site: <http://www.justice.gov/criminal/fraud/websites/idtheft.html>
- FDIC Identity Theft Site: <http://www.fdic.gov/consumers/consumer/alerts/theft.html>
- Spend On Life: <http://www.spendonlife.com/identitytheft>

For more crime prevention resources, please visit:

<http://www.ci.minneapolis.mn.us/police/crime-prevention/>

To locate your Crime Prevention Specialist in Minneapolis, please visit:

<http://www.ci.minneapolis.mn.us/safe/docs/safe-staff-map.pdf> or

<http://www.ci.minneapolis.mn.us/safe/safe-teams.asp>