

Tyndall AFB Preventive Law Program Series

Legal Assistance Series

IDENTITY THEFT

WHAT TO DO WHEN AN IMPOSTER STRIKES

This handout contains basic information on the above area. If you have specific questions, come in to see a Judge Advocate for legal assistance



OFFICE OF
THE STAFF JUDGE ADVOCATE 325 FW/JA
TYNDALL AFB, FL 32403

Identity Theft

What To Do When An Imposter Strikes

It can happen to anyone. The phone rings and a collection agency demands that you pay past-due accounts for merchandise you never ordered. The supermarket refuses your checks because you have recently bounced several. You cannot understand what is happening because you have a perfect record and always pay bills on time. What has happened?

The crime of identity theft is on the rise. Using a variety of methods, criminals steal credit card numbers, driver's license numbers, Social Security numbers, ATM cards, telephone calling cards and other key pieces of individuals' identities. They use this information to impersonate their victims, spending as much money as they can in as short a time as possible before moving on to someone else's name and account information.

Even though victims are usually not saddled with paying their imposters' bills, they are often left with a bad credit report and must spend months and even years regaining their financial health. In the meantime, they have difficulty writing checks, obtaining loans, and renting apartments. Stealing wallets used to be the best way identity thieves obtained credit card numbers and other pieces of identification. Now more sophisticated means are commonly used:

- Accessing your credit report fraudulently, for example, by posing as an employer, loan officer or landlord and ordering a copy;
- "Shoulder surfing" at ATM machines and phone booths in order to capture PIN numbers;
- Stealing mail from mailboxes to obtain newly issued credit cards, bank and credit card statements, pre-approved credit offers, or tax information;
- "Dumpster diving" in trash bins for unshredded credit card and loan applications.

Take these preventive steps to minimize your losses in case of identity theft

Reducing access to your personal data:

1. To minimize the amount of information a thief can steal, do not carry extra credit cards, your Social Security card, birth certificate or passport in your wallet or purse, except when needed.
2. To reduce the amount of personal information that is "out there," consider the following:
 - To opt out of receiving pre-screened credit card offers, call 1-888-5-OPT-OUT. These, when tossed into the garbage, are a potential target of identity thieves who use them to order credit cards in your name.
 - Have your name and address removed from the phone book and reverse directories.

- The Direct Marketing Association's (DMA) Mail, E-Mail and Telephone Preference Service allow you to opt out of direct mail, e-mail, and phone marketing.
3. Install a locked mailbox at your residence to reduce mail theft. Or use a post office box.
 4. When you order new checks, do not have them sent to your home's mailbox. Pick them up at the bank instead.
 5. When you pay bills, do not leave the envelopes containing your checks at your mailbox for the postal carrier to pick up. If stolen, your checks can be altered and then cashed by the imposter. It is best to mail bills and other sensitive items at the post office rather than neighborhood drop boxes.
 6. Pay close attention to billing cycles. Follow up with the creditor if you do not receive a bill on time.
 7. Reduce the number of credit cards you actively use to a bare minimum. Carry only one or two of them in your wallet. Cancel all unused accounts. Even though you do not use them, their account numbers are recorded in your credit report.
 8. Keep a list or photocopy of all your credit cards, the account numbers, expiration dates and telephone numbers of the customer service and fraud departments in a secure place (not your wallet or purse) so you can quickly contact your creditors in case your cards have been stolen. Do the same with your bank accounts.
 9. Never give out your credit card number or other personal information over the phone unless you have a trusted business relationship with the company and **you have initiated the call**. Identity thieves have been known to call their victims with a fake story that goes something like this. "Today is your lucky day! You have been chosen by the Publishers Consolidated Sweepstakes to receive a free trip to the Bahamas. All we need is your credit card number and expiration date to verify you as the lucky winner."
 10. Order your credit report once a year from each of the three credit bureaus to check for inaccuracies and fraudulent use of your accounts.
 11. Always take credit card receipts with you. Never toss them in a public trash container.
 12. Watch the mail when you expect a new or reissued credit card to arrive. Contact the issuer if the card does not arrive.

Passwords and PINS:

13. When creating passwords and PINs (personal identification numbers), do not use the last four digits of your Social Security number, your birth date, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves.

14. Ask your financial institutions to add extra security protection to your account. Most will allow you to use an additional code (a number or word) when accessing your account. Do not use your mother's maiden name, as identity thieves can easily obtain that.
15. Memorize all your passwords. Don't record them on anything in your wallet or purse.
16. Shield your hand when using a bank ATM machine or making long distance phone calls with your phone card. "Shoulder surfers" may be nearby with binoculars or video camera.

Social Security numbers:

17. Protect your Social Security number (SSN). Release it only when absolutely necessary (like tax forms, employment records, most banking, stock and property transactions). The SSN is the key to your credit and banking accounts and is the prime target of criminals. If a business requests your SSN, ask if it has an alternative number that can be used instead. Speak to a manager or supervisor if your request is not heeded. Ask to see the company's policy on SSNs. If necessary, take your business elsewhere. If the SSN is requested by a government agency, look for the Privacy Act notice. This will tell you if your SSN is required, what will be done with it, and what happens if you refuse to provide it.
18. Do not have your SSN printed on your checks. Don't let merchants hand-write it onto your checks because of the risk of fraud. There is no law against this, so you may need to be assertive.
19. Order your Social Security Earnings and Benefits Statement once a year to check for fraud.

Responsible information handling:

20. Carefully review your credit card statements and phone bills, including cellular phone bills, for unauthorized use.
21. Do not toss pre-approved credit offers in your trash or recycling bin without first tearing them into small pieces or shredding them. They can be used by "dumpster divers" to order credit cards in your name and mail them to their address. Do the same with other sensitive information like credit card receipts, phone bills and so on. Home shredders can be purchased in many office supply stores.
22. Demand that financial institutions adequately safeguard your data. Discourage your bank from using the last four digits of the SSN as the PIN number they assign to customers. Insist that banks remove account numbers from ATM slips (many have already done so). Also insist they shred all paper records before discarding them. By not adopting responsible information-handling practices, they put their customers at risk for fraud.

23. When you fill out loan or credit applications, find out how the company disposes of them. If you are not convinced that they store them in locked files and/or shred them, take your business elsewhere. Some auto dealerships, department stores, car rental agencies, and video stores have been known to be careless with customer applications. When you pay by credit card, ask the business how it stores and disposes of the transaction slip. Avoid paying by credit card if you think the business does not use adequate safeguards.
24. Store your canceled checks in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your phone number and driver's license number. Never permit your credit card number to be written onto your checks.
25. Any entity that handles personal information should train all its employees on responsible information-handling practices. Persuade the companies, government agencies, and nonprofit agencies with which you are associated to adopt privacy policies and conduct privacy training.

If you become the victim of identity theft, it is important to act immediately to stop the thief's further use of your identity:

26. Report the crime to the police immediately. Give them as much documented evidence as possible. Get a copy of your police report. Credit card companies, your bank, and the insurance company may require you to show the report in order to verify the crime.
27. Immediately call all your credit card issuers. Get replacement cards with new account numbers. Follow-up in writing. This protects you in case of a dispute with the credit card issuer.
28. Call the fraud units of the three credit reporting companies – Experian, Equifax and TransUnion. Report the theft of your credit cards or numbers. Ask that a fraud alert be placed on your accounts. Be sure to ask how long the fraud alert is posted on your account, and how you can extend it if necessary.
29. Notify your bank(s) of the theft. Cancel your checking and savings accounts and obtain new account numbers. Ask the bank to issue you a secret password that must be used in every transaction. Put stop payments on any outstanding checks that you are unsure of.
30. To prove your innocence, you may be required to fill out fraud affidavits with banks and credit grantors where fraudulent accounts have been established in your name.
31. If you use an ATM card for banking services, get a new card, account number and password. Do not use your old password. When creating a password, avoid such commonly used numbers as the last four digits of your Social Security number and your birth date.

32. If you have had checks stolen or misused, report it to the major check verification companies so they can notify retailers not to accept the checks.
33. You may want to have your SSN changed if your number has become associated with bad checks and credit. Contact your local office of the Social Security Administration.
Caution: This step should be reserved for only the most extreme situations. You must be sure to notify all credit grantors and credit reporting bureaus of your new SSN.
34. Notify the Postal Inspector if you suspect mail theft. Theft of mail is a felony.
35. If you have a passport, notify the passport office to be on the lookout for anyone ordering a new passport fraudulently.
36. Call your telephone, electrical, gas and water utilities. Alert them to the possibility that someone may attempt to open new service using your identification. Also contact your long distance company. You may need to cancel your long distance calling card if it has been stolen or if “shoulder surfers” have accessed the account number.
37. You may want to change your driver's license number if someone has been using yours as identification on bad checks. When requesting a new number from the Department of Motor Vehicles, you might be asked to prove that you have been damaged by the theft of your driver's license.
38. In dealing with the authorities and financial institutions, keep a log of all conversations, including dates and names. Send correspondence by certified mail. Keep copies of all letters and documents. Provide your police report number to expedite reporting the crime.
39. Consider seeking legal counsel, especially if you have difficulty clearing up your credit history, or your case is complex and involves a lot of money. An attorney can help you recover from the fraud and determine whether your rights under various credit, banking, SSN and other laws have been violated.
40. Pay attention to your own mental health. Victims of identity theft often report they feel they are somehow to blame. They can also feel violated, even powerless, due to the fact that few, if any, of the authorities that have been notified of the crime step forward to help the victim. Discuss your situation with a friend or counselor. Seek help from a victims' rights organization.

Resources

Credit Reporting Bureaus

Equifax — www.equifax.com

To order your report, call: 1-800-685-1111

or write: P.O. Box 740241, Atlanta, GA 30374-0241

To report fraud, call: 1-800-525-6285
and write: P.O. Box 740241, Atlanta, GA 30374-0241

Experian — www.experian.com

To order your report, call: 1-888-EXPERIAN (397-3742)
or write: P.O. Box 2104, Allen TX 75013

To report fraud, call: 1-888-EXPERIAN (397-3742)
and write: P.O. Box 9532, Allen TX 75013

TransUnion — www.transunion.com

To order your report, call: 800-916-8800
or write: P.O. Box 1000, Chester, PA 19022.

To report fraud, call: 1-800-680-7289
and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton,
CA 92834-6790

Remember, you are entitled to a free credit report if you are a victim of identity theft, if you have been denied credit in the past 60 days, if you receive welfare benefits, or if you are unemployed.

If your SSN has been used fraudulently for employment purposes, report the problem to the Social Security Administration at (800) 269-0271. You may order your Earnings and Benefits Statement by calling (800) 772-1213. Unfortunately, the SSA has no procedures in place to deal with non-employment types of SSN fraud, such as credit application fraud. For extreme cases of identity theft, they may be willing to change your SSN.

To remove your name from mail, e-mail and phone lists (DMA – www.the-dma.com)

- Mail Preference Service – P.O. Box 9008, Farmingdale, NY 11735-9008
- E-Mail Preference Service – visit www.e-mps.org
- Telephone Preference Service – P.O. Box 9014, Farmingdale, NY 11735-9014

To report fraudulent use of your checks

- TeleCheck:
1-800-710-9898 or 927-0188
- Certegy, Inc. (previously
Equifax Check Systems):
1-800-437-5120
- International Check Services:
1-800-631-9656
- To find out if the identity thief has been passing bad checks in your name, call:
 - SCAN: 1-800-262-7771

To stop the credit bureaus from sharing your personal information

- Equifax, Inc.
Options
PO Box 740123
Atlanta, GA 30374-0123
- Experian
Consumer Opt-Out
701 Experian Parkway
Allen, TX 75013
- TransUnion
Marketing List Opt Out
PO Box 97328
Jackson, MS 39288-7328

The Federal Trade Commission web site provides valuable information

<http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm#intro>

If you have been a victim of Identity Theft, call the FTC's Identity Theft Hotline

1-877-IDTHEFT