

Safeguard yourself from Identity Theft

Identity Theft—the unauthorized and illegal use of your name, Social Security number or other personal information—is the fastest growing crime in the United States. The Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year. At ING DIRECT, we want to make sure you know all the facts about protecting yourself. From training our employees about Identity Theft to establishing rigorous security standards to data encryption and fraud detection, we've put serious safeguards in place to protect you, your information, and your money.

Avoid becoming a victim by:

- Removing mail from your mailbox every day (or better yet, sign up for electronic statements!).
- Never leaving bills in your mailbox overnight—always put them in a secure US postal mailbox (or better yet, get rid of them and pay bills online!).
- Knowing your billing cycles. Follow up with creditors if bills or new cards don't arrive on time. (An identity thief may have filed a change of address request in your name with the creditor or the post office.)
- Shredding receipts and mail, especially pre-approved credit card applications.
- Eliminating the receipt of pre-approved offers of credit by calling 1-888-5-OPT-OUT.
- Never carrying your Social Security card or bank passwords or other sensitive information in your wallet.
- Accounting for all new checks when you receive them in the mail.
- Removing your name from direct mail lists and writing to the companies you do business with, asking them not to sell or rent your name. You can visit the Direct Marketing Association's website (www.the-dma.org) to learn about the laws that protect you as a consumer and how to get your name removed from these lists.
- Ordering copies of your credit report once a year from one of the three national credit-reporting agencies and looking for accuracy and for indications of fraud, such as unauthorized applications, unfamiliar credit accounts, credit inquiries and defaults and delinquencies that you did not cause. (Need some examples? Please visit the Tips & Tools section of our website.)
- Checking your Social Security Earnings and Benefits statement once each year to make sure that no one else is using your Social Security number for employment.

Be suspicious about telephone calls where:

- The company has a name that is intended to sound like a government agency or a well-known company.
- The company is unwilling to send you written information on the offer or give you references.
- Someone claims you've won a prize and you haven't entered a contest.
- A telemarketer asks for your Social Security number, calling card or credit card number, so you can purchase products or qualify for prizes.
- You have to pay a fee before you receive complimentary goods or services.
- In general things sound too good to be true!

Bank, shop and spend wisely by:

- Canceling your unused credit cards so that their account numbers will not appear on your credit report.
- Signing your credit cards immediately upon receipt.
- Doing business with companies you know are reputable, particularly online.

- Using a secure browser when you conduct business online that encrypts or scrambles purchase information. (Make sure your browser's padlock or key icon is active.)
- Avoiding opening e-mail from unknown sources. We recommend purchasing virus detection software.
- Never clicking on an e-mail link. Go to the company's website yourself and fill out information there or call them.
- Asking businesses what their privacy policies are and how they will use your information: Can you choose to keep it confidential? Do they restrict access to data?

Just how much are you liable for?

By law you are only liable for the first \$50 of unauthorized charges against a credit card account. Still, restoring your identity can be a tremendous inconvenience. Exercise a little preventive maintenance. Protect yourself against this crime. For more personal finance tips, visit the Tips & Tools section of our website at ingdirect.com/tools, the American Bankers Association's Consumer Connection at www.aba.com, the Federal Trade Commission's OnGuard Online site at <http://onguardonline.gov/idtheft.html>, or the Identity Theft Resource Center at www.idtheftcenter.org.

Just what are we doing to help you?

ING DIRECT's Privacy Policy exceeds the standards required by congressional legislation. One requirement of the Gramm-Leach-Bliley Financial Modernization Act of 1999, or GLB, requires financial institutions to provide customers with the ability to "opt-out" of information sharing. We're proud to report that ING DIRECT has adopted an "opt-in" Privacy Policy, which means that we will not share your data unless you say we can.

With ING DIRECT's Orange Security Guarantee, your money and privacy are protected from the instant you open your account. Our security features are top-notch and we continue to make enhancements. If your security is ever compromised, we'll make things right. That's the Orange Security Guarantee.

What to do if you are a victim

1. Contact your bank(s) and credit card issuer(s) immediately to:

- Protect the access to your accounts.
- Stop payments on missing checks.
- Change personal identification numbers (PINs) and online banking passwords.
- Open a new account if appropriate.

Be sure to indicate to the bank or card issuer all of the accounts and/or cards potentially impacted, including ATM cards, check (debit) cards and credit cards. Contact the major check verification companies to request they notify retailers using their databases not to accept these stolen checks, or ask your bank to notify the check verification service with which it does business. Two of the check verification companies that accept reports of check fraud directly from consumers are Telecheck **1-800-710-9898** and International Check Services **1-800-366-5010**.

2. File a report with your local police department and:

- Obtain a police report number with the date, time, police department, location and name of the police officer taking the report.
- **Agree to an investigation (if the police recommend it)** into the loss. The police report will be helpful when clarifying to creditors that you are a victim of identity theft. Complete an Identity Theft Affidavit form and submit it to the appropriate companies. You can download a copy of this form at www.consumer.gov/idtheft.

3. Contact the three major credit bureaus and request a copy of your credit report and:

- Review your reports to make sure additional fraudulent accounts have not been opened in your name or unauthorized changes made to your existing accounts.
- Request the “inquiries” be removed from your report from the companies that opened the fraudulent accounts. Here are the major credit bureaus and their phone numbers: Trans Union **1-800-680-7289**, Experian **1-888-397-3742** and Equifax **1-800-525-6285**. You may also contact the FTC’s ID Theft Consumer Response Center toll-free at **1-877-IDTHEFT**.

Recheck your credit report in a few months to:

- Verify your corrections and changes.
- Make sure no new fraudulent activity has occurred.
- Request a “fraud alert” for your file and a victim’s statement asking creditors to call you before opening new accounts or changing your existing ones. This can help prevent an identity thief from opening additional accounts in your name.

Check your mailbox for stolen mail to:

- Make sure no one has requested an unauthorized address change, title change, or PIN change or ordered new cards or checks to be sent to another address.
- If a thief has stolen your mail, contact your local post office and police.

Maintain a written chronology of what happened by noting:

- What was lost.
- The steps you took to report the incident to the various agencies, banks and firms impacted.
- The date, time, contact telephone numbers, name of the person you talked to and any relevant report or reference number and instructions.

Send a registered letter to all creditors where fraudulent accounts have been opened and:

- Include a copy of the police report.
- Include the ID Theft Affidavit.
- Request that the institution send you a letter of release to clean up the account and acknowledge that it is fraudulent.

IMPORTANT CONTACT INFORMATION

For credit checks and theft information, contact:

Institution	Phone Number	Internet Address
Federal Trade Commission	1-877-IDTHEFT	www.consumer.gov/idtheft
Trans Union	1-800-680-7289	www.transunion.com
Equifax	1-800-525-6285	www.equifax.com
Experian	1-888-397-3742	www.experian.com
Telecheck	1-800-710-9898	www.telecheck.com
International Check Services	1-800-366-5010	N/A
OnGuard Online	N/A	http://onguardonline.gov/index.html
Identity Theft Resource Center	1-858-693-7935	www.idtheftcenter.org
Social Security Administration	SSN Fraud Hotline 1-800-269-0271	www.ssa.gov
The National Fraud Information Center	1-800-876-7060	www.fraud.org
U.S. Postal Inspection Service	SSN Fraud Hotline 1-800-372-8347	www.usps.gov/postalinspectors

To find out if the thief has been passing bad checks in your name, call the Shared Check Authorization Network (SCAN) at 1-800-262-7771.

For ING DIRECT, contact:

Name	Phone Number	Email Address/ Internet Address
Bob Addeo	1-302-255-3010	raddeo@ingdirect.com
Theresa Ciabattoni	1-302-255-3207	tciabattoni@ingdirect.com
Loss Prevention	1-866-877-2995 (toll-free)	fraudwatch@ingdirect.com
Visitors/Sales	1-800-ING DIRECT	www.ingdirect.com

