

# IDENTITY THEFT PREVENTION TIPS

Understanding how it can happen...learning how to protect yourself Identity theft and account fraud is making big headlines. They happen when someone steals personal information such as bank account numbers or Social Security numbers and then pose as the owner of that information. The thief's goal is to drain your bank accounts of all its cash or to charge as much on a credit card before getting caught, resulting in enormous debt in your name.

The threat is real, and the government estimates that 400,000 people are victimized by these crimes each year. Kingston National Bank works hard every day to ward off these threats, but maximum security is possible only with increased awareness and attention. Below are some steps you can take to help prevent the theft of your identity. Together, we can head off identity theft and account fraud before it happens.

- [Reduce Access to Your Personal Information](#)
- [Social Security Number](#)
- [Bank Accounts](#)
- [Passwords and PINS](#)
- [Credit Cards](#)
- [Mail](#)
- [Resources](#)

## **Reduce Access to Your Personal Information**

- Remove your name from the marketing lists of the three credit reporting bureaus—Equifax, Experian, and Trans Union. This will limit the number of pre-approved offers of credit that you receive. Any pre-approvals you do received that are tossed into the garbage without being shredded are a potential target of identity thieves who use them to order credit cards in your name.
- Sign up for the Direct Marketing Association's Mail Preference Service and the Telephone Preference Service. Your name will be included on computerized name deletion lists used by nationwide marketers.
- Have your name and address removed from the phone book and reverse directories.
- Never give out credit card or personal information over the telephone 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." Do not give information to a stranger; even one claiming to be from your bank.
- Keep all personal information secured.
- Do not carry extra credit cards, social security card, passport or a birth certificate in your wallet or purse, except when needed.
- Verify credit reports annually.

## **Social Security Number**

- 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 which can be used instead

- Do not let merchants hand-write your SSN onto your checks.
- When you receive your annual Social Security Earnings and Benefits Statement, take time to read it and check for fraud.

### **Bank Accounts**

- Do not print your SSN, driver's license number, credit card number or telephone number on your checks.
- When you order new checks, do not have them sent to your home mailbox. Pick them up at the bank instead.
- Store your canceled checks or images in a safe place. In the wrong hands, they could reveal a lot of information about you, including the account number, your telephone number and driver's license number.
- Report lost or stolen checks immediately. Your bank will block payment on the check numbers involved.
- Balance account statements promptly.
- Keep a list of your bank account numbers with telephone numbers of customer service and fraud departments in a safe place.
- Notify your banker of suspicious phone inquiries such as those asking for account information to "verify a statement" or "award a prize."

### **Passwords and PINS**

- Memorize your passwords. Do not record them on anything in your wallet, purse, or electronic organizer. Keep your passwords safe and secure.
- When creating passwords and PINs (personal identification number) do not use the last four digits of your social security number, your birthdate, middle name, pet's name, consecutive numbers or anything else that could easily be discovered by thieves.
- Avoid anyone looking over your shoulder during an ATM transaction or using your phone card for long distance calls.

### **Credit Cards**

- Keep a list or photocopy of all you 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.
- Always take credit card receipts with you; do not leave them on the table – be sure your server picks up the original. Never toss them in a public trash container.
- Do not toss pre-approved credit offer 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, unused bank deposit tickets, bank statements, phone bills and so on. Home shredders can be purchased in most office supply stores.
- 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. Although you do not use them, their account numbers are recorded in your credit report that is full of data that can be used by identity thieves.

- Watch the mail when you expect a new or reissued card to arrive. Contact the issuer if the card does not arrive.
- Carefully review your statements for unauthorized use.

## **Mail**

- Install a locked mailbox at your residence to reduce mail theft, or use a post office box.
- Shred all received mail containing sensitive information: bank statements, canceled checks, credit card applications, credit card checks, and credit card statements.
- 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. Also, pay attention to your billing cycles. Follow up with creditors if bills do not arrive on their normal billing cycle.

## **Resources**

### **Credit-Reporting Bureaus**

#### **To request a credit report:**

Experian 1-888-397-3742  
Equifax 1-800-685-1111  
Trans Union 1-800-916-8800

#### **To report fraud:**

Experian 1-888-397-3742  
Equifax 1-800-525-6285  
Trans Union 1-800-680-7289

### **Marketing Lists:**

Mail Preference Service  
c/o Direct Marketing Association  
P.O. Box 9008  
Farmingdale, NY 11735

For more information, visit [www.e-mps.org](http://www.e-mps.org)

Telephone Preference Service  
c/o Direct Marketing Association  
P.O. Box 9014  
Farmingdale, NY 1135-9014

For more information, visit [www.the-dma.org](http://www.the-dma.org)

## Federal Government

### Federal Trade Commission (FTC) — [www.ftc.gov](http://www.ftc.gov)

The FTC is the federal clearinghouse for complaints by victims of identity theft. Although the FTC does not have the authority to bring criminal cases, the Commission helps victims of identity theft by providing them with information to help resolve the financial and other problems that can result from identity theft. The FTC also may refer victim complaints to other appropriate government agencies and private organizations for action.

If you've been a victim of identity theft, file a [complaint with the FTC](#) by contacting the FTC's Identity Theft Hotline by telephone: toll-free 1-877-IDTHEFT (438-4338); TDD: 202-326-2502; by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

Ask for a copy of **ID Theft: When Bad Things Happen to Your Good Name**, a free comprehensive consumer guide to help you guard against and recover from identity theft.

### Social Security Administration (SSA) — [www.ssa.gov](http://www.ssa.gov)

SSA may assign you a new SSN - at your request - if you continue to experience problems even after trying to resolve the problems resulting from identity theft. SSA field office employees work closely with victims of identity theft and third parties to collect the evidence needed to assign a new SSN in these cases. Call the Social Security Administration should someone obtain your SSN.

1-800-772-1213

#### *SSA Office of the Inspector General (SSA/OIG)*

The SSA/OIG is one of the federal law enforcement agencies that investigates cases of identity theft. Direct allegations that an SSN has been stolen or misused to the SSA Fraud Hotline. Call: 1-800- 269-0271; fax: 410-597-0118; write: SSA Fraud Hotline, P.O. Box 17768, Baltimore, MD 21235; or e-mail: [oig.hotline@ssa.gov](mailto:oig.hotline@ssa.gov)

SSA publications:

- [SSA Fraud Hotline for Reporting Fraud](#)
- [Social Security When Someone Misuses Your Number](#) (SSA Pub. No. 05-10064)
- [Social Security: Your Number and Card](#) (SSA Pub. No. 05-10002)

## Check Verification Companies

SCAN: 1-800-262-7771

TeleCheck: 1-800-710-9898 or 927-0188

CrossCheck: 1-707-586-0431

Equifax Check Systems: 1-800-437-5120

International Check Services: 1-800-526-5380

United Check Control: 1-800-299-1331