Protect Your Information from Thieves

More than **17.6 million Americans** were victims of identity theft in 2014 alone.[1] Most victims discovered their information had been compromised when their banks contacted them about suspicious activity.[1] Thieves are more sophisticated than ever, often using technology to help them steal information. Other times, they prey on the trusting nature of people to procure personal information.

85% of Americans took steps to prevent identity theft, such as shredding documents, checking their credit reports and changing their passwords.[1]

BEWARE OF ATM SKIMMING

If you use an ATM or other card reader, you may become a victim of identity theft and not realize it until you look at your account statement. Thieves have been using counterfeit card readers in tandem with hidden cameras to steal the information on ATM cards for several years. Once you slide your card into the reader and punch in your PIN, the thief has enough information to make another card. Incidents were up **546%** in 2015, with more than **60%** of incidents occurring at non-bank ATMs.[2] While more financial institutions are incorporating EMV chips into their debit and ATM cards, which make it more difficult to counterfeit a card, not all of them have converted yet. Reduce your risk by avoiding non-bank ATMs and monitoring your accounts for unauthorized activity.

MEDICAL IDENTITY THEFT IS ON THE RISE

More than two million Americans are victims of medical identity theft each year.[3] This type of theft costs the average victim **$22,346**.[3] Thieves steal a person's name and social security number or Medicare number to receive medical care, drugs or to submit false Medicare claims. Unfortunately, a victim may not realize it's happened until they get a bill for a medical service they didn't receive or collection notices for bills they know nothing about.

Prevent Medical Identity Theft

- Be wary of giving out personal information.
- Keep paper copies of your insurance records and forms locked away in a safe place.
- Shred documents you want to throw away.
- Remove or destroy the labels on prescription pill bottles before you dispose of them.

WHAT SHOULD YOU DO IF YOU'RE THE VICTIM OF IDENTITY THEFT?

1. **Report it** to your local police and ask them to issue a police report. Keep a copy of it to share with your creditors.
2. **Document everything**, from phone calls to emails, pertaining to the incident.
3. **Contact the fraud department at one of the major credit bureaus**—Equifax, TransUnion or Experian—to place a fraud alert on your file. One bureau will notify the other two of the flag on your credit.
4. **Review your credit report** and look for unauthorized charges or new credit lines.
5. **Contact your creditors, financial institution, utilities and services** to let them know your identity has been stolen.
6. **Contact the IRS** if you think your identity has been used in connection with tax violations.
7. **Contact the postal service** to see if anyone has submitted change of address forms on your behalf.

Don't Fall Prey to These Scams

Although **85%** of people who reported a scam didn't fall for it, the cumulative losses of victims totaled more than one trillion dollars in 2015. If you suspect you've been contacted by a scam, use the Scam Tracker from the Better Business Bureau to report it.

Source: 1. Bureau of Justice Studies, September 2015
2. USA Today, April 17, 2016
3. ProtectMyID
4. Kroll Investigator Insight, The Top 10 Scams Reported to the BBB

BEWARE OF THESE COMMON SCAMS[4]

- **Tax scams** comprised more than **24%** of reported scams in 2015. Thieves call to say you owe back taxes and will be arrested if you withhold payment. In reality, the IRS won't call you if you owe money and won't threaten you to get it.
- **Debt collection scams** made up **8.3%** of scams reported in 2015. Thieves call to say you have unpaid debt and threaten you with lawsuits or arrest if you don't pay. If you receive such a call, request written evidence of your debt. The law states you can request validation of your debts in writing. True debt collectors won't threaten you or require you pay your debts immediately.
- **Credit card scams** made up **3%** of reported scams in 2015. Thieves contact you claiming to be from your credit card company and offer you a lower interest rate on your credit card, but only if you "verify" a transaction or your card number and security code.
- **Sweepstakes and prize scams** may be one of the oldest tricks in the book, but they comprised **8%** of scams reported in 2015. Thieves contact you to tell you you've won a prize, but you have to pay a fee or cover delivery and processing to claim it. If you have to pay money upfront for your prize, it's not a real prize.
- **Tech support scams** comprised **6%** of reported scams in 2015 and are becoming more common. Thieves contact you claiming to be computer technicians who have detected a virus or security threat to your computer. They'll say they can get rid of it, but they have to access your computer remotely. In reality, they're trying to steal your password and personal information.

Tips to Avoid Being the Victim of a Scam

1. Beware of claims that require immediate action.
2. Beware of offers that require you to wire money or send a pre-paid card.
3. Trust your gut—if you feel something is wrong or an offer sounds too good to be true, it's probably a scam.

Ways to Protect Your Child from Identity Theft

Since children are financial "blank slates," their information is an ideal target for thieves. Unfortunately, parents may not realize their child's identity has been stolen until the child tries to open a bank account or apply for a job.

4 Ways to Protect Your Child from Identity Theft

1. Don't give away their personal information, over the phone or online.
2. Keep their identity documents, such as their birth certificate and social security card, in a safe or locked filing cabinet.
3. Teach your children to protect their personal information.
4. If you suspect your child's identity has been stolen, contact the police and credit bureaus.