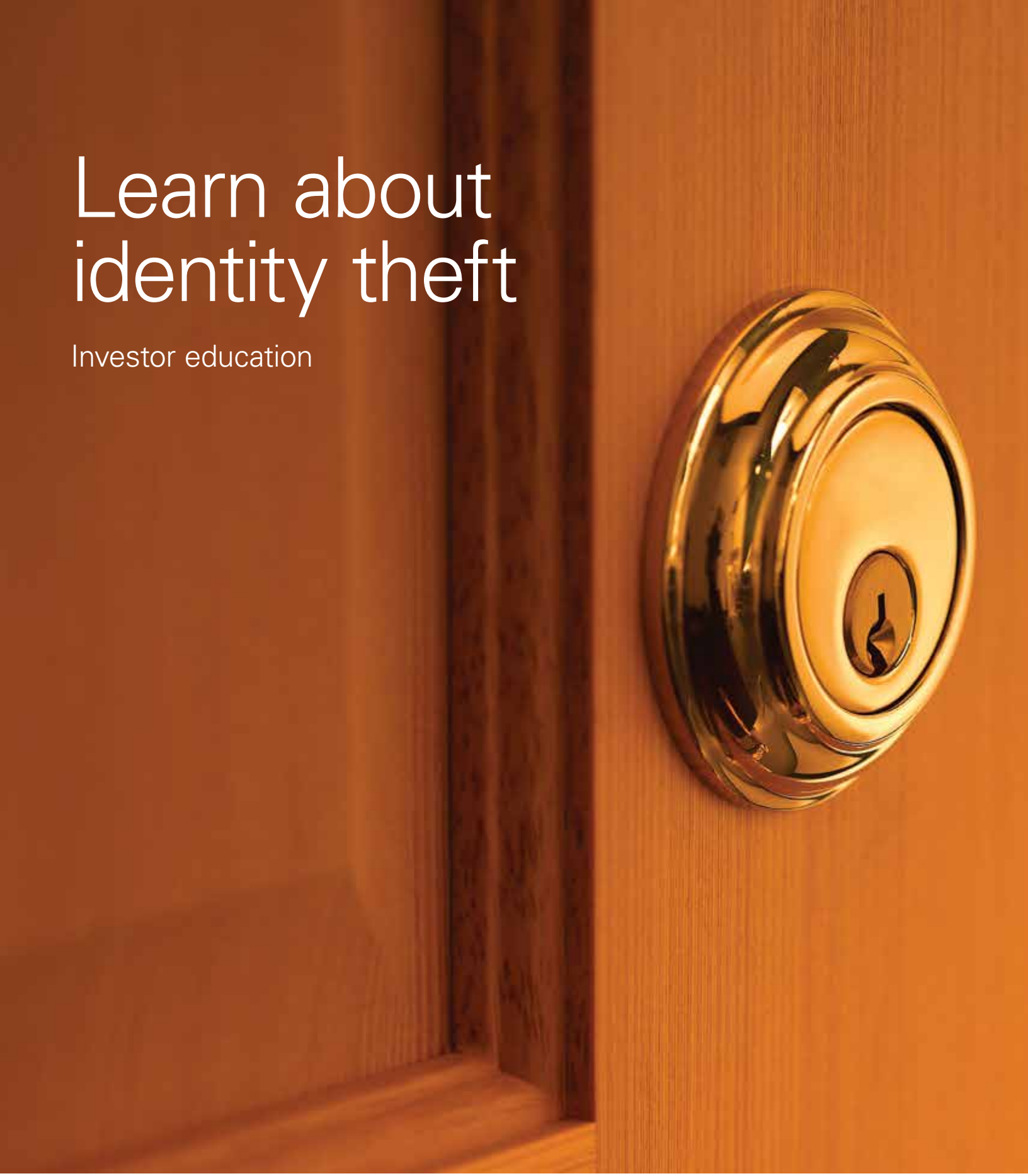
Learn about identity theft

Investor education



Vanguard®

Protecting a vital asset: Your identity

A 2017 report on identity theft by Javelin Strategy & Research found that more than 15 million Americans were the victims of identity theft in 2016. Collectively, thieves made off with about $16 billion.[1]

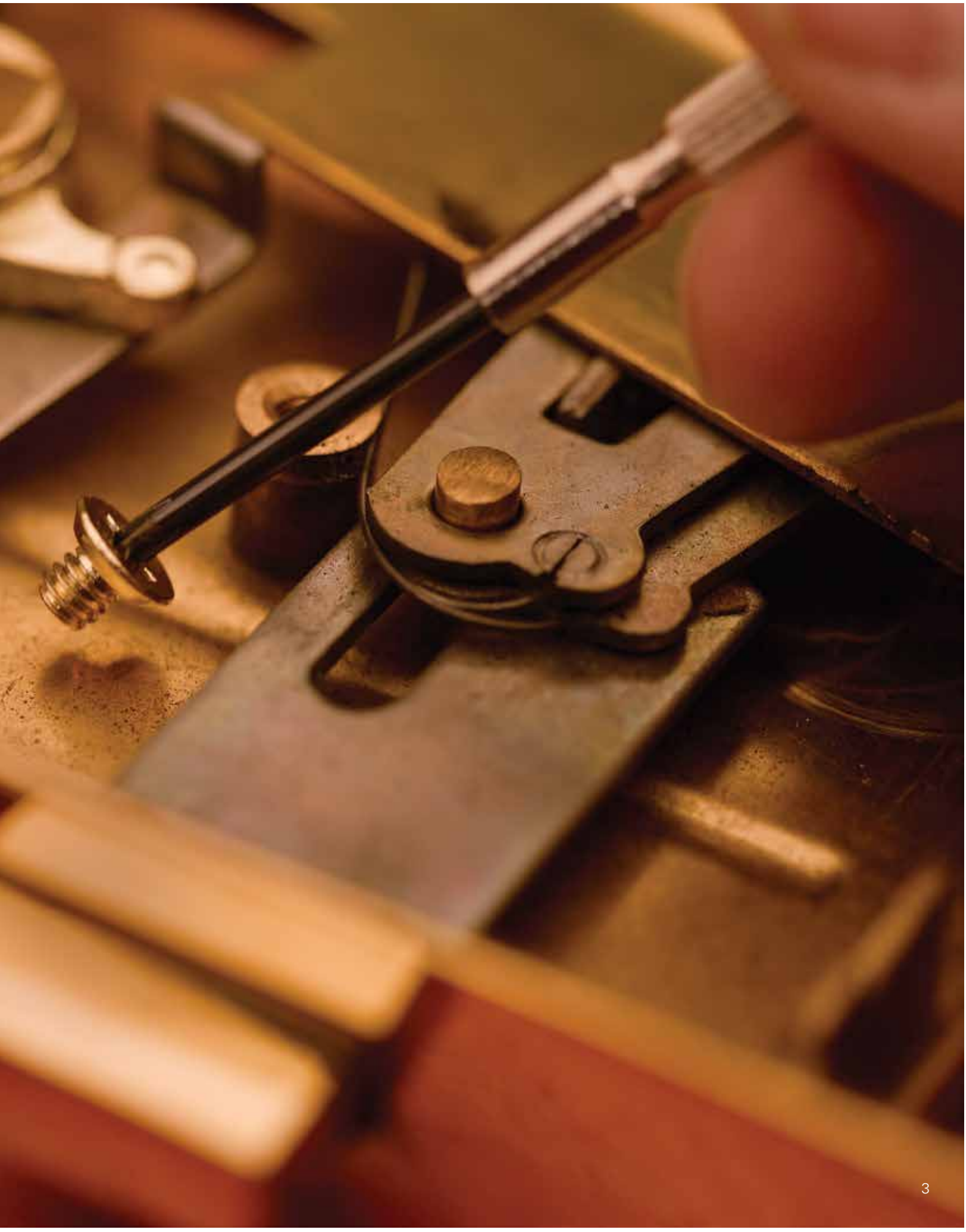
Identity theft happens frequently and takes many forms. This brief guide is designed to help you understand how identity theft occurs, how to avoid it, and what to do if you become a victim.

1 Al Pascual, Kyle Marchini, and Sarah Miller, 2017. *2017 identity fraud: Securing the connected life.* Pleasanton, Calif.: Javelin Strategy & Research.

What is identity theft? 2
Detecting identity theft 7
Minimizing your risk 11
What to do if you're a victim 14

What is identity theft?

It doesn't take much more than your name, your Social Security or credit card number, or even your telephone bill for someone to steal your identity. It's an insidious crime that can compromise your financial security and cost you hours of frustration as you work to repair the damage.



Defining identity theft

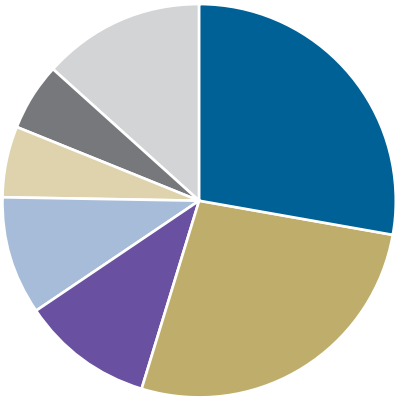
Identity theft occurs when a criminal obtains a key piece of your personal identifying information, such as your driver's license number, your bank account number, or your Social Security number, and uses it to commit fraud.

Often, people don't realize they are the victims of identity theft until it's too late to recover their losses or catch the thief. In fact, the longer identity theft goes undetected, the more damaging the effects can be.

Focusing on the intangible

Identity thieves don't focus on property such as cars, jewelry, cash, or art. They concentrate on intangible financial assets, notably bank and credit card accounts. The most common form of identity theft is the misuse of employment- or tax-related information.

The primary forms of identity theft



- 34% Employment- or tax-related
- 33% Credit cards
- 13% Phone/utilities
- 12% Bank accounts
- 7% Government documents/benefits
- 7% Loans/leases
- 16% Other

Does not equal 100% because 25% of identity-theft complaints in 2016 involved more than one category.

Source: Federal Trade Commission, 2017. *Consumer sentinel network data book for January–December 2016*. Washington, D.C.: Federal Trade Commission.

How your identity is stolen

Identity thieves can get your information in a variety of ways—some of which are surprisingly simple. For instance, in public places, a thief can easily write down your credit card number when you give it to a merchant over the telephone.

These criminals frequently resort to old-fashioned forms of theft—stealing wallets, purses, mail, preapproved credit card offers, bank statements, and other documents that contain personal information—to gain access to your identity.

"Dumpster diving" is a common tactic in which thieves rummage through your trash looking for bills, credit card or bank statements, and other records that contain your name, address, telephone number, or other personal information that help them get control of your identity.

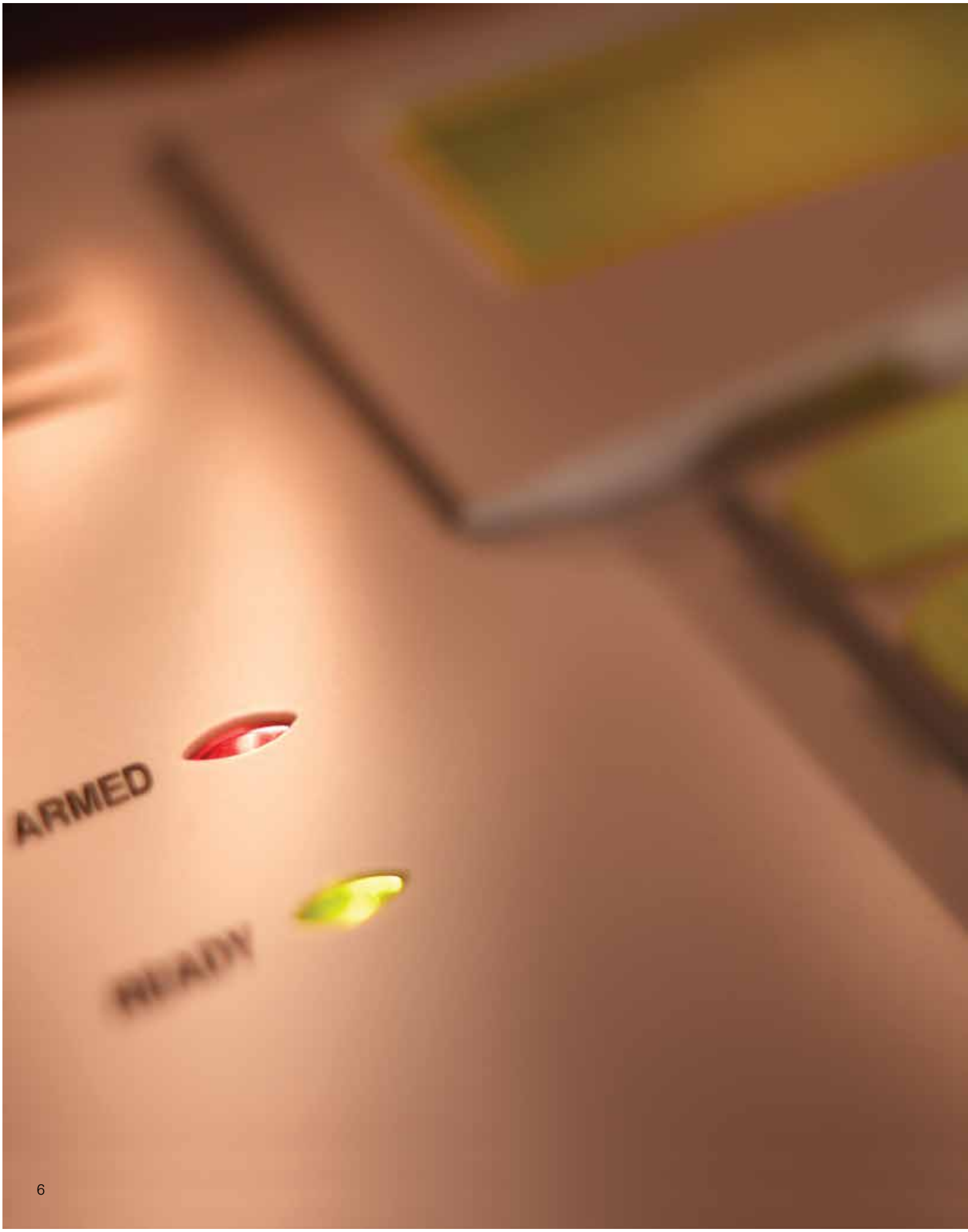
The internet offers many opportunities for criminals to obtain information about you. Phishing—which involves a thief's posing as a legitimate financial institution or company and sending spam or pop-up messages to get you to share your personal information—is particularly popular.

Thieves have lots of ways to use your identity

Identity thieves have countless ways to use your personal information. Some of the most common include:

- Government benefits fraud.
- Credit card fraud.
- Telephone or utilities fraud.
- Bank or investment fraud.

In addition, identity thieves can use your Social Security number or other personal information to get a job, obtain medical services, or even pose as you in the event they are arrested.


ARMED

Detecting identity theft

Too often, people learn their identity has been stolen after the damage has been done. A good defense against becoming a victim is recognizing the warning signs of identity theft.

Common ways to detect identity theft

Sorting out the effects of identity theft can be messy and time-consuming. Here are some ways to tell if a thief may have stolen your identity.

Unauthorized charges appear on your credit card statements. Never take your monthly credit card bill for granted. Compare each purchase you've made with the charges on your statement.

Unusual deposits or withdrawals have been made to your bank account. Just as you do with your credit card statements, always examine your bank statements for irregularities. Also, notify your bank immediately if you don't receive your statement on time. A late or missing bank statement may signal that a thief has stolen your account information and redirected the mail from your bank. Another option is to have your statements delivered to you electronically.

Inaccurate information appears on your credit reports. Your credit reports provide a history of your credit activity. In addition, they contain information about where you've lived; where you've worked; and whether you've ever been arrested, been sued, or filed for bankruptcy. It's smart to review your credit reports once a year for indications that your identity has been tampered with.

You are denied credit. Being denied credit or being offered unfavorable credit terms for no apparent reason are warning signs that someone may have stolen your identity.

How to obtain copies of your credit reports

As previously mentioned, reviewing your credit reports is a valuable way to monitor the security of your personal information. The information that appears in the reports is collected by three major consumer credit reporting companies—Equifax, Experian, and TransUnion.

The Fair Credit Reporting Act, as amended by the Fair and Accurate Credit Transactions Act of 2003, requires each of these companies to provide you with a free copy of your credit report, at your request, once a year. Here's how you can order a report from any or all of these companies.

Online: annualcreditreport.com
By phone: 877-322-8228
By mail:
Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281

Minimizing your risk

There are no guarantees you won't become a victim of identity theft. However, you can take a number of practical steps to protect your personal information.

Help ensure your security

When it comes to preventing identity theft, the best defence is a good offence. Make it tough for criminals to get your personal information by taking the steps outlined here. In addition, as mentioned earlier, make it a point to check your credit reports at least once a year for irregularities.

Protect your Social Security number

Social Security numbers are a prime target of identity thieves. Provide your Social Security number only when absolutely necessary. Except for your employer and your financial institutions, which need your Social Security number for wage and tax purposes, question businesses that request the number. Keep these other precautions in mind, as well.

- Do not carry your Social Security card in your wallet, unless you must physically present it, for example, when starting a job.
- Avoid saying your Social Security number out loud when strangers are within earshot.
- Do not have your Social Security number printed on checks. And don't allow merchants to write your Social Security number on checks either.
- Each year you should go to ssa.gov (log on to, or create, your "my Social Security" account) and review your Social Security Statement for signs of fraud.

- While the Real ID Act of 2005 prohibits states from displaying Social Security numbers on drivers' licenses and state ID cards, some individuals, particularly in Arizona, may still have drivers' licenses that use their Social Security numbers. If you hold such a license, request that your Department of Motor Vehicles replace it with one that uses a different ID number.

Protect your credit, debit, and ATM cards

One of the most practical ways to defend yourself against credit and debit card fraud is simply to reduce the number of cards you own. But regardless of how many cards you carry, consider these practical tips for protecting yourself.

- Never write credit card numbers on checks. Or consider paying credit card bills online instead of by mail.
- Always take credit card receipts with you, and destroy them when they are no longer needed. Never throw them in the trash without shredding them.
- Keep a list of or photocopy your credit and debit cards, including their expiration dates and the telephone numbers of the customer-service departments, for use in the event that your cards are lost or stolen.
- Memorize your credit card, debit card, and ATM personal identification numbers (PINs). Never carry a record of your PINs with you.
- Avoid using debit cards when shopping online. Credit cards provide more effective fraud protection.
- Create intricate passwords for your credit and debit card account access. Steer clear of information such as your mother's maiden name, your birthday, and your pet's name. Combinations of numbers and letters—the more random the better—make the safest passwords.
- Purchase a shredder, and destroy unneeded credit card offers, receipts, bank statements, credit card bills, and other documents that contain personal information that a thief could use to steal your identity.

Protect your computer

The internet offers opportunities that would have been unimaginable a generation ago. You can buy movie tickets, make dinner reservations, invest in the stock market, converse with your doctor, pay your taxes, or even buy a car online. The possibilities seem limitless. Unfortunately, so are the opportunities for scammers, hackers, and identity thieves to steal your personal information. Here are some tips to help make your computer safer.

- Install antivirus and antispyware software—making sure to update it regularly—and a firewall.

- Protect your passwords. Never share them. Change them regularly (at least every three months). Never use the same password for different accounts.
- Never respond to emails that ask you to confirm your account information, provide your Social Security number, or provide other personal information.
- Back up important files by copying them onto a disc, a flash drive, or some other portable storage medium, keeping it in a safe place. As well, you could consider backing up your data to an off-site server in the cloud.
- Avoid file-sharing programs, which can expose your computer to unwanted access by others.

Reduce the amount of personal information you make available

These days, we're bombarded with opportunities to share our personal information. Here are a few steps you can take to control the amount of information you make available.

- Remove your name from the marketing lists of Equifax, Experian, Innovis, and TransUnion by calling 888-5-OPT-OUT (888-567-8688) or going to optoutprescreen.com. Removing your name from their lists will limit the number of credit card and insurance offers you receive.
- Contact the Direct Marketing Association's DMAchoice mail preference service at dmachoice.org to have your name removed from lists that marketers use.
- Sign up for the National Do Not Call Registry at donotcall.gov.
- Be wary of how much personal information you share on social networking sites, such as Facebook, Twitter, LinkedIn, and YouTube.

Getting professional help

You may also want to explore using an identity-theft protection service. These companies typically monitor your accounts and credit reports and alert you to activity that could be identity theft. They will also assist you in resolving problems should a theft occur.

What to do if you're a victim

Regardless of how carefully you protect your identity, you may still become a victim. Fortunately, there are ways to recover from identity theft.

Act fast

If you suspect that your identity has been stolen, you should act immediately. The faster you respond, the more likely you'll be able to minimize the damage. Here are four steps to take.

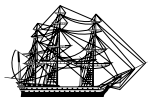
- Close compromised accounts. Contact the bank, creditor, or financial institution associated with any account that has been tampered with. Experts advise that in addition to calling, you should notify your bank, credit card company, or financial institution of the situation in writing and ask for a letter acknowledging that the company has closed the disputed account and cleared any fraudulent charges.
- Place fraud alerts on your credit reports. Contact Equifax (800-525-6285), Experian (888-397-3742), or TransUnion (800-680-7289) and explain that you have been a victim of identity theft. You need to contact only one of the three companies. Whichever company you call will notify the others that you have requested the fraud alert.

  The fraud alert will result in your credit reports being flagged, so potential creditors will need to call you to verify your identity before extending credit.

Once you receive a copy of your credit report, examine it carefully. Report fraudulent activity in writing to the credit bureaus and the credit issuers. In addition, read all the instructions on the report carefully to ensure that you are taking every step you can to correct inaccurate information and protect your identity in the future.

- Call the Federal Trade Commission's (FTC) toll-free identity-theft helpline at 877-ID-THEFT (877-438-4338), or visit the FTC's identity-theft website, identitytheft.gov, to file a fraud complaint. While the FTC does not investigate individual identity-theft cases, the commission shares data with investigators around the country and abroad who pursue identity thieves.
- File an identity-theft report with your local or state police department. Include a copy of the FTC's Identity Theft Report and other documentation you may have.

You might not be able to completely eliminate the threat of identity theft, but one of the best ways to avoid becoming a victim is to be vigilant. Make it a point to carefully protect your personal information. And if you suspect fraudulent activity, act quickly to protect yourself.



Vanguard Financial
Advisor Services™

P.O. Box 2900
Valley Forge, PA 19482-2900

Please note: The organizations and websites listed in the guide are for informational purposes only and do not imply endorsement by Vanguard.

Financial advisors: Visit advisors.vanguard.com or call 800-997-2798.

Investment Products: Not FDIC Insured • No Bank Guarantee • May Lose Value

FAEDID 012018