Better Money Habits®

How to help protect yourself: Understanding fraud and scams

BANK OF AMERICA

What you'll learn

1 Understanding fraud

2 Common scams and their red flags

3 Identity theft

Understanding fraud

What is fraud?

Fraud is an intentional act, misrepresentation or omission of material fact designed to deceive for improper gain or other benefit regardless of whether financial loss occurs. Why would someone want to commit a fraudulent act?

Motivation

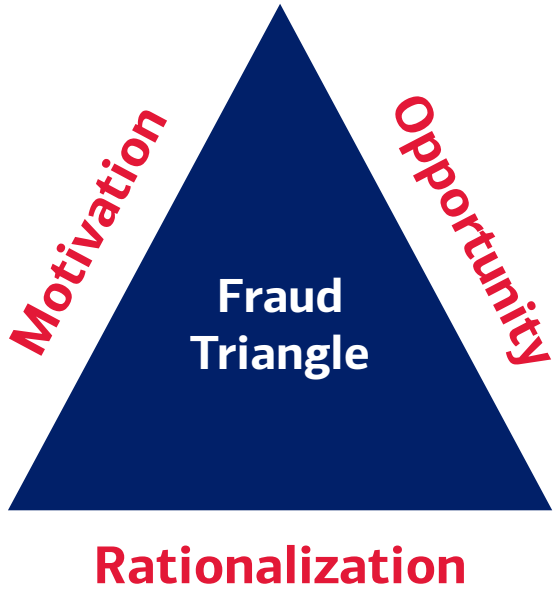
- Financial pressure, such as credit card or medical debt
- Greed or desire to live beyond means
- Professional criminals or companies like scam rings that exist for the sole purpose of stealing money

Opportunity

- Easy targets
- Potentially vulnerable control environment
- Access to information

Rationalization

- “The money won’t be missed.”
- “I deserve or need this money.”
- “It’s my job to steal your money.”

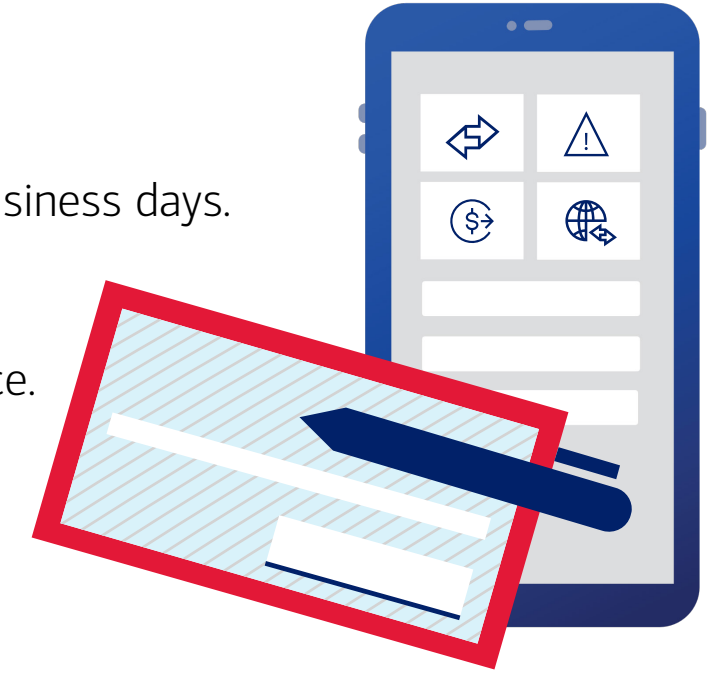


Source: Association of Certified Fraud Examiners

Check fraud

Paper checks contain personal information that can be seen by whoever gets their hands on them. Fraudsters often target the mail to steal checks and other personal or financial information in order to commit fraud and identity theft. Here are some things you can do to help protect yourself:

- Pay bills or send money using secure digital payment methods.
- Turn on transaction alerts.
- Shred paper checks based on the applicable banking agreement, typically after ten business days.
- Set up direct deposit or deposit checks using a Mobile Banking app.
- Send checks through certified mail, a secured mailbox or directly within the post office.
- Review your deposit account activity and bank statements as soon as possible.
- Report any unauthorized transactions as outlined in your deposit agreement.
- Store your checkbooks in a safe place.



While these efforts may not completely eliminate fraud, they can help prevent it.

Mobile Banking requires that you download the Mobile Banking app and may not be available for select mobile devices. Message and data rates may apply. Moving from checks to digital payments does not guarantee you're protected from all fraud and scams. Please see bofa.com/security for information on other steps you can take to help further protect your accounts.

How banks may help protect you from fraud

Banks work hard to keep your accounts and information secure. Some of the ways they may help protect you is by:

- Helping to keep your personal and financial information protected and secure through responsible information collection and processing.
- Helping to protect against threats via cybersecurity teams.
- Monitoring for suspicious account activity and alerting you to potential fraud through the mobile app, text alerts, email or phone.

Always report fraud or suspicious activity on any of your accounts to your bank.

Mobile Banking requires that you download the Mobile Banking app and may not be available for select mobile devices. Message and data rates may apply. Moving from checks to digital payments does not guarantee you're protected from all fraud and scams. Please see bofa.com/security for information on other steps you can take to help further protect your accounts.

How to help protect yourself: Basic rules to follow

- In your mobile banking app, keep your contact information up to date, allow push alerts and set up two-factor authentication or fingerprint/facial recognition sign-on.
- Keep spare keys, credit cards, Social Security card, birth certificate and other sensitive papers in a safe place.
- Stop your mail or put a hold on it if you're away.
- Use secure digital payment methods instead of sending checks.
- Drop mail off at the post office or mailbox.
- Use computer safeguards such as pop-up blockers, anti-spyware and anti-virus programs.
- Shred paper checks based on the applicable banking agreement, typically after ten business days.

While these efforts may not completely eliminate fraud, they can help prevent it.

Mobile Banking requires that you download the Mobile Banking app and may not be available for select mobile devices. Message and data rates may apply. Moving from checks to digital payments does not guarantee you're protected from all fraud and scams. Please see bofa.com/security for information on other steps you can take to help further protect your accounts.

How to help protect yourself: Mobile security tips

Use strong passcodes

Strong passcode

ILv4Btng!

Start with a memorable sentence like “I live for boating!” and transform it.

VS

Weak passcode

password1234

Avoid using passcodes that can be easily guessed or are based on personal information.

How to help protect yourself: Mobile security tips (continued)

- Don’t use a code with personal details to unlock your phone.
- Secure your smartphone by setting it to lock automatically.
- Don’t keep sensitive information on your phone.
- Download apps only from authorized stores.
- Limit what you share on social media.
- Keep technology up to date.

How to help protect yourself: Online safety

- Use strong passwords.
- Limit the personal information you share online.
- Lock your phone when you're not using it and require a unique PIN or passcode to unlock it.
- Don't keep sensitive information on your phone.
- Keep technology and anti-virus software up to date.
- Avoid connecting to unsecured public Wi-Fi hotspots.

What to do if it happens to you: Fraud

- Contact creditors, financial institutions and speak to the fraud department.
- Consider changing your logins and passwords.
- Check your credit report.
- Consider putting a fraud alert and credit freeze on file with the credit reporting agencies:
  - Experian: Experian.com or 888.397.3742
  - TransUnion: Transunion.com or 800.680.7289
  - Equifax: Equifax.com or 888.766.0008
- You may also choose to file a report with your local law enforcement.

Key takeaways

1

Fraud is the intentional act of deceit, based on motivation, opportunity and rationalization.

2

Banks typically monitor activity to help protect you.

3

You can protect yourself from fraud by following basic rules.

4

Mobile and online safety is key to helping to protect your personal information from fraud.

Common scams and their red flags

What is a scam?

A scam is a deceptive trick used to obtain something valuable from you, including money or personal information. Scammers are master manipulators who use persuasive emotional tactics to target their victims in a variety of ways.

- Scammers play on emotions.
- Scammers may pose as people, like friends or family members, government employees and companies.
- Scams can occur over the phone, through the mail, over the internet or in person.

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Trending scams

- Social engineering scams
- Suspicious online retailers
- Bogus tech support
- Online romance scams
- Investment scams
- Threat of harm
- Payment scams

Look up current scams

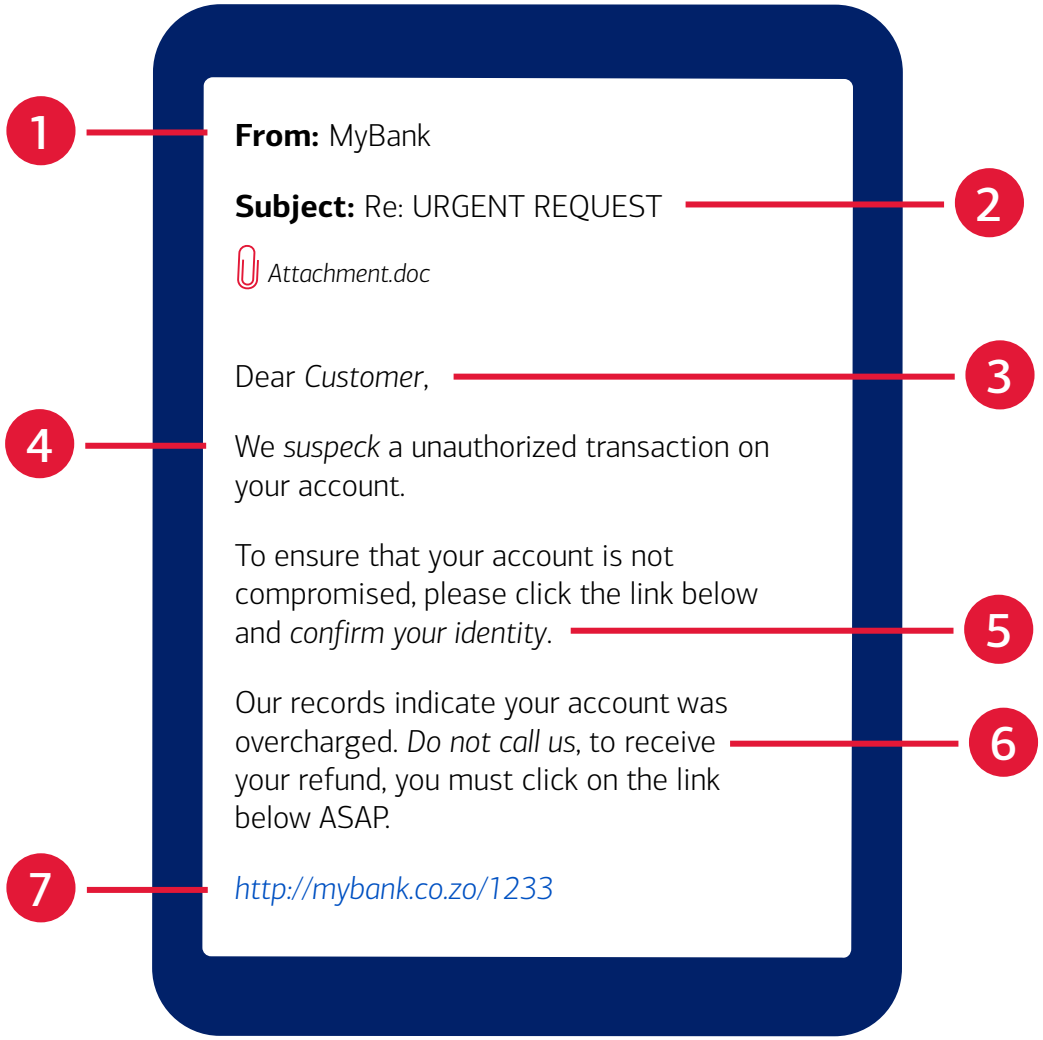
Visit bankofamerica.com/helpprotectyourself

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Types of scams: Social engineering scams

Scammers use social engineering tactics, such as phishing, to try to get your personal and financial information. A phishing email, text or phone call scam may include some of these components:

1. Sent from an odd or unfamiliar source
2. Demands urgent or immediate action
3. Doesn't use your name
4. Has misspelled words in the body copy
5. Asks you to verify your information
6. Tells you not to call
7. Includes strange URLs or links



HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Types of scams: Online retailers

Imposters set up a fake store online (or on social media) that offers products at a cheaper-than-usual price or items you might urgently need. What to look for:

- Look closely at the domain name — is it spelled correctly?
- Check the domain on the Better Business Bureau (bbb.org).
- Search for reviews or warnings about potential scams.
- Check the quality of the website design — poor visuals, no phone numbers or addresses are red flags.

If it looks too good to be true, it probably is. Trust your instincts.

Types of scams: Tech support

Tech support scammers want you to believe you have a serious problem with your computer, like a virus. They want you to pay for tech support services to fix a problem that doesn't actually exist. Here are some tech support tactics to look out for:

Unsolicited telephone calls from an imposter impersonating computer, bank, utility companies and other familiar companies (in addition to government)

Online ad leading to a fraudulent website

Pop-up messages that claim a virus has been found on your computer and ask you to call a phone number to an imposter or click on a fraudulent link or download an app

Types of scams: Online romance scams

Scammers use online dating apps or social networking sites to strike up conversations with unsuspecting, potential targets. After earning your trust, they'll need funds for a plane ticket, investment opportunity or other expenses, or even to help them out because they are in "trouble". They may ask you to wire money or buy a gift card to help pay for it.

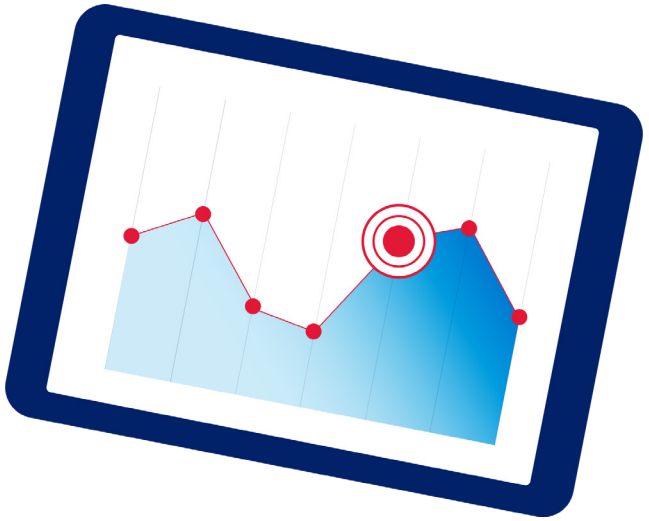
- Be cautious about sharing too much personal information on online dating sites or social media.
- It's never a good idea to send money, credit or gift card numbers to someone you've never met in person.
- Be wary of a stranger on social media sharing irresistible pictures and professing their love for you — they're most likely setting you up!

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Types of scams: Investment

An investment scammer deceives others into investing money in a fake or non-existent investment opportunity, often promising high returns with little or no risk. Sometimes you'll even receive small returns at first to build your confidence and prompt you to "invest" larger amounts. Signs of an investment scam:

1. The scammer contacts you with a unique investment opportunity.
2. The scammer convinces you to invest your money.
3. You invest large sums of money.
4. You never hear from the scammer again.



HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Types of scams: Threat of harm

Scammers may contact you by phone, email or text to threaten blackmail or bodily injury if financial or other terms aren't met. Threats may include arrest, deportation or bodily harm to you or loved ones.

Initial contact: Scammers reach out claiming to have access to you or someone in your family.

Deceptive instructions: They claim that you or your family are in danger. You're told if you don't send money, you or your family member will be hurt.

Impersonation: Scammers may use technology to impersonate your loved one's voice to manipulate you and convince you to transfer funds.

Call 911 if you feel you or someone you love is in immediate, physical danger.

Help protect yourself and your money. Consider using a "safe word" that only you and your family members know. Learn more at bankofamerica.com/helpprotectyourself

Types of scams: Payment

When using payment apps, you should only send money to someone you know and trust to help avoid being scammed. The payments are like cash and if you send money to a scammer it's unlikely to be recovered. Don't process a payment if you're:

- Pressured to act fast and urged to stay on the phone while given instructions.
- Asked to send money to help protect yourself from fraud.
- Asked to make last minute changes to the payment instructions.
- Told to ignore warning messages.
- Asked by a "bank" via phone call or text to provide a security code.

Common targets of scams

While anyone can be targeted by scammers, there are particular groups who are more at risk.

- **Older adults:** This vulnerable group may have less experience with technology, are more trusting and likely to have savings.
- **Youth and young adults:** This group may have less experience managing money.
- **Students:** Both high school and college students are more digitally active and may fall victim to scams.

If you or someone you know has been victimized, report it immediately to:

- Local law enforcement
- The FBI's Internet Crime Complaint Center

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

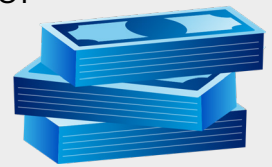
Common targets of scams: Older adults

Scams commonly affecting individuals over the age of 60 include:

- **Romance scam:** Criminals pose as interested romantic partners through dating websites to capitalize on their victims' desires to find companions.
- **Cash withdrawal scam:** Scammers impersonate the bank, telling the client there's fraud on their account and they need to protect their money. They instruct them to load their "new" card to their Digital Wallet, go to a financial center, withdraw cash and deposit it at an ATM into their "new" account.
- **Investment scam:** Investment fraud involves financial crimes often characterized as low-risk investments with guaranteed returns.
- **Tech support scam:** Criminals pose as tech support representatives and offer to fix nonexistent computer issues, gaining remote access to victims' devices and, thus, their sensitive information.
- **Artificial intelligence (AI) scam:** Scammers may use AI to impersonate a loved one or someone you know, claiming they are in danger and need money immediately.

Scams targeting people over 60 recently accounted for

$28.3 billion in annual losses.



Of that, $20.5 billion is stolen each year but likely never reported to authorities.

Source: AARP

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Common targets of scams: Youth and young adults

Here's how youth and young adults may be victimized:

1

Most scams start with an attention grabber: Youth and young adults are targeted with offers that appeal to their demographics through gaming, social media or other means.

2

They look familiar: Scammers may create fake websites or social media accounts that look familiar — impersonating celebrities, for example — to trick youth and young adults into engaging with them.

3

There may be a sense of urgency: Youth and young adults are quick to click, and scammers take advantage by pressing for immediate action.

4

A "friend" may request information or money: Fake offers and links may lure unsuspecting victims into providing passwords or payment information.

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Common targets of scams: Students

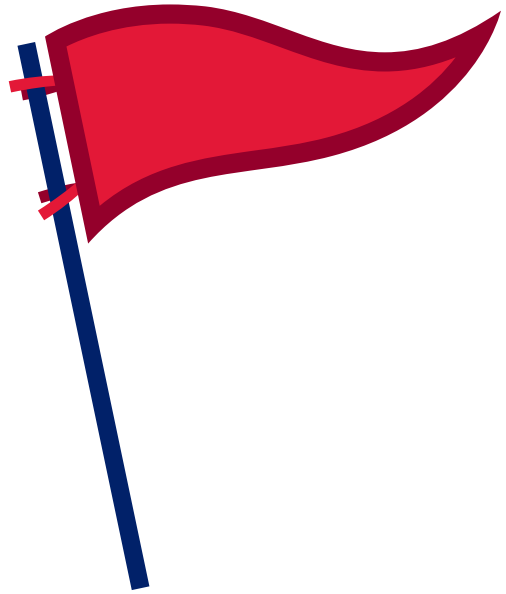
- Fake apartment listings
- Bogus scholarships, grants and debt relief
- Unpaid tuition claims
- Counterfeit check cashing
- Promise of employment for a fee
- Sweepstakes and giveaways

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Recap: Know the red flags

Scammers are constantly inventing new ways to trick people while playing on emotions. Their stories may change, but their tactics remain the same. Being aware of these red flags should make you pause, verify and help prevent scams:

- You're contacted out of the blue.
- You're pressured or threatened to act immediately.
- You're asked to help or trust someone in trouble.
- You're asked to pay in an unusual way.
- You're asked to provide personal or account information.
- You're asked to click on a link.
- It seems too good to be true.
- You're presented with a reward opportunity.
- You're told a story that plays on your emotions.



HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

How to help protect yourself

Scammers have two main goals — to steal your money and your identity. Maintaining cybersecurity is very important. Here are some steps you can take:

- Don't open any emails from people you don't know.
- Be careful with links and new website addresses that appear accurate, but have slight variations in spelling or logo.
- Secure your personal information.
- Stay informed on the latest cyber threats by researching scams online.
- Use strong passwords.
- Keep your software up to date and maintain preventative software programs.
- Update the operating systems on your electronic devices.

What to do if it happens to you: Scam victim

If you're a victim of scam, you're not alone, and there are steps you can take to recover:

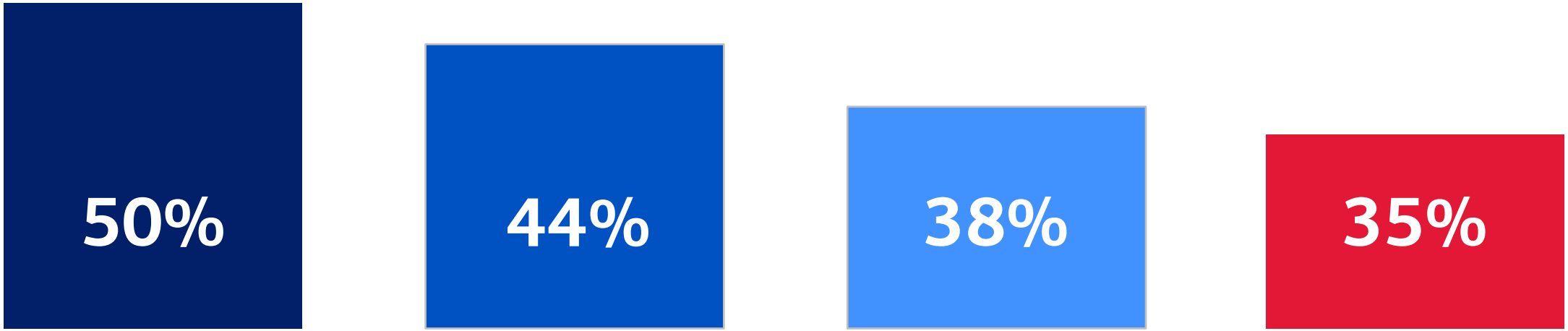
1. Contact your financial institutions and creditors and tell them you've been scammed and your identity may have been compromised.
2. Change your account passwords with financial institutions, social media platforms, medical portals or other very sensitive sites.
3. Check your computer to make sure your anti-virus software is running.
4. Contact the credit bureaus.
5. You may choose to also file a report with your local law enforcement.
6. Helpful resources:
   - AARP: aarp.org/money/scams-fraud/
   - Federal Trade Commission: ftc.gov/exploredata
   - Better Business Bureau: bbb.org/scamstracker/lookupscam

Regularly review the Security Center for trending scams.

What scam victims may experience

It’s more than money lost…

Nearly **2 in 3** victims experience 1or more **serious nonfinancial costs** of fraud



“It’s all my fault! I feel so all alone; no one understands what I’m going through.”
“How did this happen to me? I feel like I’ve lost everything.”

Source: FINRA Investor Education Foundation, “The Non-Traditional Costs of Financial Fraud.”

HELP PROTECT YOUR MONEY
PAUSE. VERIFY. HELP PREVENT SCAMS.

Key takeaways

1

Scammers use a wide range of tactics to trick and target people.

2

You can avoid being scammed by recognizing red flags.

3

Learning what to do if you've been scammed can help you react quickly to minimize financial and emotional harm.

Identity theft

Identity theft: How it happens

Both fraud and identity theft are acts of deception, often for financial gain — and they're both illegal, but identity theft is next-level deception. It may take a long time to straighten out depending on the duration and damage done to your personal and financial situation, so it's important to stay vigilant. Identity thieves steal in a variety of ways, such as:

- Phishing through email by adding hyperlinks or attachments
- Stealing your mail out of your mailbox
- Using a data collection device
- Theft by family/friends/acquaintances
- Business record theft
- Fraudulent calls or mail
- Going through garbage

Identity theft: Types of information stolen

An identity thief tries to collect as much information about you as possible, such as:

- Name
- Address
- Phone number(s)
- Social Security number
- Driver's license
- Credit cards, including expiration dates and security codes
- Bank account information
- Employee ID
- Digital signature
- Mother's maiden name
- Passports or green cards
- Health insurance card

Identity theft: The results

Once an identity thief has access to your personal information, they can use it to:

- Open new accounts
- Apply for loans
- Rent apartments or even buy a house
- Apply for unemployment benefits
- Gain medical attention
- Steal your tax refund

You may not know you've experienced identity theft immediately, but look for warning signs:

- Getting bills for items you didn't buy
- Receiving collection calls
- Finding misinformation on your credit reports
- Getting denied for a loan application
- Missing mail or lack of mail
- Plummeting credit score

How to help protect yourself: Identity theft

1. Don’t share private information online.
2. Check your credit report.
3. Watch your mailbox for missing mail.
4. Shred your personal papers.
5. Be wary of strangers.

What to do if it happens to you: Identity theft

- Contact creditors, financial institutions and speak to the fraud department.
- Consider changing your logins and passwords.
- Check your credit report.
- Put a fraud alert and credit freeze on file with the credit reporting agencies:
  - Experian: Experian.com or 888.397.3742
  - TransUnion: Transunion.com or 800.680.7289
  - Equifax: Equifax.com or 888.766.0008
- Contact law enforcement and tell them your identity may have been compromised.

What to do if it happens to you: Freezing your credit

A credit freeze locks your credit report until you approve its release — making it harder for identity thieves to open new credit accounts in your name.

Advantages

- No cost to you
- Won't affect your credit score
- Won't prevent you from obtaining your free annual credit report
- Won't impact your current credit accounts

Things to keep in mind

- No guarantee it stops credit or identity fraud
- You'll need to keep track of your PINs to unlock your credit when you need to
- Existing accounts aren't protected

What to do if it happens to you: How to freeze and unfreeze

To freeze your credit: Contact all three major credit reporting agencies to complete your request. Throughout the process, you'll need to verify your identity by entering your Social Security number, answering some questions and providing further supporting documentation.

- Experian: Experian.com or **888.397-3742**
- TransUnion: Transunion.com or **888.909-8872**
- Equifax: Equifax.com or **888.298-0045**

To unfreeze your credit: To apply for credit again, you'll need to lift the freeze in one of two ways. Credit bureaus can provide a PIN or do a general lift of the freeze, and both will allow a creditor to review your credit file. Not all creditors can use the PIN, so be aware of both methods and ask which method will be required prior to applying.

What to do if it happens to you: Locking your credit

Locking your credit through the three main credit bureaus helps prevent unauthorized access to your credit reports and may be easier and faster than a credit freeze.

- It's a great way to prevent identity theft since lenders can't check your reports
- You can lock and unlock your reports yourself at any time, making it faster than a freeze
- All three credit bureaus offer credit locks but you must enroll, some at a fee

Direct links and numbers for locking.

- **Experian**
  Experian.com or **888.397.3742**
- **TransUnion**
  Transunion.com or **800.680.7289**
- **Equifax**
  Equifax.com or **888.766.0008**

Key takeaways

1

Identity thieves will go to great measures to steal your information.

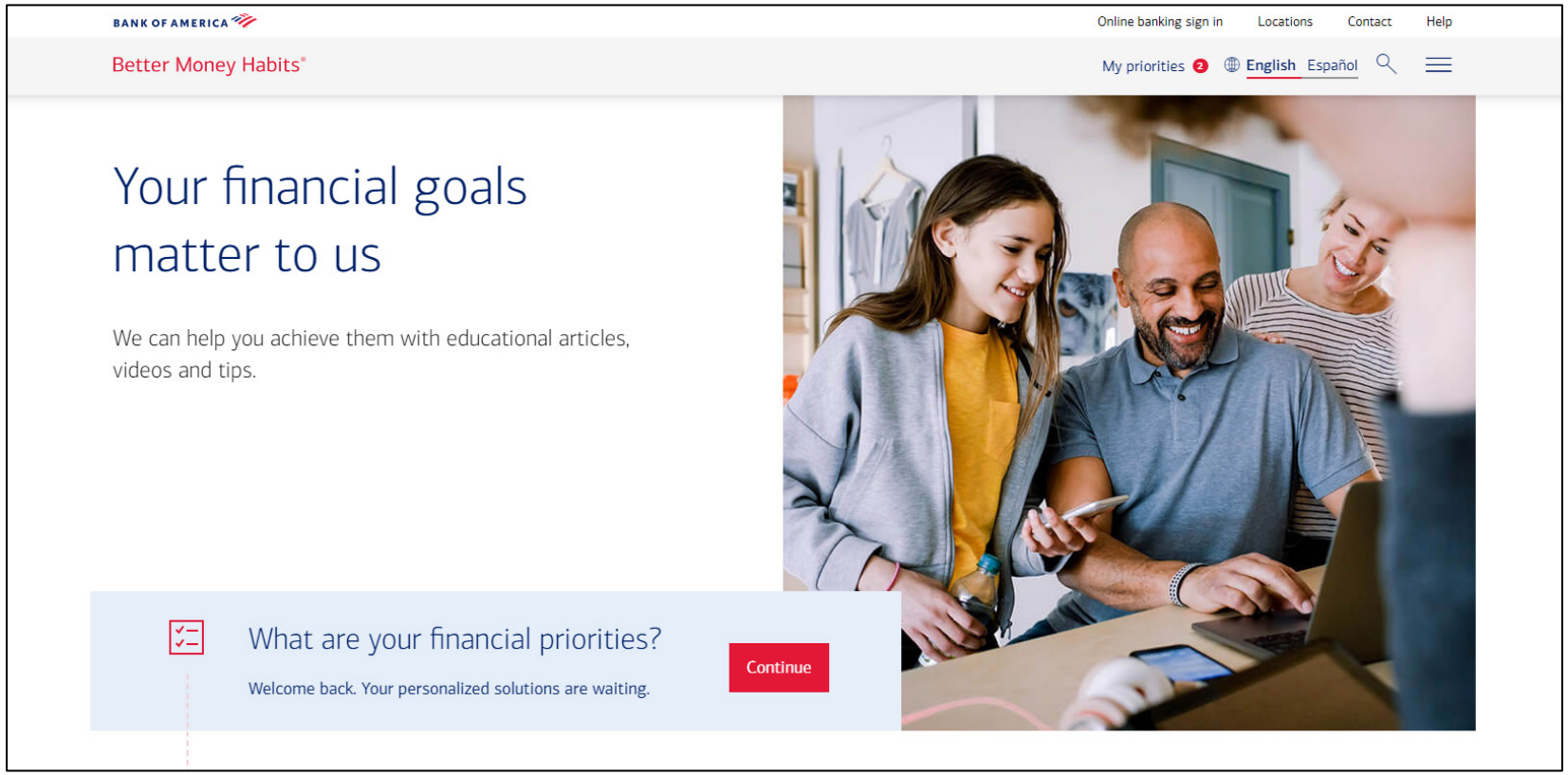
2

The more information an identity thief has, the more damage can be done.

3

Look for warning signs and act as quickly as possible.

Conclusion



BetterMoneyHabits.com

Thank you

PRES-10-24-0161.A