

Acting out fraud and identity theft

Students develop and act out skits depicting possible fraud and identity theft and ask classmates to guess which type of crime is occurring.

Learning goals

Big idea

Fraud and identity theft hurt millions of Americans every year.

Essential questions

- What are the most common types of fraud and identity theft?
- How do fraud and identity theft pose a financial risk to me?

Objectives


- Review the characteristics of common fraud and identity crimes
- Identify the types of fraud and identity theft described in a real-world scenario

NOTE

Please remember to consider your students' accommodations and special needs to ensure that all students are able to participate in a meaningful way.

KEY INFORMATION

Building block:

 Financial knowledge and decision-making skills

Grade level: High school (9-12)

Age range: 13-19

Topic: Protect (Managing risk, Preventing fraud and identity theft)

School subject: CTE (Career and technical education), English or language arts, Fine arts and performing arts, Social studies or history

Teaching strategy: Cooperative learning, Simulation

Bloom's Taxonomy level: Understand, Create

Activity duration: 75-90 minutes

National Standards for Personal Financial Education, 2021

Managing credit: 12-12, 12-13

Managing risk: 8-7, 12-11

Spending: 12-2, 12-8, 12-9

These standards are cumulative, and topics are not repeated in each grade level. This activity may include information students need to understand before exploring this topic in more detail.

What students will do

- Read a scenario describing a type of fraud or identity theft.
- Work in groups to create a skit that brings that scenario to life.
- Act out the skit for the class.
- Guess which type of fraud or identity theft is being portrayed in each skit.

Preparing for this activity

- While it's not necessary, completing the "[Defining fraud and identity theft](#)" activity first may make this one more meaningful.
- Print copies of all student materials for each student, or prepare for students to access them electronically.
- Print a single-sided copy of the fraud and identity theft scenarios in this guide and cut them into strips.

What you'll need

THIS TEACHER GUIDE

- [Acting out fraud and identity theft \(guide\)](#)
[cfpb_building_block_activities_acting-fraud-identity-theft_guide.pdf](#)

STUDENT MATERIALS

- [Acting out fraud and identity theft \(worksheet\)](#)
[cfpb_building_block_activities_acting-fraud-identity-theft_worksheet.pdf](#)
- [Fraud and identity theft scenario strips](#) (in this guide)

Exploring key financial concepts

Fraud is an illegal act that occurs when people try to trick you out of your personal information and your money. Identity theft is when someone uses your personal information – such as your name, Social Security number, or credit card number – without your permission. Millions of Americans are victims of fraud or identity theft each year. No matter where you live or how old you are, you may someday be affected by these crimes. Identity theft

TIP

Because terms and laws related to fraud and identity theft change, students should be encouraged to always look for the most up-to-date information.

can happen over the phone by answering personal questions or online by clicking suspicious links, answering social media quizzes that ask for personal information, or opening emails from unknown sources on your computer or phone. Companies or businesses that are genuine usually have passcodes or other methods to protect your personal information. For example, many companies now use something called two-factor authentication. This requires people to use two methods to sign into an account to make it harder for criminals to access the account. Criminals can also steal your personal information from companies or businesses. Knowing how to recognize fraud and identity theft can help you protect your money.

Teaching this activity

Whole-class introduction

- Ask students if someone they know has been a victim of fraud or identity theft.
 - Ask if they know how that experience made the person feel.
- Read the “Exploring key financial concepts” section to students.
- Distribute the “Acting out fraud and identity theft” worksheet and review the terms listed on the worksheet as a class.
- Be sure students understand key vocabulary:
 - **Data breach:** The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. Someone who gets the data might use it for identity theft.
 - **Elder financial exploitation:** The illegal or improper use of an older adult’s funds, property, or assets by family members, caregivers, friends, or strangers who gain their trust.
 - **Foreclosure relief scam:** Scheme to take your money or your house often by making a false promise of saving you from foreclosure; includes mortgage loan modification scams.
 - **Fraud:** An illegal act that occurs when people try to trick you out of your personal information and your money.
 - **Identity theft:** Using your personal information – such as your name, Social Security number, or credit card number – without your permission.

TIP

Visit CFPB’s financial education glossary at consumerfinance.gov/financial-education-glossary/.

- **Imposter scam:** An attempt to get you to send money by pretending to be someone you know or trust, like a sheriff; local, state, or federal government employee; a family member; or charity organization.
- **Mail fraud scam:** Letters that look real but contain fake promises. A common warning sign is a letter asking you to send money or personal information now to receive something of value later.
- **Phishing scam:** When someone tries to get you to give them personal information, such as through an email or text message, often by impersonating a business or government agency. This can be thought of as “fishing for confidential information.”
- **Romance scam:** When a new friend says they like or love you, but they really just want your money—and may not be who they say they are.
- **Scam:** A dishonest trick used to cheat somebody out of something important, like money. Scams can happen in person, through social media, or by phone, email, postal mail, or text.
- **Spoofing:** When a caller disguises the information shown on your caller ID to appear as though they are calling as a certain person or from a specific location.
- **Tax-related identity theft:** When someone steals your Social Security number to file a tax return claiming a fraudulent refund; may also be called tax-filing-related identity theft.
- **Wire transfer fraud:** Tricking someone into wiring or transferring money to steal from them. One common example of a wire transfer fraud is the “grandparent scam.” This is when a scammer posing as a grandchild or a friend of a grandchild calls to say they are in a foreign country, or in some kind of trouble, and need money wired or sent right away.

TIP

Since understanding types of fraud and identity theft is important for students to successfully complete this activity, be sure to review these definitions so students are familiar with similarities and differences. You might consider creating an anchor chart with the definitions to hang on classroom walls. Remind students to refer to these definitions to help them identify the fraud or identity theft described in each skit.

Group work

- Tell students that they’ll create and perform skits showing types of fraud or identity theft and that the class will guess which type it is.
- Divide the students into pairs or small groups and distribute one fraud or identity theft scenario to each group.

- Give groups time to plan and practice their skit.
- Ask each group to perform their skit.
 - As each group performs, ask the rest of the class to use the terms listed on their worksheet to guess what type of crime is being committed.
 - Facilitate class discussion related to the details of the various crimes, as needed.

Wrap-up

Have students complete an exit ticket using these prompts:

- How do fraud and identity theft pose a financial risk to me now and in the future?
- What can I do to protect myself?

Suggested next steps

Consider searching for other CFPB activities that address the topic of protection, including managing risk and preventing fraud and identity theft. Suggested activities include “Reporting fraud or identity theft to authorities” and “Examining the statistics on fraud and identity theft”.

Measuring student learning

Students’ skits and their responses on their worksheets and during discussion can give you a sense of their understanding.

This answer guide provides possible answers for the “Acting out fraud and identity theft” worksheet. **Keep in mind that students’ answers may vary, as there may not be only one right answer.** The important thing is for students to have reasonable justification for their answers.

Answer guide

Scenario #	Scenario description	Identify the fraud or identity theft
1	Email asks you to send personal information	C - Phishing scam
2	Someone has filed a tax return in your name	F - Tax-related identity theft
3	Send personal info to claim a prize	A - Mail fraud scam
4	Caller ID shows a call from the high school	G - Spoofing
5	Fake charity fundraising	E - Wire transfer fraud
6	Caller claiming to be with the sheriff's office	B - Imposter scam
7	Person pretending to be you	D - Identity theft
8	Neighbor is taking money from grandmother's bank account	J - Elder financial exploitation
9	Your credit card information was hacked	I - Data breach
10	Fake foreclosure notification	H - Foreclosure relief scam
11	New online friend asks you to send them \$250 for a new outfit.	K - Romance scam

Fraud and identity theft scenarios

Print these scenarios single-sided, cut them into strips, and give one to each student group.



1. You receive an email that encourages you to click a link and enter personal information, including your Social Security number and bank account number. The email looks official, but the sender's email address seems odd.

TYPE OF FRAUD: Phishing scam

2. You contact the IRS to ask for more time to file your taxes, but you find out that someone has already filed a tax return in your name.

TYPE OF FRAUD: Tax-related identity theft

3. You receive a letter from an unknown company with a message that you've won a cash prize. To claim your prize, you'll need to send them your bank account information so they can deposit the money into your account. The company then uses your bank account information to take money from you.

TYPE OF FRAUD: Mail fraud scam

4. Your caller ID shows that a local number associated with the high school in your town is calling you. You answer and the person calling says they're raising money for a local sports tournament. You soon realize the caller is not actually with the school.

TYPE OF FRAUD: Spoofing

5. You get a call from someone raising money for a charity. They ask you to wire money immediately because they have a critical and urgent humanitarian need. They get annoyed when you ask them for more information.

TYPE OF FRAUD: Wire transfer fraud



6. You get a call from someone claiming to be with the sheriff's office. They say they need your personal information to update their neighborhood records. You quickly recognize they're not actually who they claim to be.

TYPE OF FRAUD: Imposter scam

7. Someone pretending to be you used your name and personal information to borrow money to purchase a car.

TYPE OF FRAUD: Identity theft

8. Your grandmother has a neighbor who has gained her trust but has been secretly taking money from her bank account.

TYPE OF FRAUD: Elder financial exploitation

9. A hacker stole information from your credit card company, including your personal data, and used it to charge purchases.

TYPE OF FRAUD: Use of stolen data from a data breach

10. You receive a letter saying that your house is in foreclosure and will be taken by the bank unless you mail a check and your personal information immediately. You know you've been paying your mortgage on time.

TYPE OF FRAUD: Foreclosure relief scam

11. You have a friend you met through a social media app. You have not met in person, but you know it is true love. You have so much in common, and they look great in their pics. They ask you to do them a favor and send them \$250 for a new outfit they can't wait for you to see them in.

TYPE OF FRAUD: Romance scam