SCAM AWARENESS AND PREVENTION

2025 Board and Committee Leadership Conference
HeartSong Lodge and Resort
Kentucky Financial Empowerment Commission
November 7th, 2025

KENTUCKY BANK ON NETWORK

Kentucky Financial Empowerment Commission

ABOUT THE PRESENTER

Richard Bryant
Interim Executive Director
Richard.Bryant@ky.gov

- Agriculture and Aquaculture
- US Peace Corps - RAP
- Volta Catch
- "How to Start a Business" through the USDA BFRDP
- Interim Executive Director at the KFEC
- Kentucky Bank On Network Fellow
- Certified by the Kentucky Bankers Association in Fraud Education, Detection, and Prevention

Kentucky Financial
Empowerment Commission

OUR STORY

KENTUCKY BANK ON NETWORK

2018

HB 132 Mandated Financial Literacy for Kentucky High School Students

2019

HB 139 Established the Kentucky Financial Empowerment Commission as a non-profit organization

2020-Now

Growing and developing our niche as a Financial Education Convener

2025

HB 342 Mandates one credit hour of financial literacy education for all graduating Kentucky high school seniors.

Kentucky Financial
Empowerment Commission

Kentucky Financial
Empowerment Commission

OUR FOCUS GROUPS

- K-12 Commonwealth Students and Teachers
- Veterans and Military Personnel
- Kentuckians with Disabilities
- Commonwealth Employees
- Low Income Families
- Aging Kentuckians

KFEC Board of Directors

Kentucky Financial
Empowerment Commission

KENTUCKY BANK ON
NETWORK

COMMONWEALTH OF KENTUCKY
UNITED WE STAND
DIVIDED WE FALL

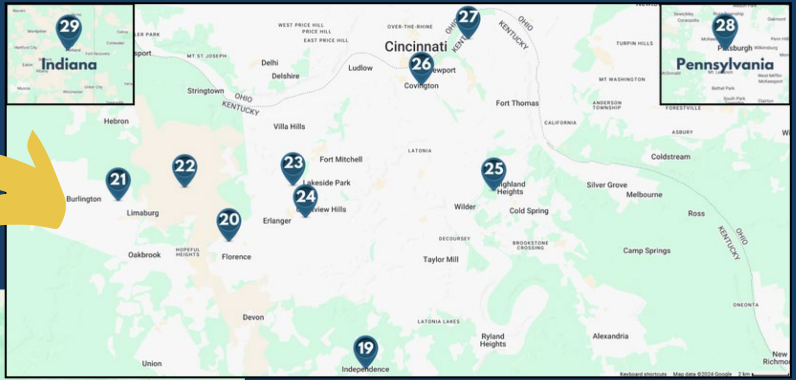
Mark H. Metcalf
KENTUCKY STATE TREASURER

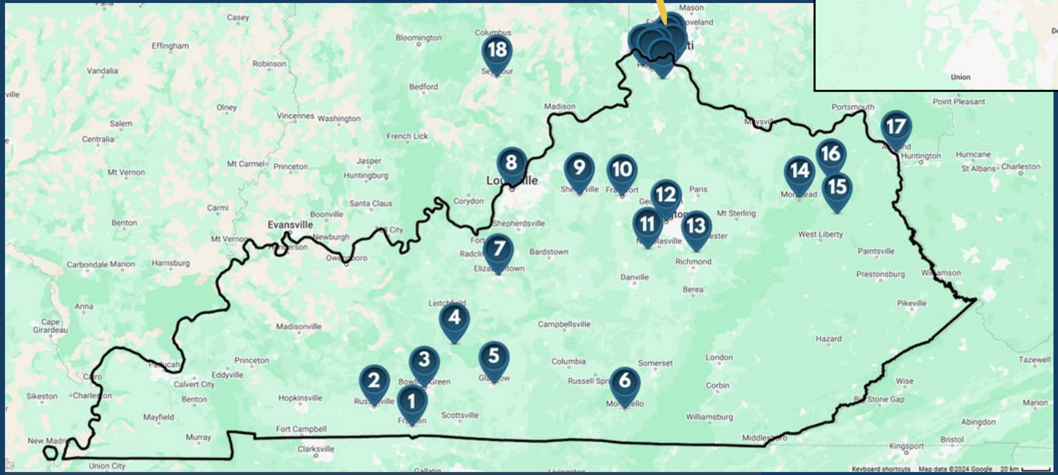
Financial wellness is a relative measure of how well a person manages their financial life.

Improving financial wellness is about practicing better money habits, setting goals and taking steps to achieve them—all with the aim of improving your overall quality of life.

-Forbes

2024





1	Franklin	Re-Entry Bootcamp: 33 Participants		
2	Russellville	Re-Entry Bootcamp: 32 Participants		
3	Bowling Green	EFEW: 408 Participants		
		K-12 Teachers and Students: 46 Participants		
4	Mammoth Cave	Re-Entry Bootcamp: 16 Participants		
5	Glasgow	Aging Kentuckians: 129 Participants		
6	Monticello	Aging Kentuckians: 44 Participants		
7	Elizabethtown	EFEW: 27 Participants		
8	Louisville	K-12 Teachers and Students: 146 Participants		
9	Shelbyville	Disability Workshops: 129 Participants		
10	Frankfort	K-12 Teachers and Students: 72 Participants		
		EFEW: 4 Participants		
		KCTCS Ready to Work: 112 Participants		
11	Wilmore	K-12 Teachers and Students: 50Participants		
12	Lexington	K-12 Teachers and Students: 235 Participants		
		EFEW: 63 Participants		
		Disability Workshops: 6 Participants		
13	Somerset	Aging Kentuckians: 61 Participants		
14	Morehead	K-12 Teachers and Students: 70 Participants		

15	Sandy Hook	Bank On: 37 Participants
16	Olive Hill	Bank On: 6 Participants
17	Ashland	Bank On: 13 Participants
18	Seymore, IN	K-12 Teachers and Students: 18 Participants
19	Independence	EFEW: 408 Participants
20	Florence	K-12 Teachers and Students: 318 Participants
21	Burlington	K-12 Teachers and Students: 313 Participants
22	Hebron	EFEW: 210 Participants
23	Erlanger	EFEW: 600 Participants
		Disability Workshops: 73 Participants
24	Edgewood	EFEW: 240 Participants
		Disability Workshops: 7 Participants
25	Highland Heights	K-12 Teachers and Students: 38 Participants
26	Covington	EFEW: 376 Participants
27	Dayton	EFEW: 104 Participants
28	Pittsburg, PA	K-12 Teachers and Students: 20 Participants
29	Portland, IN	K-12 Teachers and Students: 85 Participants
30	Statewide	Bank On: 23 Participants
		K-12 Teachers and Students: 131 Participants

KENTUCKY BANK ON NETWORK

Opening a safe and affordable bank account is a great first step as you return to the community. It can help you manage your money, avoid costly fees, build your credit, and feel more in control of your financial future.

BANKING ACCESS FOR ALL KENTUCKIANS

Why Banking Access Helps

- Safe place to store money
- Direct deposit for paychecks or benefits
- Protection from theft or loss
- Lower fees than check cashers or payday loans
- Helps build credit and qualify for loans later
- Easy access to debit cards and online banking

To open an account, you'll need:

- Photo ID – State ID or Driver's License
- Social Security Number or ITIN
- Proof of Address – Some banks accept shelter or program letters
- Need help getting ID? call 211.

These Kentucky Bank On certified partners offer low-cost accounts with:

- No overdraft fees
- $25 or less to open
- $5 or less monthly fees

- Alliant Credit Union
- Ally Bank
- Armed Forces Bank
- Bank of America
- BMO Harris
- Chase
- City National Bank
- Discover Bank
- Fifth Third Bank
- First Financial Bank
- First Harrison Bank
- Forcht Bank
- Heritage Bank
- Lending Club
- Old National Bank
- PNC Bank
- Regions
- Republic Bank
- Truist
- Traditional Bank
- U.S. Bank
- Woodforest National Bank

For more information visit www.kyfec.org

Kentucky Financial Empowerment Commission

Bank On

WHAT ARE KFEC'S STUDENTS SAYING ABOUT OUR COURSES

96% Agreed KFEC Instructors were prepared for teaching their class

98% Agreed that our courses increased their financial literacy knowledge

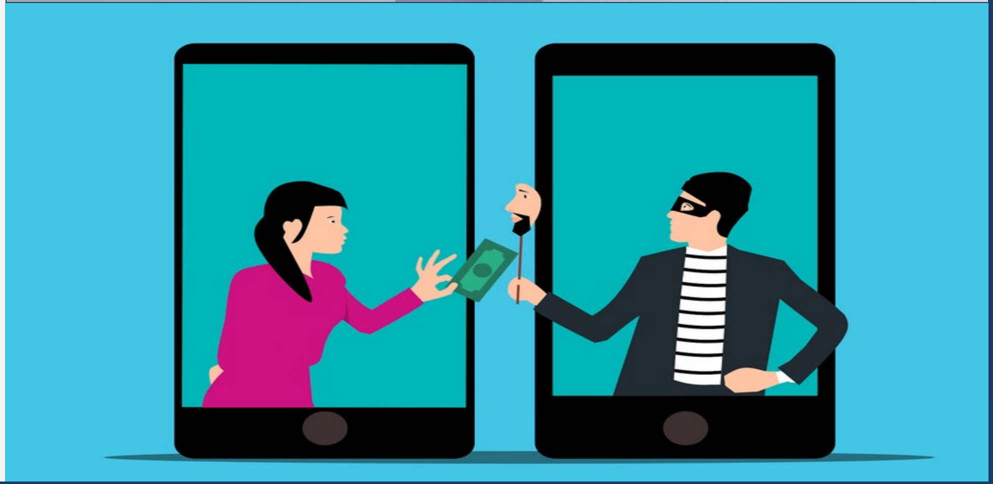
97% Overall Average Course Rating

100% Agreed KFEC Instructors communicated clearly and were easy to understand

96% Felt confident that they could apply what they learned to their personal / professional life

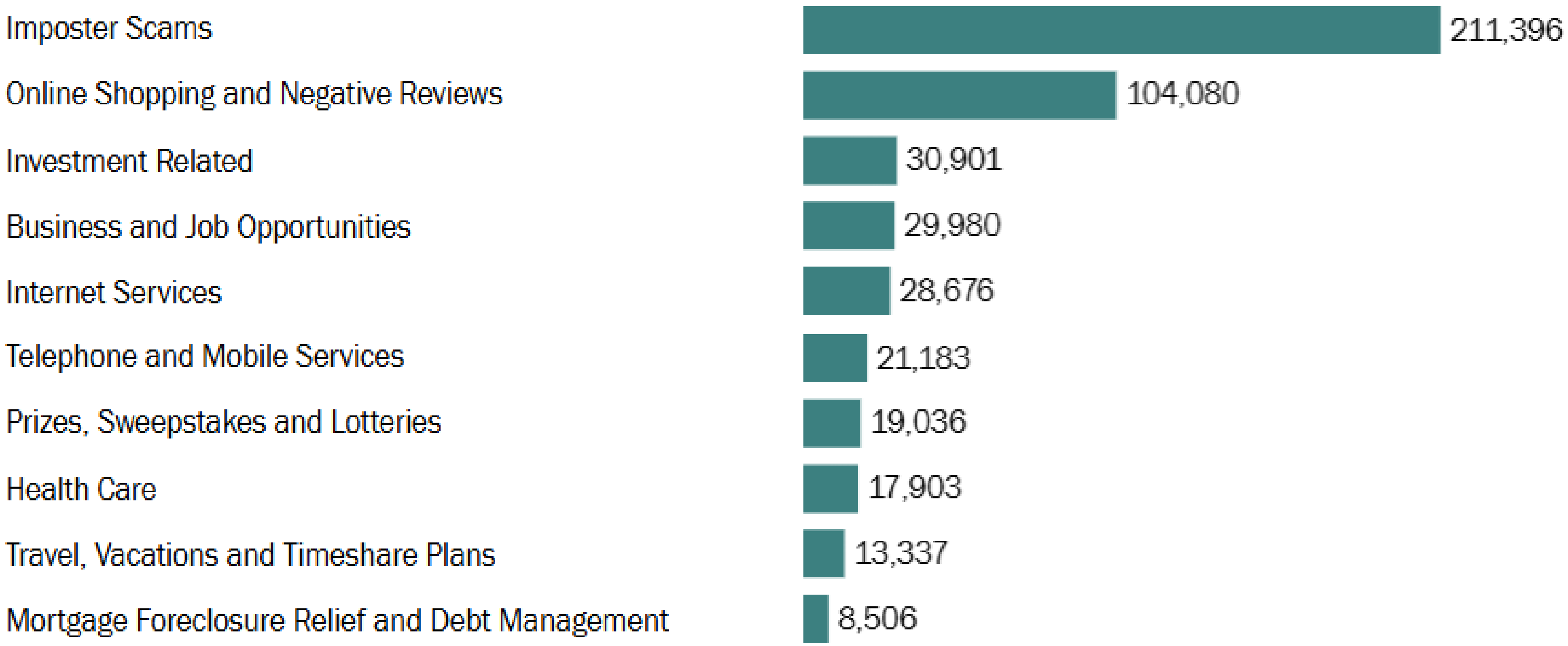
What's the #1 fraud committed on social media?

What's the #1 fraud committed on social media?

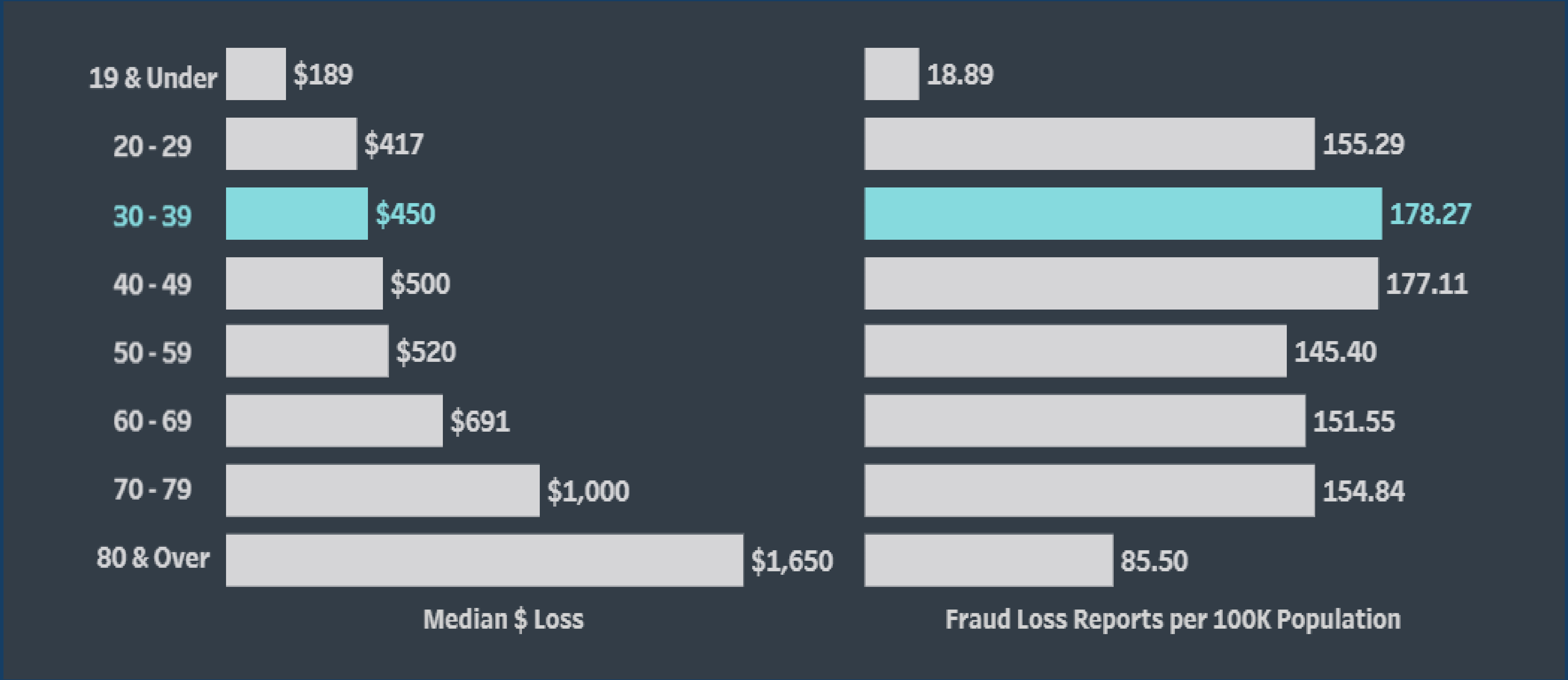


Top Fraud Reports in the USA

Top 10 Fraud Report Categories

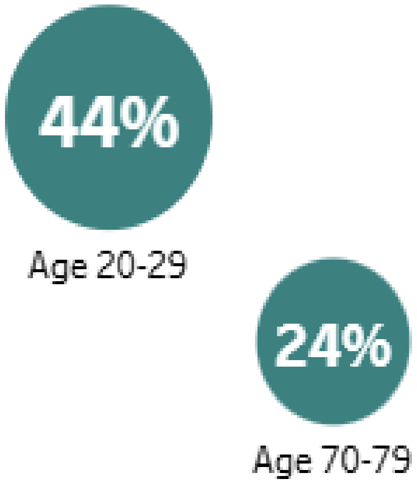


Age and Fraud Loss

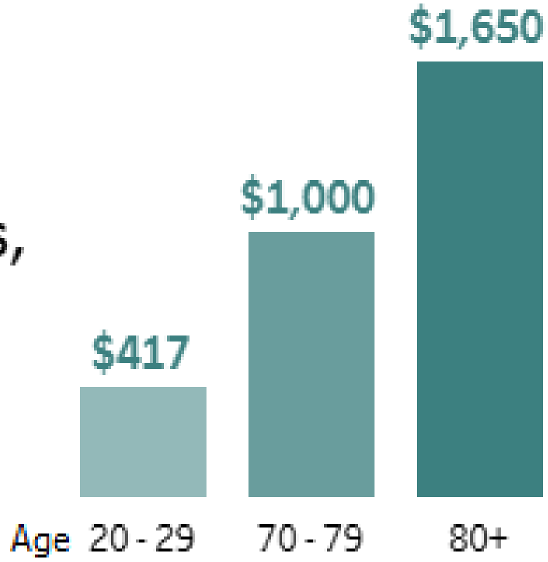


Fraud affects every generation differently

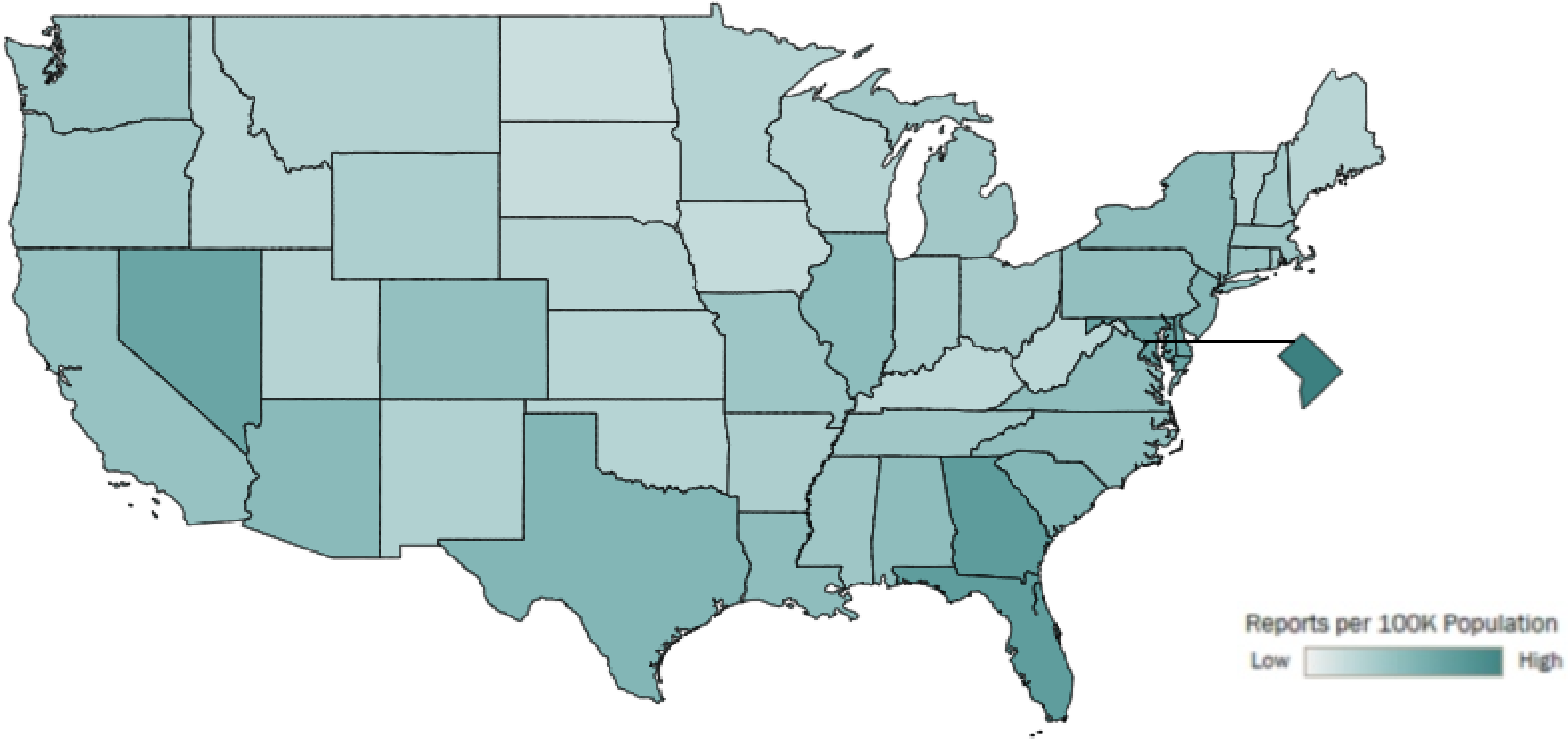
Younger people reported losing money to fraud **more often than older people.**



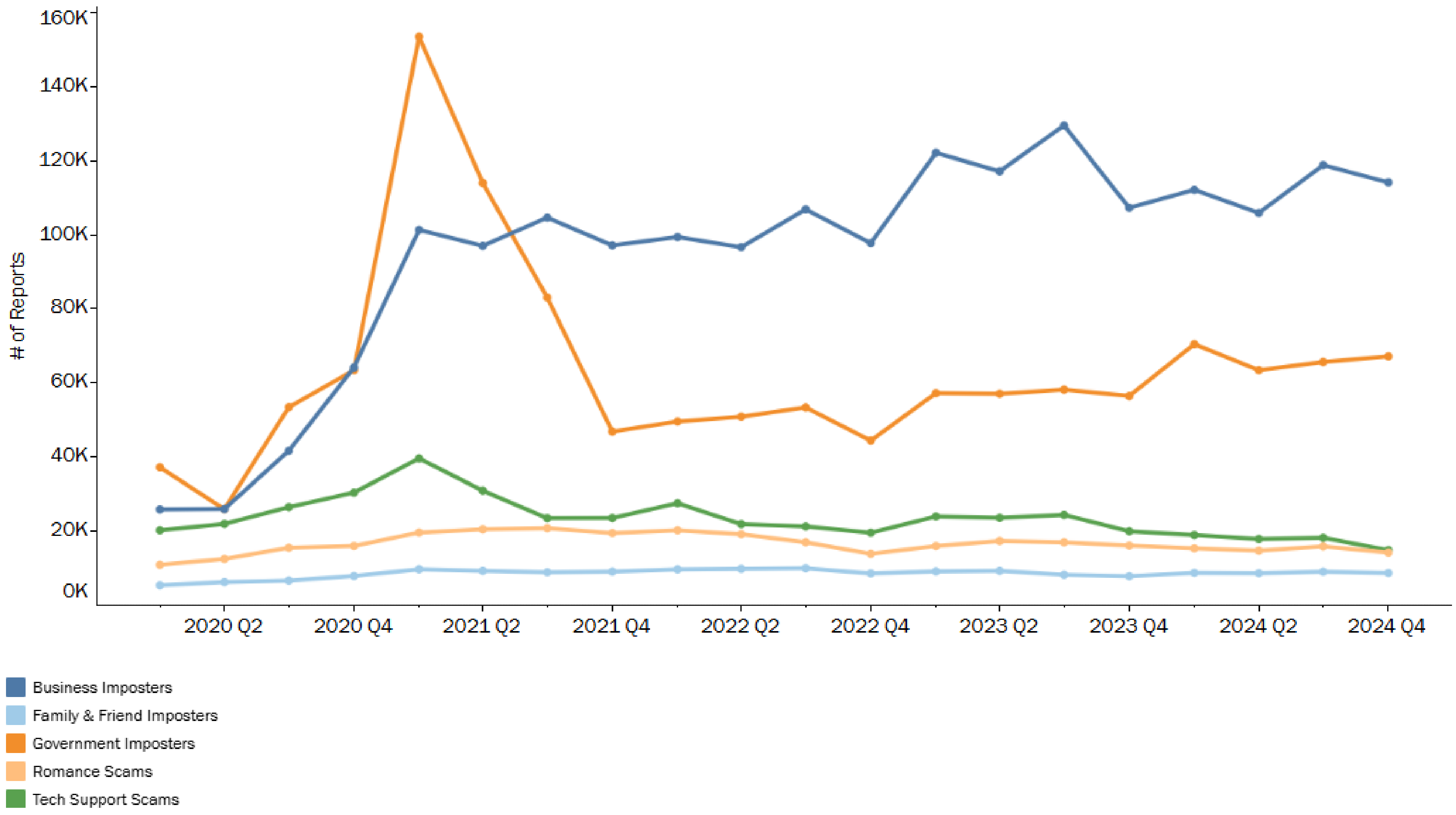
But when people aged 70+ had a loss, **the median loss was much higher.**



Fraud reports across the USA



Trends Among Fraud Reported in the USA



Common Payment Methods used by scammers

- Wire transfers
- Money transfers
- P2P (peer-to-peer or person-to-person) payment services and mobile payment apps
- Gift cards
- Cryptocurrency

You’ve Won Scams

How it works:

- A call, text message, email, or mailer says “You’ve won”
  - A prize!
  - A sweepstakes!
  - A lottery!
  - A vacation or cruise!

What happens next:

- Scammers say you must pay fees, taxes, customs duties
- Scammers pressure you to act now
- Scammers tap into your emotions
- Scammers tell you to keep this a secret

You’ve Won Scams

What to do:

- Stop
- Don’t give personal or financial information
- Don’t send payment

Report it:

- ReportFraud.ftc.gov
- 1-877-FTC-HELP

Job and Money-making Scams

Working and making money from home:

- Earn money in retirement
- Try a new occupation
- Have a flexible schedule

How job scams work:

- You post a resume on a job search site
- You answer a job listing
- You're asked for personal information or payment

Job and Money-making Scams

How money-making scams work:

- You answer an ad to make big money working from home
- You buy a "proven" system to help start a business
- You're pressured to spend money to make money

Job and Money-making Scams

What to do:

- Stop
- Check it out
- Don't share personal or bank information
- Don't pay for the promise of a job

Report it:

- ReportFraud.ftc.gov
- 1-877-FTC-HELP

Investment Scams

How it works:

- Infomercial or ad online says you can learn how to make lots of $$$
- Quick, easy, low risk
- “Proven” system

Why it works:

- Scammers are convincing
- They tap into your emotions
- They have testimonials

Investment Scams

What to do:

- Stop
- Consider the risk
- Take time to research the offer

Report it:

- **ReportFraud.ftc.gov**
- 1-877-FTC-HELP

Romance Scams

How it Works:

- Someone contacts you on social media
- You meet someone on a dating website

What happens next:

- They quickly say they're in love with you
- Asks for money for plane ticket or an emergency

Why it works:

- They're convincing
- They tap into your emotions

Romance Scams

Things they might say:

- "I wish I could come meet you, but I don't have enough money for a plane ticket."
- "I want to come visit, but my son is sick and I don't have money to take him to the doctor."
- "If I could only get a visa, we could be together. Can you send money to help pay for it?"

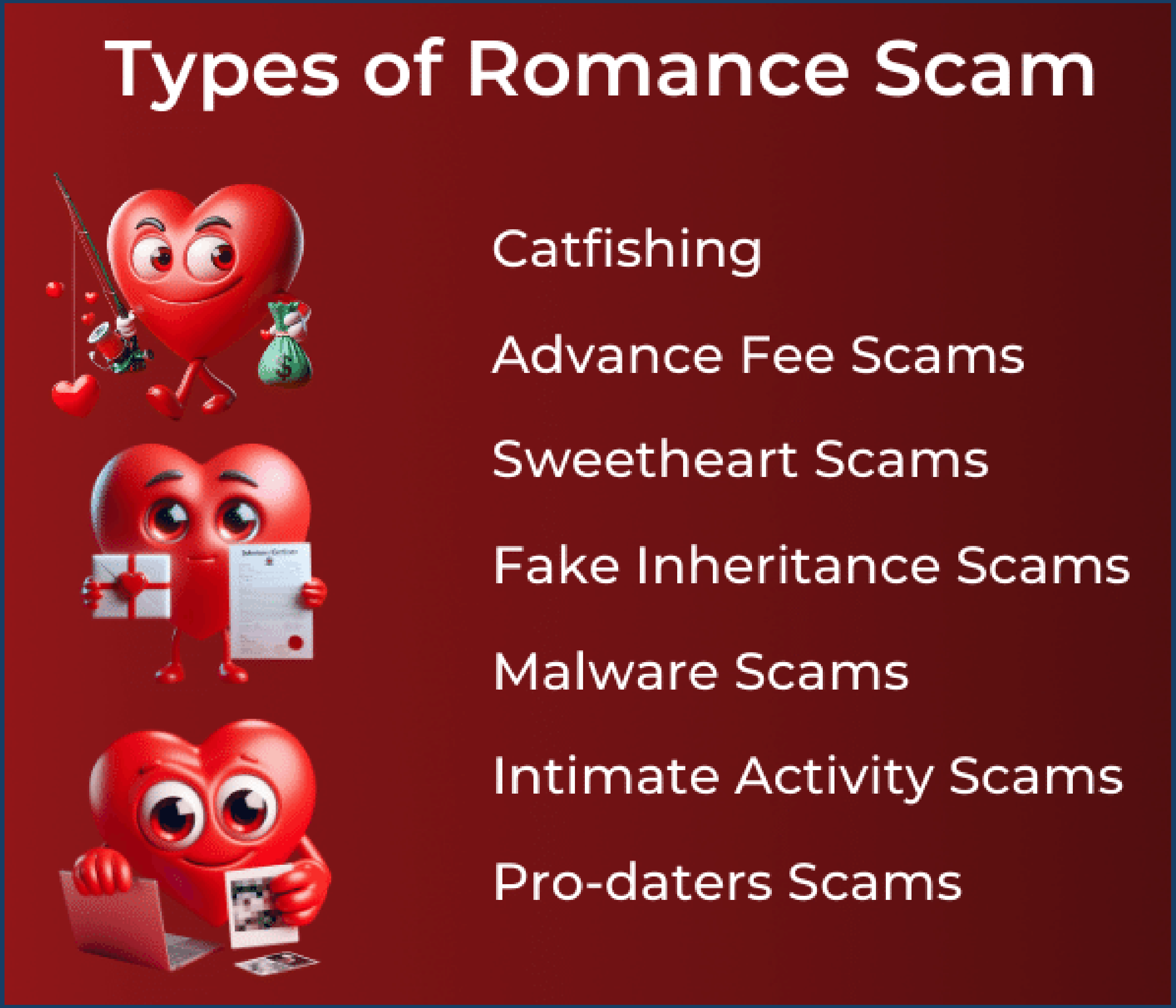
Romance Scams

What to do:

- Always take it slow
- Never send money
- Pass this information on to a friend

Report it:

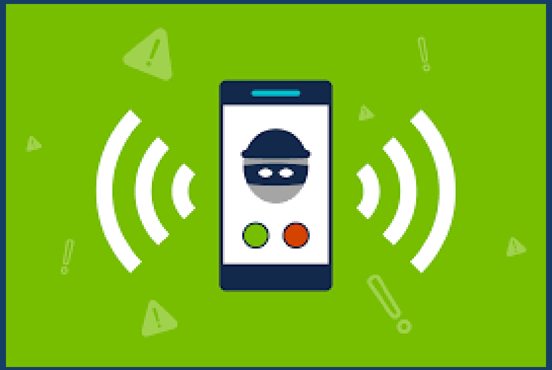
- **ReportFraud.ftc.gov**
- 1-877-FTC-HELP



Unwanted Calls and Text Messages

Unwanted and unexpected calls saying

- "This is the Social Security Administration."
- "Your car warranty is about to expire."
- "You're eligible for a vacation cruise."



What to do:

- Ignore unknown calls or hang up
- Don't say anything
- Don't press buttons on your phone
- Consider call blocking: ftc.gov/calls

Unwanted Calls and Text Messages

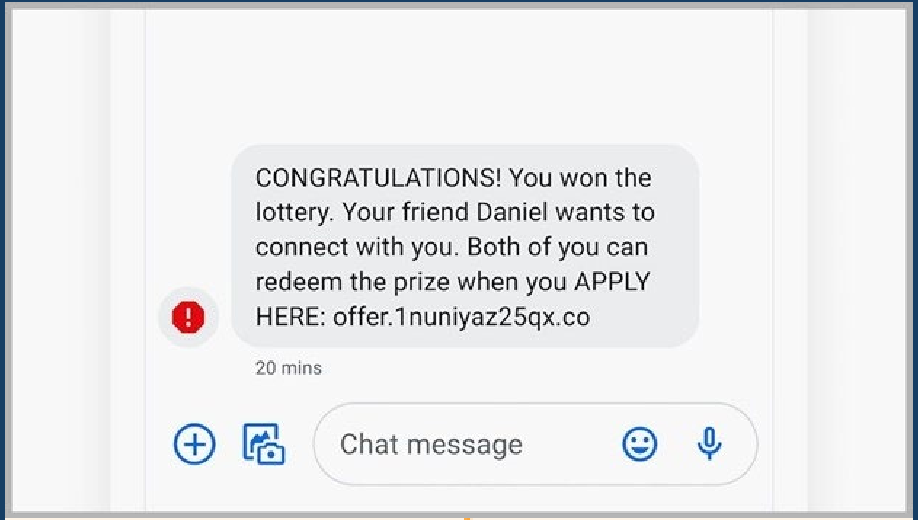
Unwanted and unexpected text messages saying:

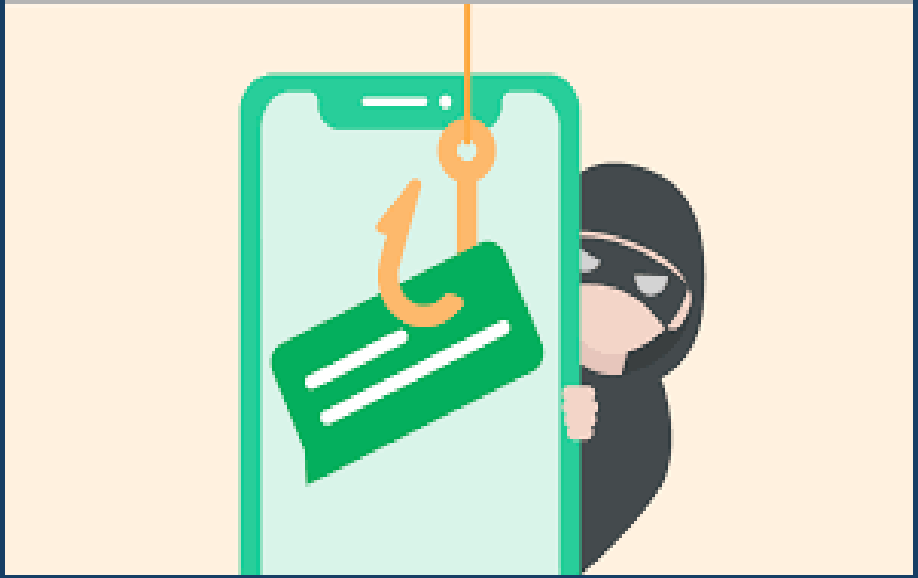
- “Click to confirm your delivery.”
- “Click to claim your discount coupon.”
- “There’s a problem with your account.
- “Verify your information.”

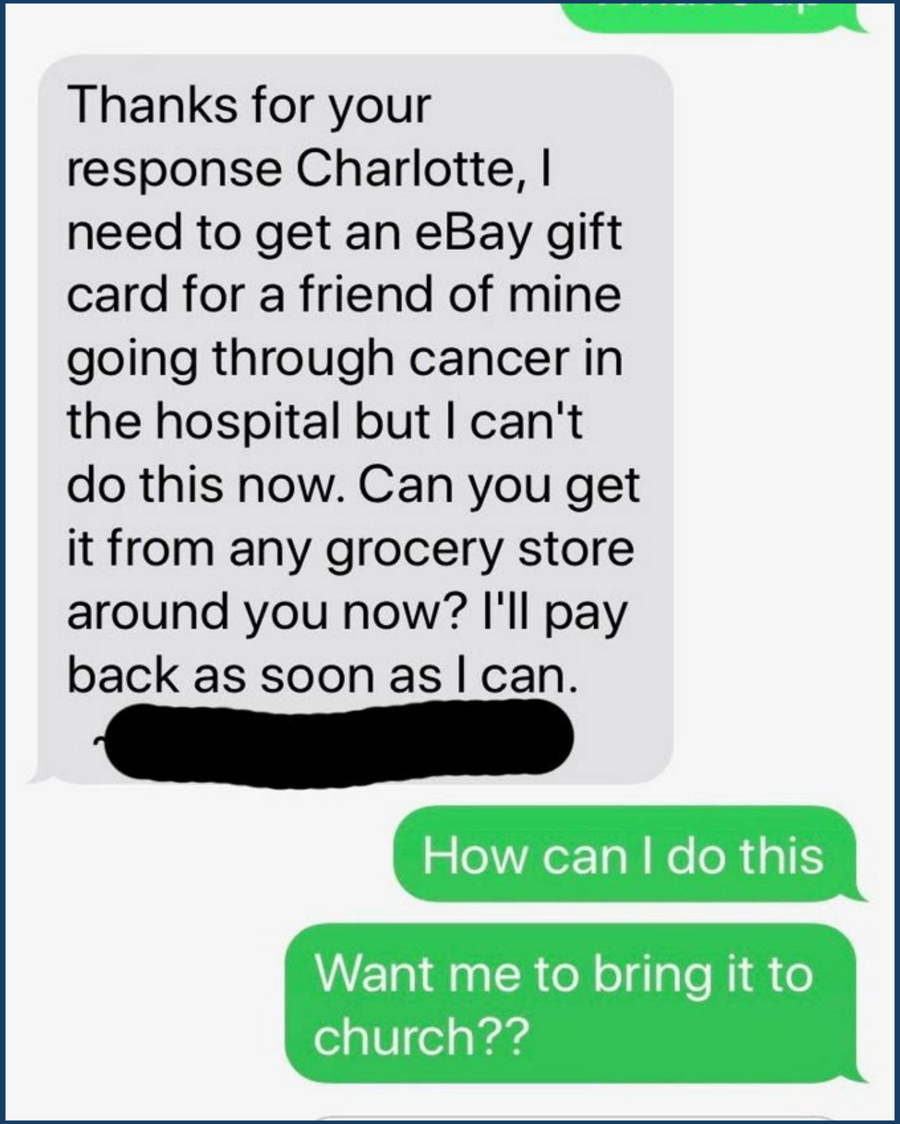
What to do:

- Ignore the text message
- Don’t reply
- Never click on links
- Consider text filtering and blocking

Unwanted Calls and Text Messages



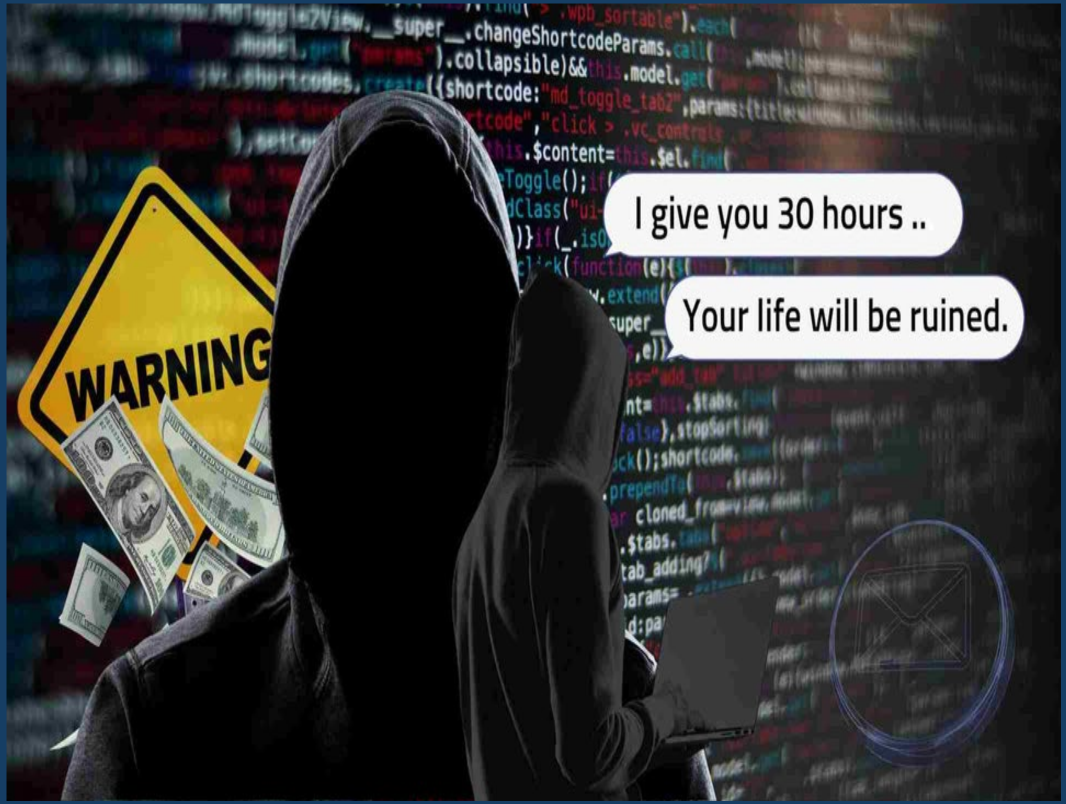




Blackmail Scams

- Scare you into sending them money by threatening to distribute private content—from your computer or phone, or shared with them over an email, text, or social media—that could embarrass you.

- Could be complete strangers and other times they might be someone you met online and thought you could trust.



Blackmail Scams

What to do:

- Stay calm in spite of blackmailers' intimidation and high-pressure tactics.
- Stop communicating with them and don't pay them.
- Keep all messages as evidence to help law enforcement.
- Keep in mind that you don't need to deal with this alone.

Charity Scams

- Thief poses as a real charity or makes up the name of a charity that sounds real to get money from you.
- Often increase during the holiday season as well as after natural disasters and emergencies, such as storms, wildfires, or earthquakes.
- Be careful when a charity calls to ask for donations, especially ones that suggest they're following up on a donation pledge you don't remember making.
- Watch for scammers that try to get you to donate by using live streaming on social media platforms, altered images, or images or voices generated by artificial intelligence (AI).

Charity Scams

What to do:

- Ask for detailed information about the charity, including address and phone number.
- Look up the charity through their website or a trusted third-party source to confirm that the charity is real.

Debt Settlement and Debt Relief Scams

- Debt settlement or debt relief companies often promise to renegotiate, settle, or in some way change the terms of a debt you owe to a creditor or debt collector.
- Can be risky and could leave you even further in debt.

Debt Settlement and Debt Relief Scams

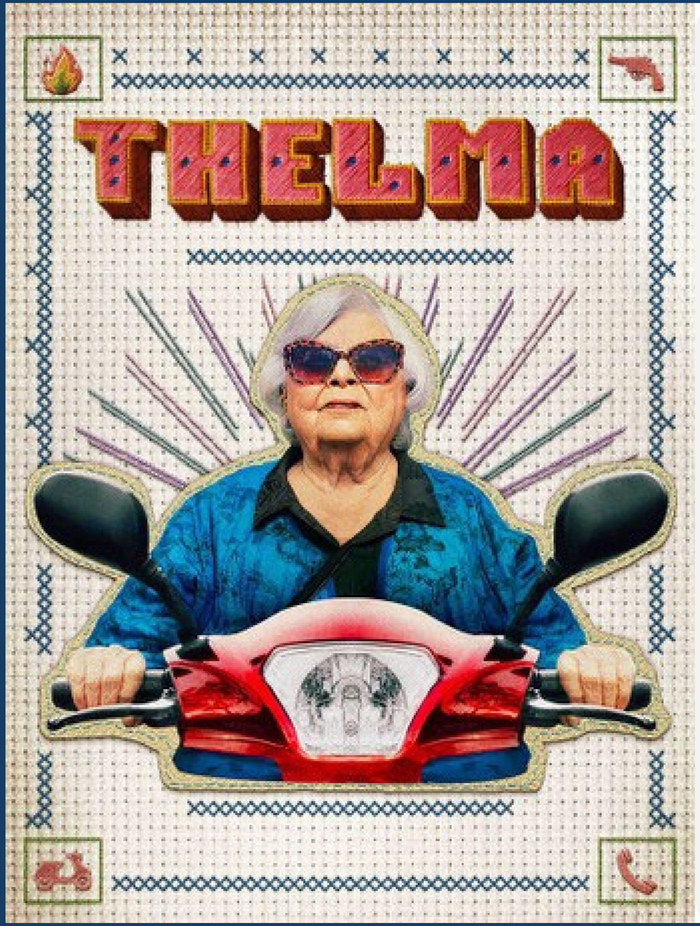
What to do:

- Avoid doing business with a company that guarantees they can settle your debts, especially those that charge up-front fees before performing any services.
- Instead, you can work with a reputable nonprofit credit counseling program that can help you work with your creditors.

Grandparent Scams

- Will call and sounds like a grandchild or relative asking you to wire or transfer money or send gift cards to help them out of trouble.
- Artificial intelligence has made it easier for scammers to clone voices and alter images to make it seem like someone you know needs help.
- Meant to play on your emotions.
- Target older adults, especially during the holidays.

Grandparent Scams



98%
Tomatometer
207 Reviews

83%
Popcornmeter
250+ Verified Ratings

Inspired by a real-life experience of director Josh Margolin's own grandmother, THELMA puts a clever spin on movies like MISSION: IMPOSSIBLE, shining the spotlight on an elderly grandmother as an unlikely action hero. With infectious humor, Margolin employs the familiar tropes of the action genre in hilarious, age-appropriate ways to tackle aging with agency. In the first leading film role of her 70-year career, Squibb portrays the strong-willed Thelma with grit and determination, demonstrating that she is more than capable of taking care of business -- despite what her daughter Gail (Parker Posey), son-in-law Alan (Clark Gregg), or grandson Danny might believe.

Watch on Fandango at Home

STREAM NOW

Grandparent Scams

What to do:

- Beware of a caller who insists on secrecy and contact your relative yourself to verify the story.
- If you can’t reach them, try to get in touch with them through another trusted person, another family member, or their friends.

Sale of Nonexistent Goods or Services Scams

- Use mobile payment apps to trick people into sending money or merchandise without holding up their end of the deal.
- For example, a scammer may offer to sell you concert or sports tickets, or a puppy or other pet, but then never actually give them to you.
- Scammer might purchase an item from you, appear to send a payment, and then cancel it before it reaches your bank account.

‘Tis the Season to Avoid Online Shopping Scams

In 2021, the FBI’s Internet Crime Complaint Center (IC3) reported that Americans lost $337 million to non-payment and non-delivery scams. In these scams, buyers pay for products or services online, but never receive them. Conversely, sellers ship goods or provide services, but never receive payment.

Recognize Warning Signs

- Products and services advertised at **incredibly low prices**—significantly lower than competitors.
- **Sellers that only accept payments by wire transfer, money orders, gift cards, or peer-to-peer payment services** like CashApp, Venmo and Zelle.
- **Vague or non-existent contact details** or information about returns, exchanges or privacy policies.
- Websites with **poor spelling or grammar**.

Sale of Nonexistent Goods or Services Scams

What to do:

- Never send money to someone you don't know.
- If you think you made a payment to a scammer, contact your bank or the company you used to send the money immediately and alert them that there may have been an unauthorized transaction.
- You can also file a complaint with the Federal Bureau of Investigation's Internet Crime Complaint Center at www.ic3.gov

Disaster Scams

After a disaster, be wary of scams, especially those involving fake charities, fraudulent contractors, or impersonation of government officials or insurance adjusters, and always verify information and sources before acting.

1. Fake Charities:
   - What to watch out for:
     - Scammers may create fake charities or impersonate legitimate ones to solicit donations.

How to protect yourself:

- Donate to well-known, trusted charities with a proven track record. Verify a charity's legitimacy through its official website or reputable organizations like Charity Navigator or CharityWatch.

Disaster Scams

2. Contractor Fraud:

What to watch out for: Scammers may offer to repair or rebuild homes but demand payment upfront and then disappear without completing the work.

How to protect yourself: Never pay upfront for any repairs. Get multiple quotes from reputable contractors and verify their credentials.

Tip: Ask for references and check with the Better Business Bureau.

Disaster Scams

3. Impersonation Scams:

What to watch out for: Scammers may impersonate government officials, insurance adjusters, or law enforcement officers to gain access to your information or money.
How to protect yourself: Always ask for identification and call the organization the person claims to work for to confirm their identity.

Tip: Never give personal information to anyone you don't know.

Disaster Scams

4. Phishing Scams:

What to watch out for: Scammers may send phishing emails or text messages containing malicious links or requesting personal information under the guise of assistance.

How to protect yourself: Be cautious of emails or texts with disaster-related subject lines, attachments, or hyperlinks.

Tip: Never click on suspicious links or open attachments from unknown senders.

Disaster Scams

BEWARE *of* FRAUD *when Seeking* DISASTER ASSISTANCE

Disaster Survivor Assistance Teams and home inspectors are often sent to rural areas to help disaster survivors, but not all individuals offering assistance are who they say they are.

Don't take a financial hit from scams during your recovery process!

BEFORE YOU ENGAGE, FOLLOW THESE TIPS:

- FEMA representatives and inspectors from other agencies will always have identification.
- Do NOT give cash. Government workers never ask for a fee or payment.
- Do NOT give personally identifiable information over the phone.

Scams Warning Signs

- Claiming to be from the government, a bank, a business, or a family member, and asking you to pay money.
- Asking you to pay money or taxes upfront to receive a prize or a gift.
- Asking you to wire them money, send cryptocurrency, send money by courier, send money over a payment app, or put money on a prepaid card or gift card and send it to them or give them the numbers on the card.
- Asking for access to your money-such as your ATM cards, bank accounts, credit cards, cryptocurrency wallet keys or access codes, or investment accounts.
- Pressuring you to "act now" or else the deal will go away, or trying hard to give you a "great deal" without time to answer your questions.
- Creating a sense of urgency or emergency to play on your emotions.

Tips for Preventing Scams

- **Don’t share numbers or passwords for accounts, credit cards, or Social Security.**
- **Never pay up front for a promised prize.** It’s a scam if you are told that you must pay fees or taxes to receive a prize or other financial windfall.
- **After hearing a sales pitch, take time to compare prices.** Ask for information in writing and read it carefully.
- **Too good to be true?** Ask yourself why someone is trying so hard to give you a “great deal.” If it sounds too good to be true, it probably is.

Tips for Preventing Scams

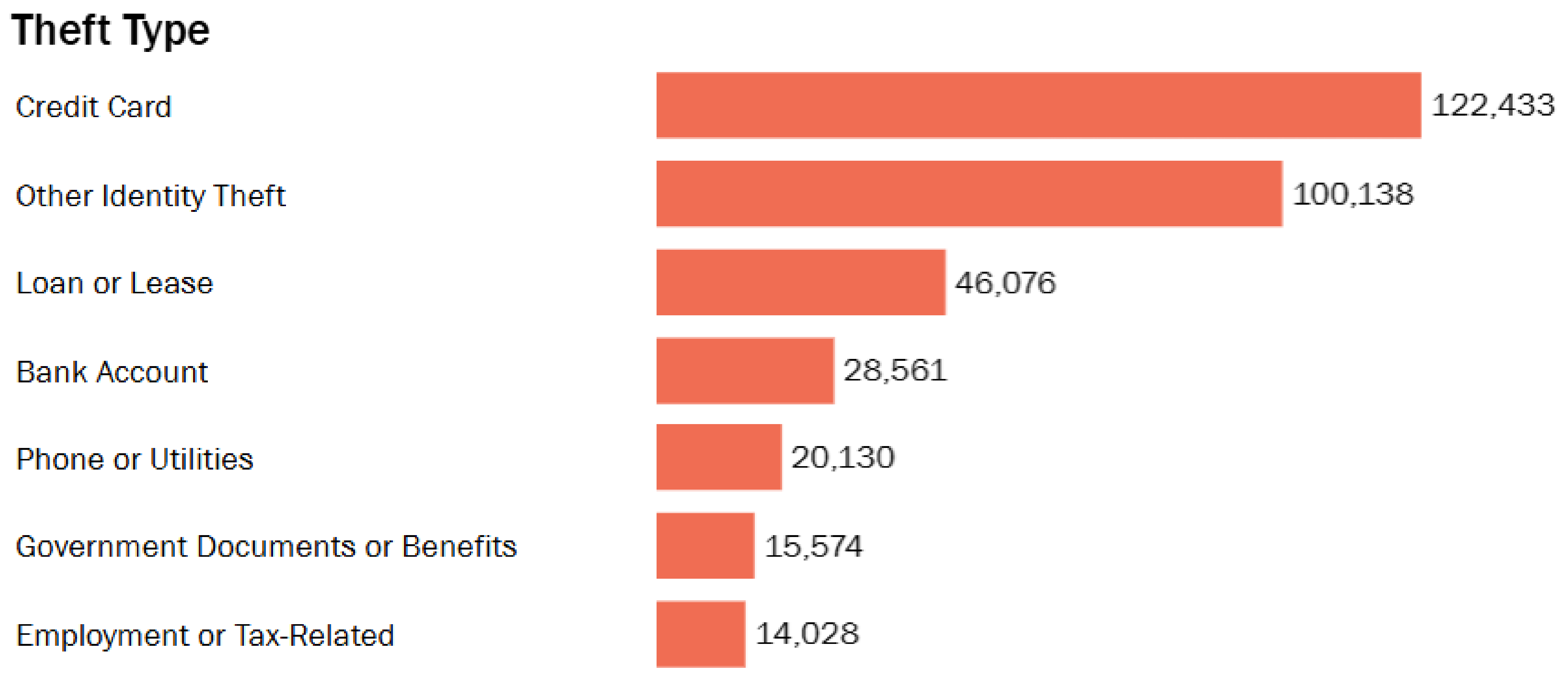
- **Watch out for deals that are only "good today" and that pressure you to act quickly.** Walk away from high-pressure sales tactics that don't allow you time to read a contract or get legal advice before signing. Also, don't fall for the sales pitch that says you need to pay immediately, for example by wiring the money, sending it by courier or over a payment app, or by sending cryptocurrency.
- **Beware when someone plays on your emotions or claims there's an urgent situation**. Advances in artificial intelligence make it easier for scammers to clone voices and alter images to make it seem like someone you know needs help. Contact the person yourself to verify the story. Use contact information you know is theirs. If you can't reach them, try to get in touch with them through another trusted person, like a family member or their friends.

Tips for Preventing Scams

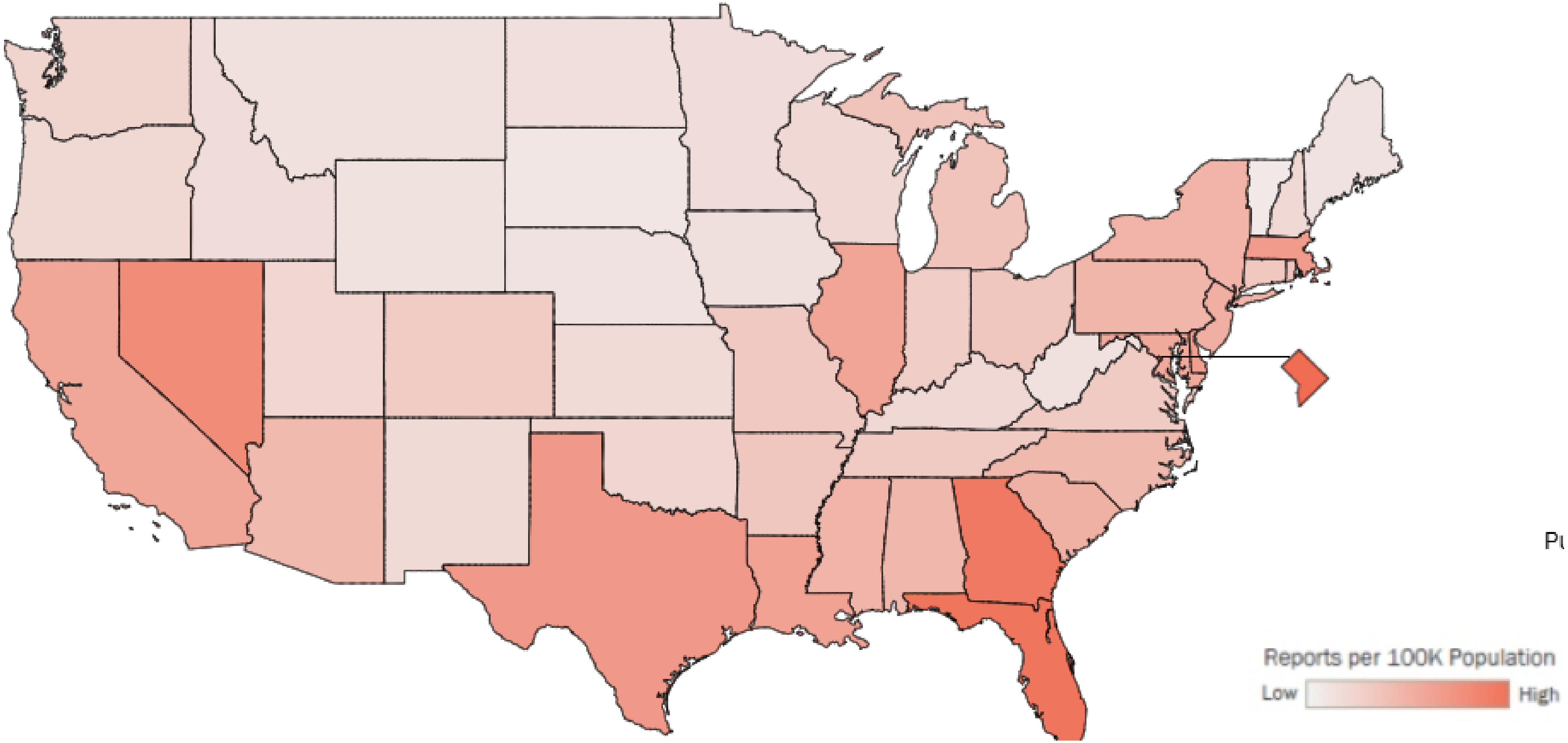
- **Don't click on links or scan QR codes.** These can take you to scammers' malicious websites or give them access to your device.
- **Put your number on the National Do Not Call Registry.** Go to www.donotcall.gov or call (888) 382-1222.

Do not buy or rent from somebody that you do not know or have not checked out previously	Do not invest in a product or service that seems too good to be true	Keep your confidential information private	Do not wire cash
Be naturally skeptical	Educate those around you who are vulnerable to scams such as children or the elderly	Do not click on links or attachments if you do not know/trust the sender	Only donate to charities that you know

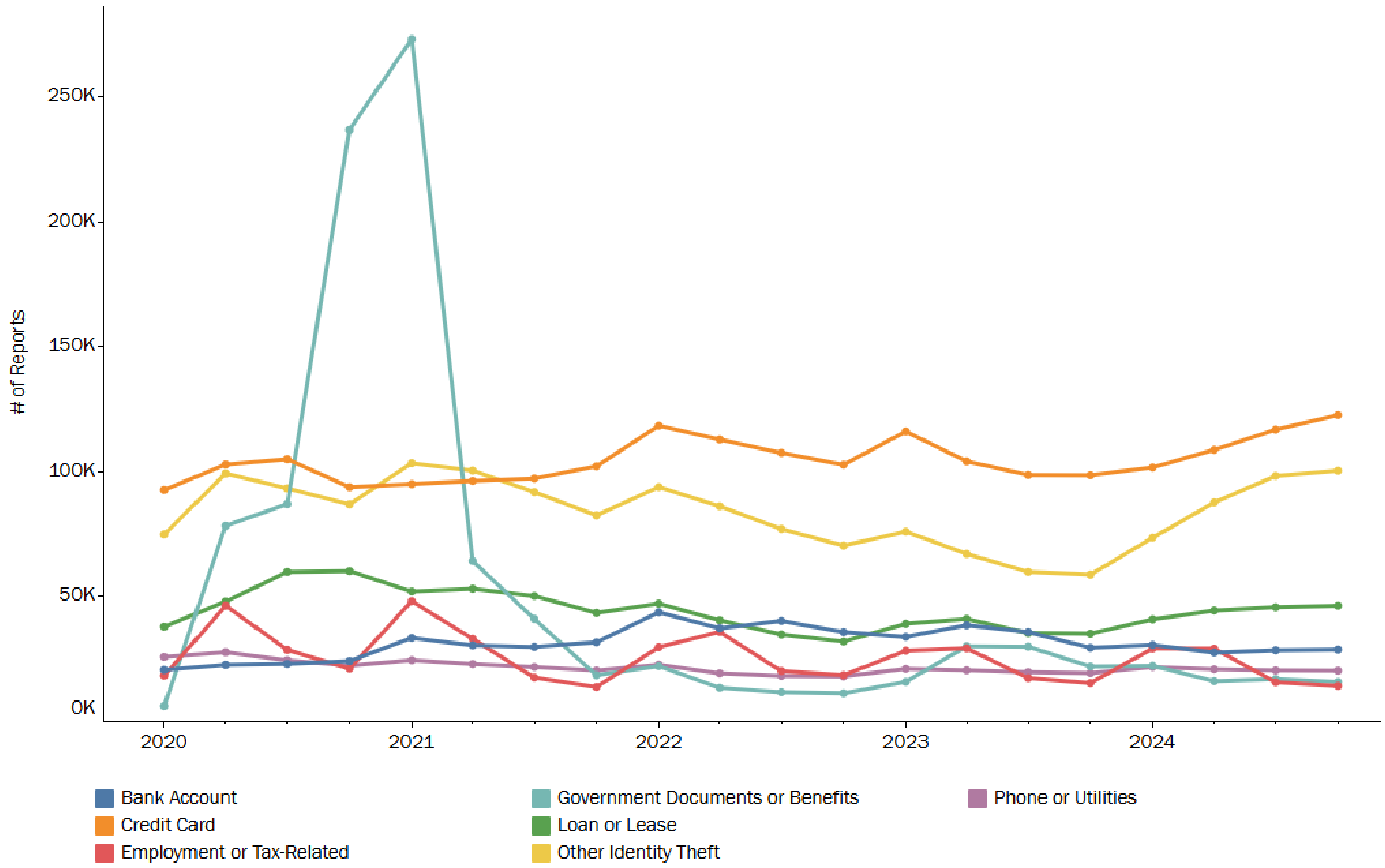
Top Identity Theft type across the USA



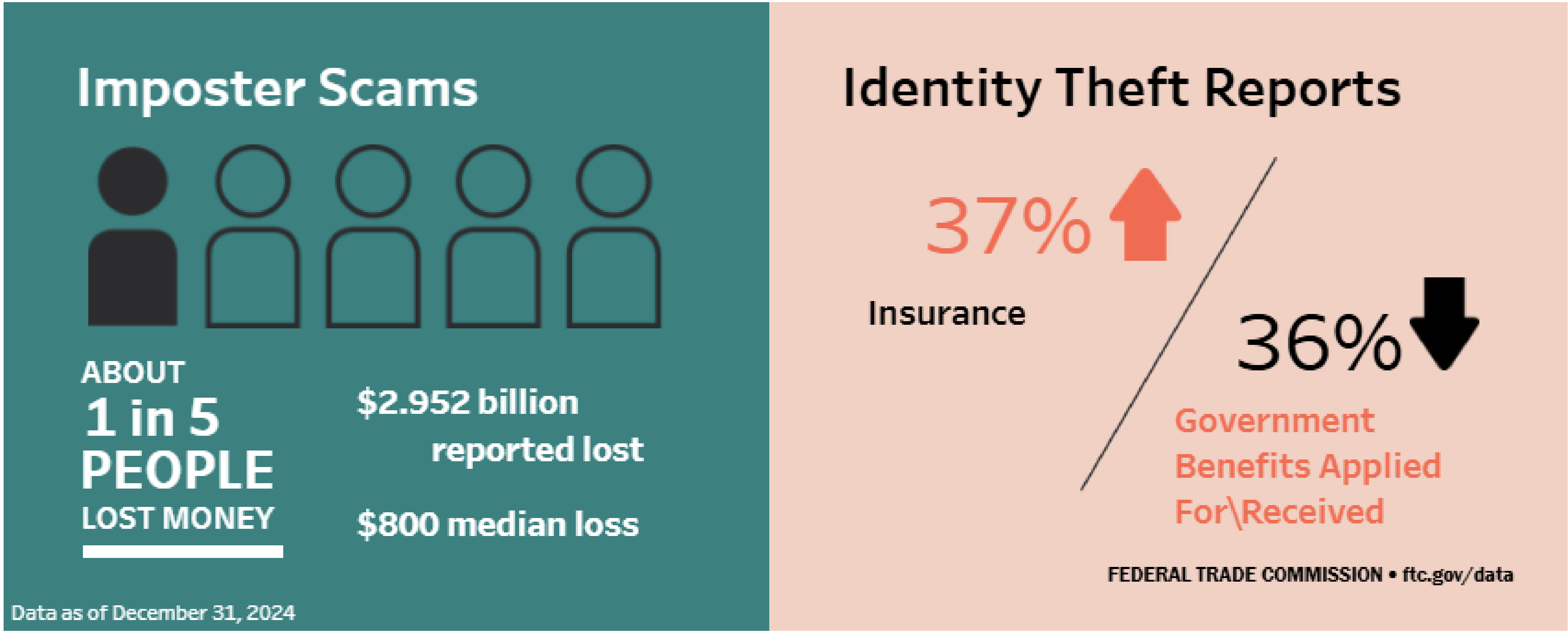
Identity Theft across the USA



Identity Theft trends in the USA

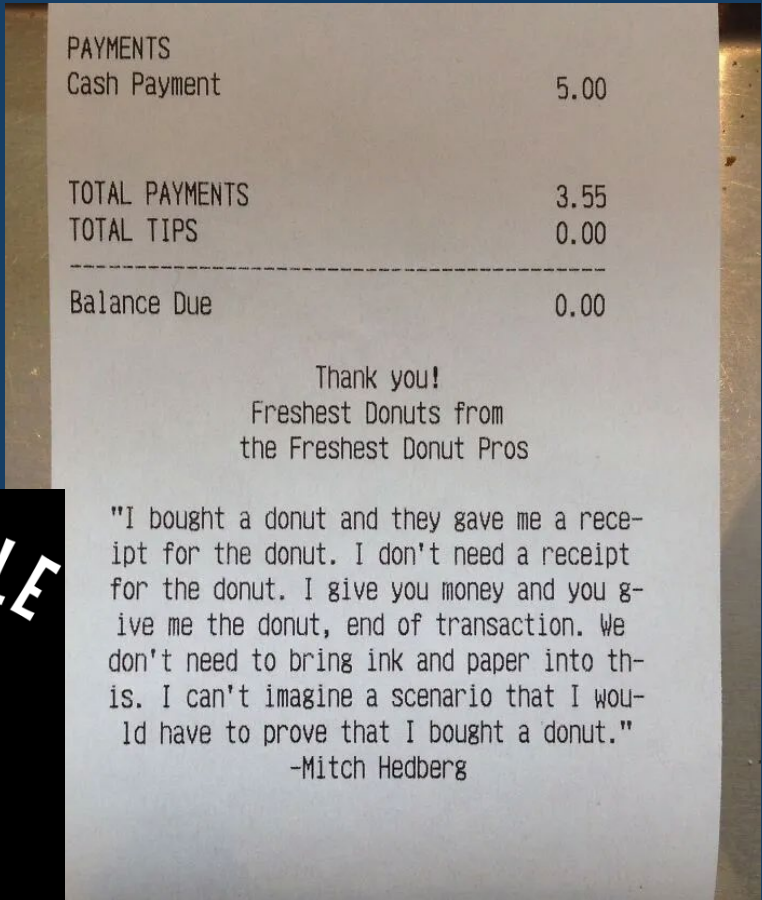


Identity Theft trends in the USA



How much information do you carry with you?

- Driver's License
- Multiple Credit Cards or Receipts
- Social Security Card
- Checkbook or Blank Check
- Work or Picture ID
- Medical Bills
- List of Passwords
- Birth Certificate
- Mail
- House Key
- Family Picture
- Insurance Card



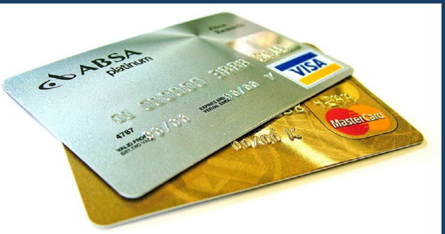
PAYMENTS
Cash Payment 5.00

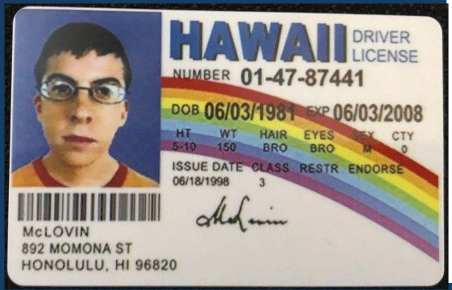
TOTAL PAYMENTS 3.55
TOTAL TIPS 0.00

Balance Due 0.00

Thank you!
Freshest Donuts from
the Freshest Donut Pros

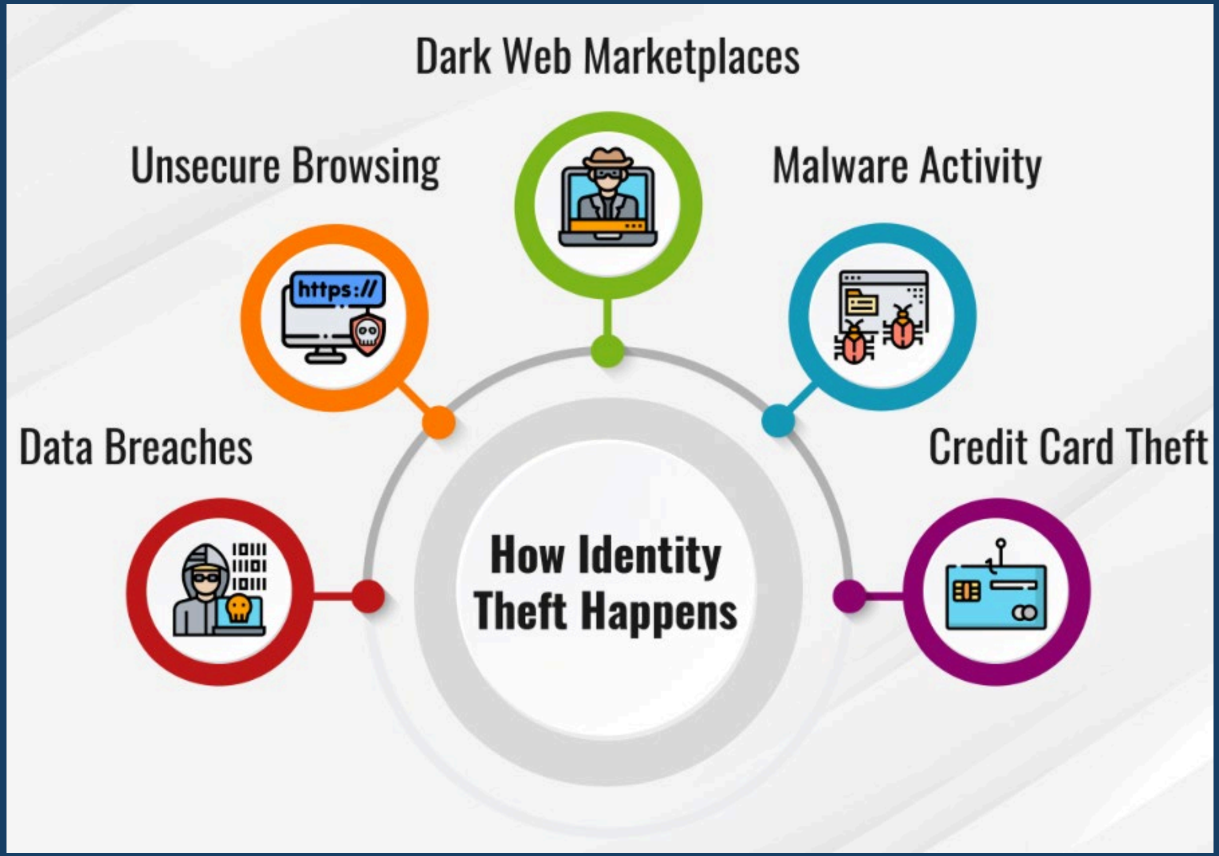
"I bought a donut and they gave me a rece-
ipt for the donut. I don't need a receipt
for the donut. I give you money and you g-
ive me the donut, end of transaction. We
don't need to bring ink and paper into th-
is. I can't imagine a scenario that I wou-
ld have to prove that I bought a donut."
-Mitch Hedberg





Identity Theft

- More than a million reports of identity theft were made to the Federal Trade Commission (FTC) in 2023, making it the number 1 type of fraud.
- Less is more when it comes to what's in your wallet because criminals have begun creating synthetic identities, a fast-growing form of fraud..



Synthetic Identities: A Growing Threat

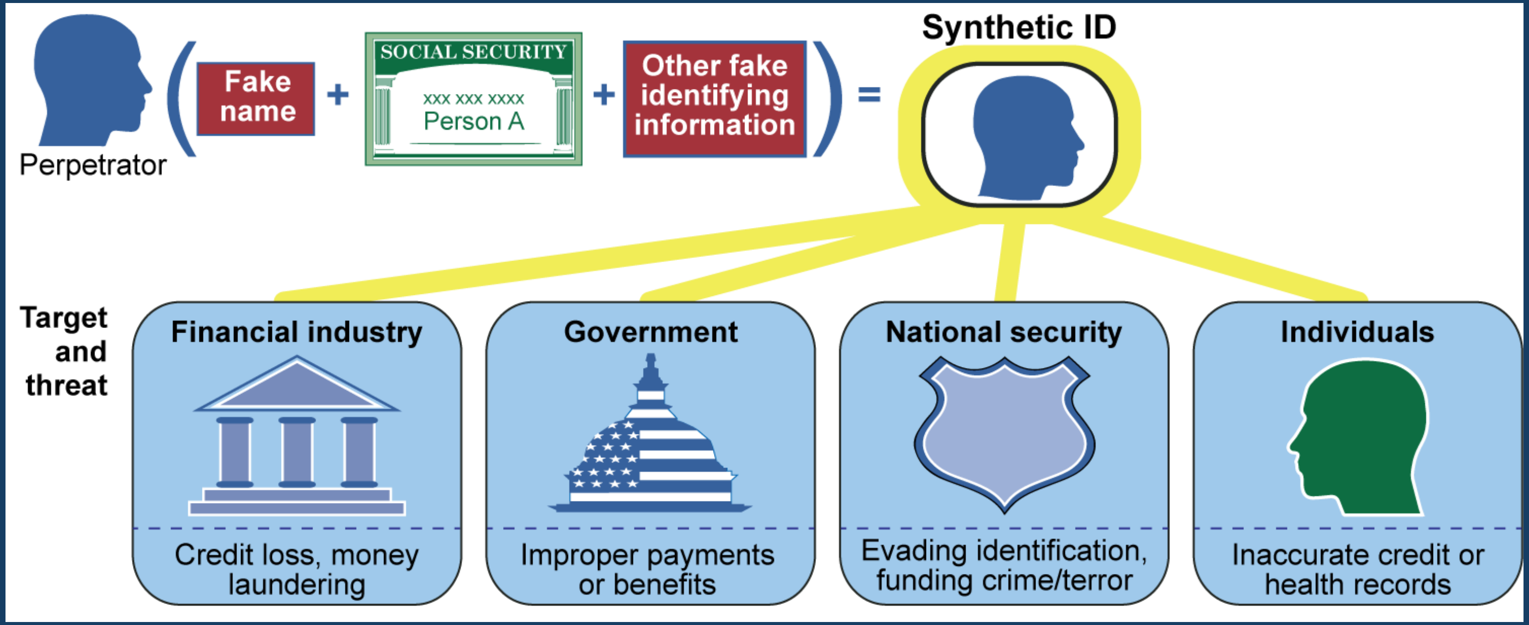
Here's how they operate:

They combine this information with fake information to build a new identity, making synthetic identity fraud difficult to detect. Criminals will often "incubate" identity information and upload and sell it on the dark web, hard-to-access portions of the internet where illicit transactions can occur. Then it can be used by another criminal to perpetrate fraud. Once a synthetic identity is in place, criminals can create accounts in your name.

Synthetic Identities: A Growing Threat

Here's how they operate:

It could be a year or more before a fraudulent account is created and longer before the criminal "busts out" with stolen funds, catching victims off guard and wondering when and where their information was compromised.



Synthetic Identities: A Growing Threat

- **Track what bills you owe and when they're due.** If you stop getting a bill, that could be a sign that someone changed your billing address.
- **Review your bills.** Charges for things you didn't buy could be a sign of identity theft. So could a new bill you didn't expect.
- **Check your bank account statement.** Withdrawals you didn't make could be a sign of identity theft.
- **Get and review your credit reports.** Accounts in your name that you don't recognize could be a sign of identity theft.

What you can do to detect identity theft

Visit

IdentityTheft.gov

FEDERAL TRADE COMMISSION

IdentityTheft.gov

Pass it On

- Start a conversation
- Share what you know, your strategies and ideas
- Get more information at **ftc.gov/PassItOn**

Report it:

- **ReportFraud.ftc.gov**
- 1-877-FTC-HELP

Richard Bryant
Interim Executive Director
Richard.Bryant@ky.gov
(502) 330-8676

Kentucky Financial
Empowerment Commission

Kentucky Bank On
Network

https://www.kyfec.org

Thank You For Attending! Your Feedback is Greatly Appreciated!

Thank you!

Kentucky Financial
Empowerment Commission

Kentucky Financial Empowerment Commission

Richard Bryant
Interim Executive Director
Richard.Bryant@ky.gov
502-330-8676
https://www.kyfec.org