#### **Scams Against Americans**

Wednesday, March 6 2:00 PM – 3:00 PM ET



#### **Today's Speakers**

- Mel Lanning Trumpower, Executive Director, BBB Institute for Marketplace Trust
- Patricia Poss, Senior Attorney, Bureau of Consumer Protection, Federal Trade Commission
- Alvaro Puig, Consumer Education Specialist, Division of Consumer and Business Education, Federal Trade Commission
- Gauri Sharma, Vice President, Professional Certifications, American Bankers Association
- Samuel Kunjukunju, Vice President, Consumer Education, ABA Foundation



#### **Agenda**



**BBB Report** 

Riskiest scams



**FTC Data** 

Consumer Sentinel Network



Resources

ABA Certifications & ABA Foundation Programs



Q&A

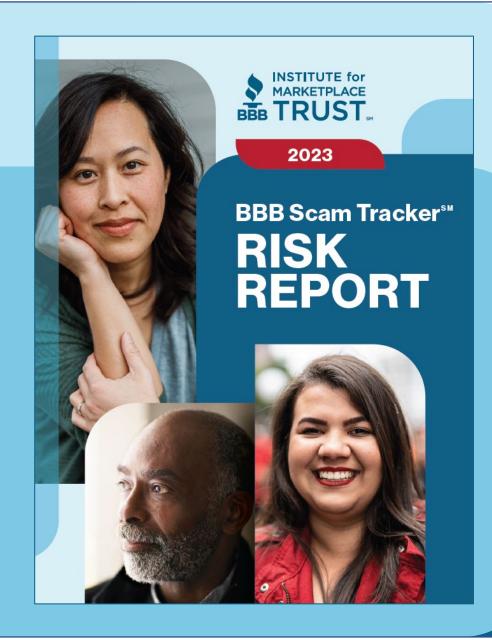
We want to hear from you!



#### **Housekeeping Announcements**

- Webinar is being recorded.
- Slides and recording will be emailed.
- Ask questions via the chat.
- We'll get to questions at the end!





#### 2023 BBB Scam Tracker Risk Report

**Key Findings** 



### **BBB Institute for Marketplace Trust**

## Better Business Bureau's 501(c)(3) educational foundation:

- ✓ Marketplace research
- ✓ Consumer education
- ✓ Fraud prevention programs
- ✓ Business programs



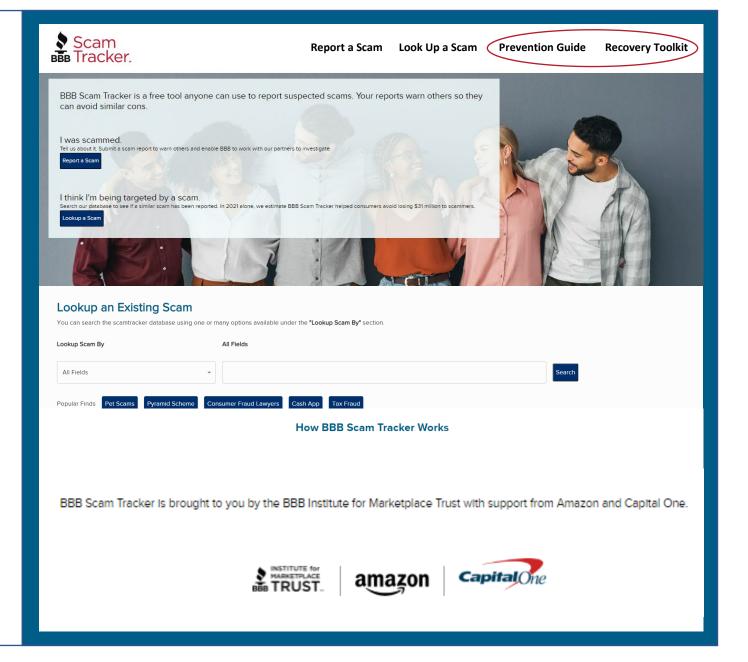


A consumer prevention and reporting platform:

- ✓ Search scams.
- ✓ Report scams

BBB.org/ScamTracker







#### **BBB Risk Index**





- #1 Investment/cryptocurrency
- #2 Employment
- #3 Online purchase (shopping)
- #4 Home improvement
- #5 Romance
- #6 Advance fee loan
- #7 Phishing/social engineering
- #8 Credit repair/debt relief
- #9 Tech support
- #10 Travel/vacation/timeshare

### 10 Riskiest Scams in 2023



## #1 Riskiest: Investment/ Cryptocurrency Scams

- **#1** riskiest for ages 45+
- **#2** for ages 25-44
- \$3,800 median dollar loss
- 80.4% reported losing money when targeted





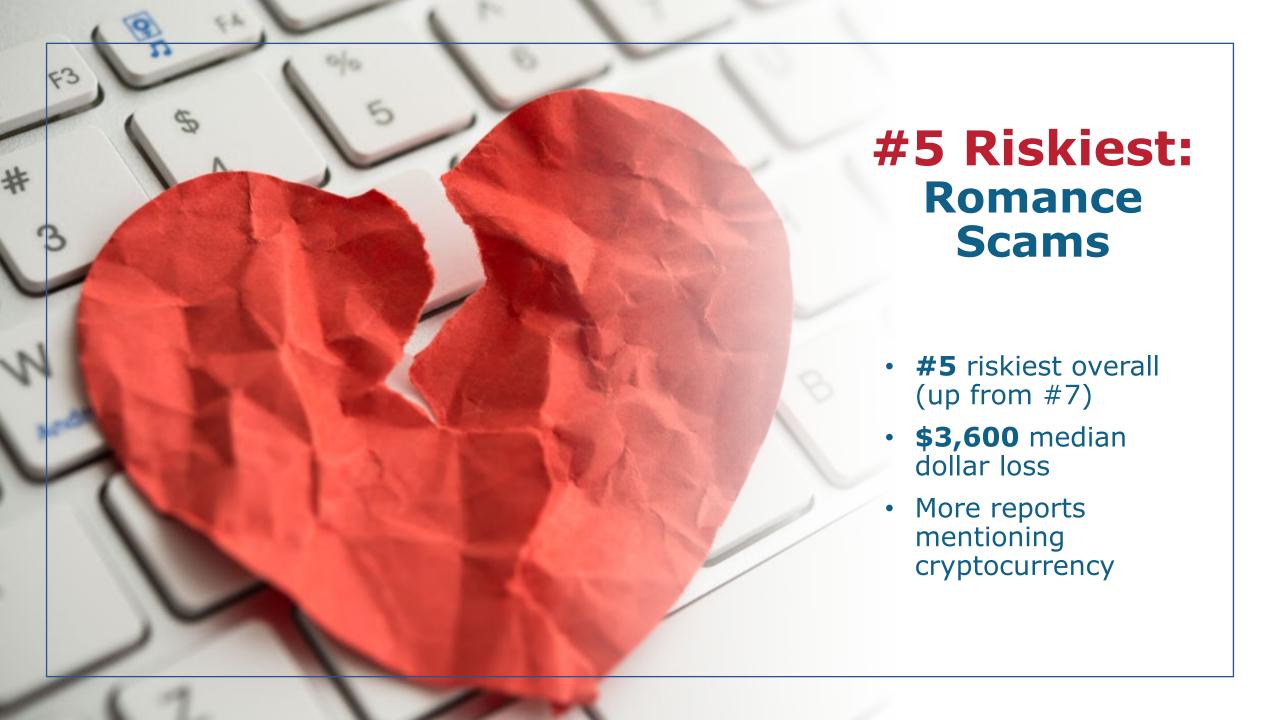
- #1 riskiest for ages 18-44
- #2 riskiest for ages 45-54
- \$1,995 median dollar loss (up from \$1,500)

## #3 Riskiest: Online Purchase (Shopping) Scams

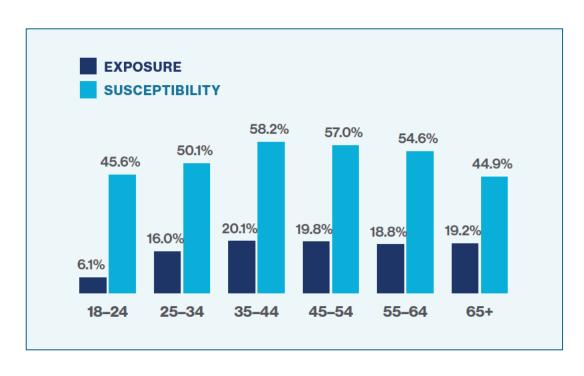
- #2 riskiest for ages 18-24 and 55-64
- Make up 41.9% of all reports to BBB Scam Tracker
- 82.6% reported losing money to this scam type







#### **Demographics: Age**







#### Demographics: Age

	18–24	25-34	35-44	45-54	55-64	65+
1	Employment	Employment	Employment	Investment/ cryptocurrency	Investment/ cryptocurrency	Investment/ cryptocurrency
2	Online purchase	Investment/ cryptocurrency	Investment/ cryptocurrency	Employment	Online purchase	Romance
3	Investment/ cryptocurrency	Online purchase	Online purchase	Online purchase	Home improvement	Home improvement



### **Highlights: Contact Method**

- Scams perpetrated online increased to 68.4% of all scam types (up from 56.5%)
- Top three contact methods:
  - Social media (29.3%)
  - Website (28.9%)
  - o **Email** (18.5%)



## Highlights: Payment Method

- Payment types with highest median \$ loss:
  - Wire transfer (\$8,000)
  - Cryptocurrency (\$3,300)
  - o Check (\$2,625)
- Most reported payment methods with a \$ loss:
  - Credit card
  - Bank account debit
  - Online payment system

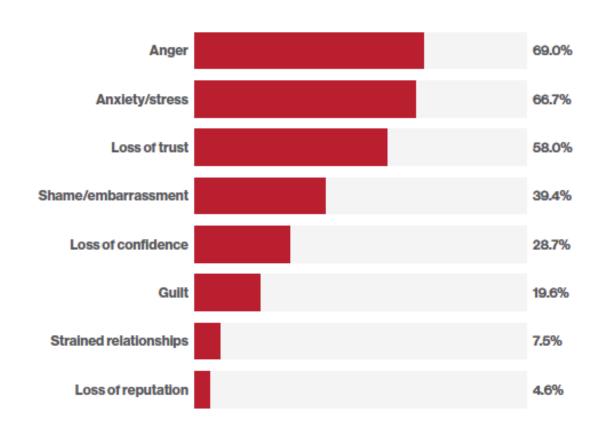


#### **Impersonated Organizations**

<	1	U.S. Postal Service	804	11	Better Business Bureau				
	2	Amazon	606	12	Bed Bath & Beyond				
	3	Publishers Clearing House	536	13	IRS				
	4	Geek Squad	430	14	Medicare				
	5	Norton	387	15	Advance America				
	6	PayPal	384	16	Macy's				
	7	Microsoft	206	17	Spectrum				
	8	Walmart	198	18	Best Buy				
	9	Facebook	189	19	Capital One				
	10	McAfee	188	20	Lending Club				



#### **Top Emotions**



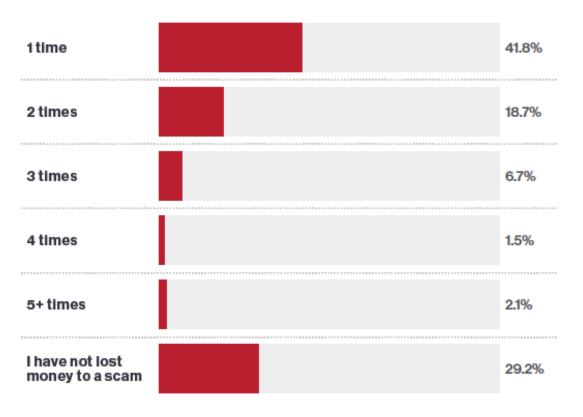
Anxiety/stress top emotions for ages 18-44

**Anger** top emotion for ages 44+



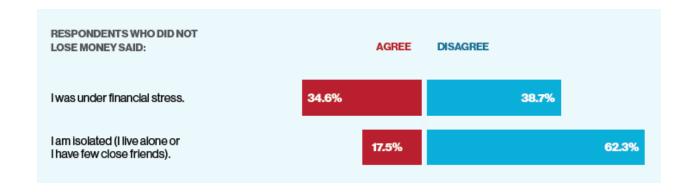
#### **Repeat Victimization**

Number of times respondents reported losing money



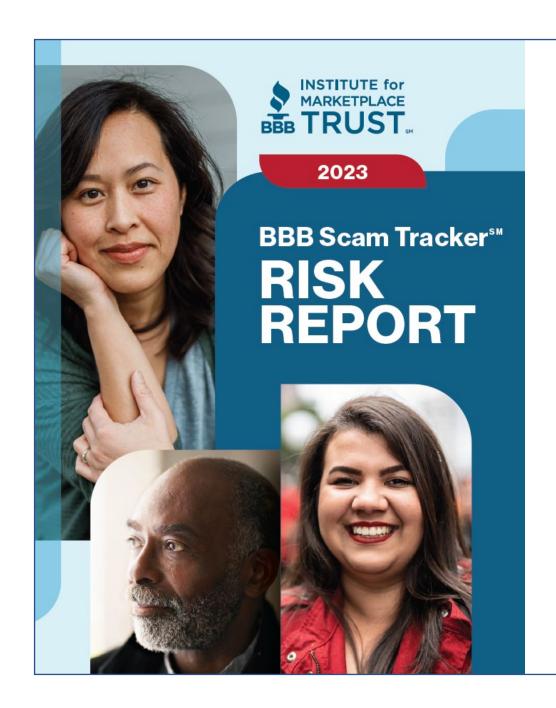


#### **Other Factors Impacting Susceptibility**









#### Thank you!



Melissa Lanning Trumpower mlanning@iabbb.org

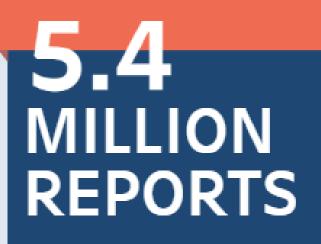
BBBMarketplaceTrust.org/RiskReport



## Top Consumer Protection Issues & FTC Resources

Patti Poss | Alvaro Puig Bureau of Consumer Protection, FTC March 6, 2024 CONSUMER
SENTINEL
NETWORK
DATA BOOK 2023

**SNAPSHOT** 



#### **TOP THREE CATEGORIES**

- 1 Identity Theft
- 2 Imposter Scams
- 3 Credit Bureaus, Info Furnishers and Report
  Users

2.6 million fraud reports

27% reported a loss

\$10.0 billion total fraud losses

\$500 median loss

ftc.gov/databook









Online shopping and negative reviews



Prizes, sweepstakes, lotteries



4 Investments



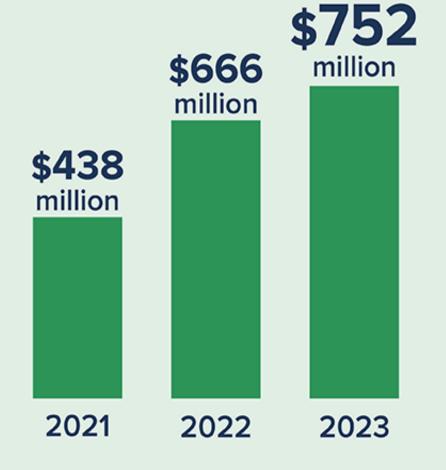
**5**Business and job opportunities

ftc.gov/scams



Losses to business imposters climbed.

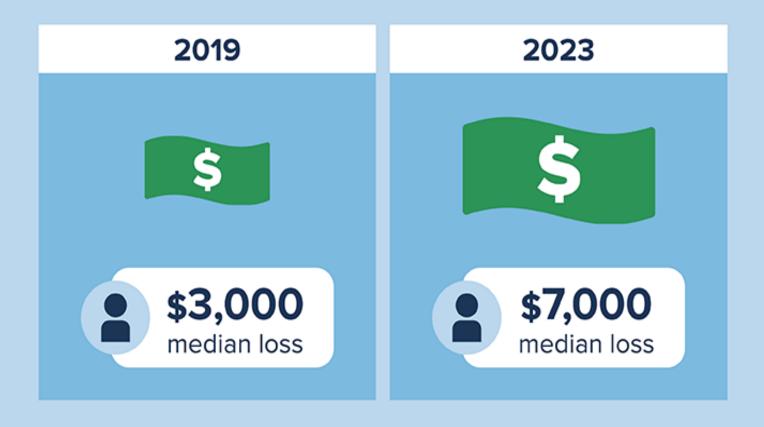




ftc.gov/scams



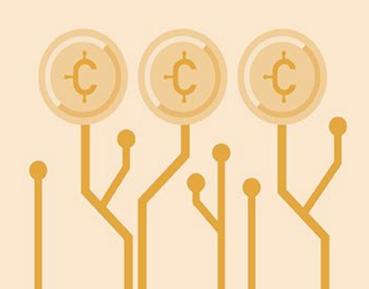
Losses to FTC imposters soared.

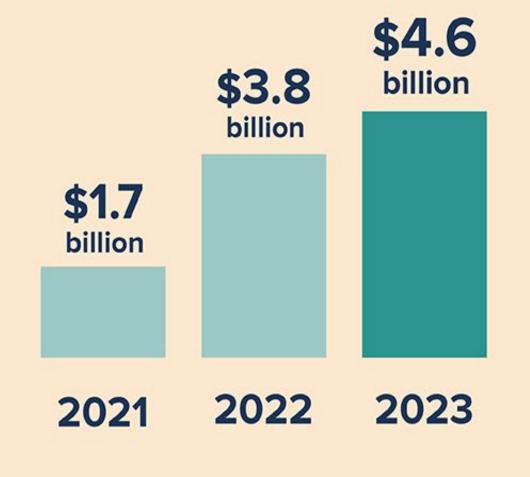


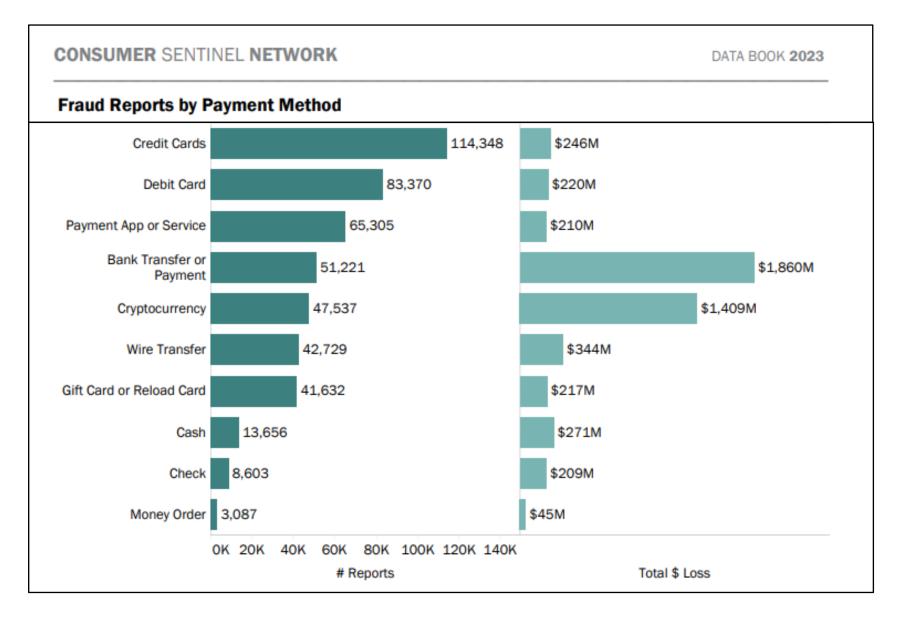
ftc.gov/scams



Reported losses to investment scams **grew**.







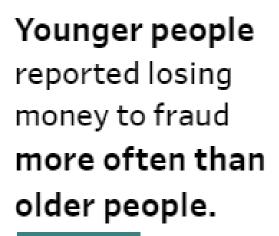


# Top Payment Methods

#### Older Adults and Fraud



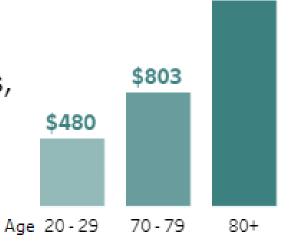
\$1,450



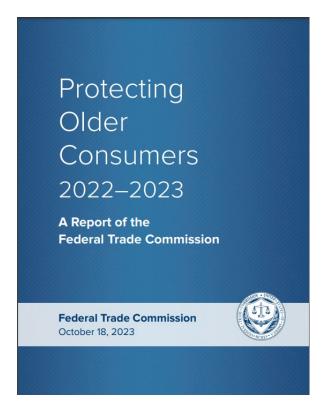




But when people aged 70+ had a loss, the median loss was much higher.



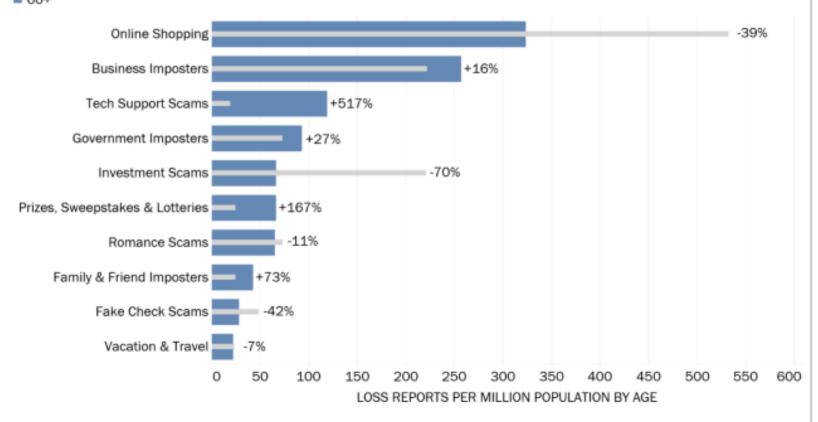
#### Annual Report



#### FIGURE 3: 2022 LOSS REPORTS BY AGE AND FRAUD TYPE

Older and younger consumers differ on loss reporting rates by fraud type. Percentages indicate the difference in the loss reporting rates for each fraud type by older adults as compared to consumers ages 18-59.





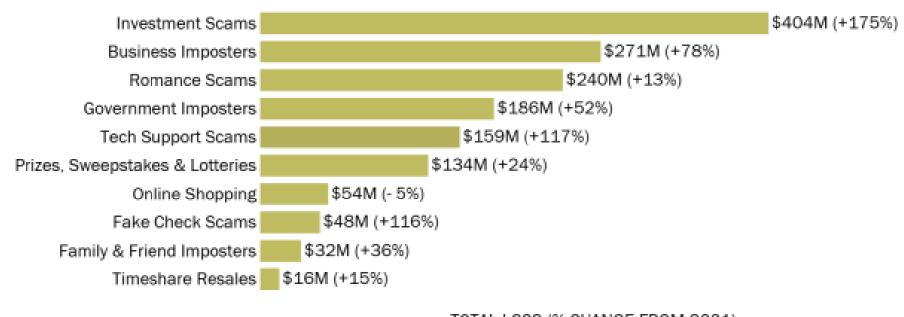
Fraud types are ranked by the number of loss reports filed by consumers 60 and over. Figures are normalized using U.S. Census Bureau data for population by age. See U.S. Census Bureau, 2017-2021 American Community Survey 5-Year Estimates. Reports categorized as unspecified and reports provided by IC3 are excluded.

#### Annual Report



#### FIGURE 4: 2022 TOP FRAUD TYPES BY TOTAL DOLLARS LOST (AGES 60 AND OVER)

Reports suggest that some fraud types are far more costly in aggregate than others, and losses to a number of fraud types soared from 2021 to 2022.



TOTAL LOSS (% CHANGE FROM 2021)

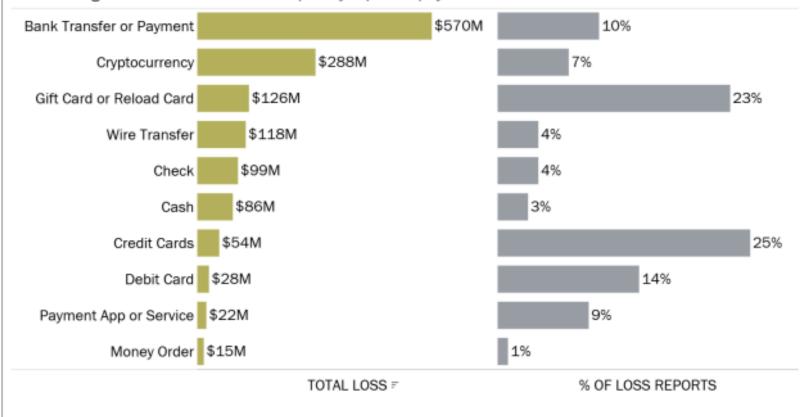
Percent change from 2021 is shown in parentheses. Reports categorized as unspecified and reports provided by IC3 are excluded.

#### Annual Report



#### FIGURE 6: 2022 TOTAL LOSSES AND LOSS REPORTS BY PAYMENT METHOD (AGES 60 AND OVER)

Bank transfers and payments and cryptocurrency were highest on total reported dollar losses, but credit cards and gift cards were the most frequently reported payment methods.



Reports that did not indicate a payment method and other payment methods consumers wrote in were excluded.



#### Anatomy of an Imposter Scam









Suspicious Charge on Amazon Robocall Scam

Scammers say they're from Amazon, calling about a suspicious transaction

- Don't trust the caller ID. Scammers spoof their number.
- Worried? Log in to your account.





**Scammers say** we discovered fraudulent accounts in your name

- Get your free credit report
  - AnnualCreditReport.com

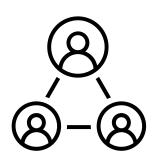




Scammers say we'll connect you to someone who's going to help you

- Call your real bank, broker, or investment advisor if you're worried
  - Use a number you know is real





**Scammers say,** "Don't trust anyone. They're in on the scam."

- No one legitimate will tell you to keep a secret
- Talk with someone you trust





**Scammers say** you have to transfer your money to protect, safeguard, or legalize it

- Never move or transfer your money to "protect it"
- Only a scammer will tell you to do that





**Scammers say** to deposit money in a gov't Bitcoin account, wallet, or federal safety locker

### **Advice for consumers**

 Nobody legit will ever insist you get cryptocurrency of any kind





Scammers say to buy gold and drop it off with someone

### **Advice for consumers**

Only a scammer will tell you to buy gold





**Scammers say** to buy gift cards and give them the PIN

### **Advice for consumers**

 Never buy gift cards because someone tells you to

## What can banks do to disrupt fraud?



- Know the latest scams
- Share information about scams
- Train employees
- Develop relationships with law enforcement



## Resources

## ftc.gov/scams

#### **How to Avoid a Scam**



#### Four Signs That It's a Scam





Scammers often pretend to be contacting you on behalf of the government. They might use a real name, like the FTC, Social Security Administration, IRS, or Medicare, or make up a name that sounds official. Some pretend to be from a business you know, like a utility company, a tech company, or even a charity asking for donations.

They use technology to change the phone number that appears on your caller ID. So the name and number you see might not be real.

#### 2 Scammers say there's a PROBLEM or a PRIZE.



They might say you're in trouble with the government. Or you owe money. Or someone in your family had an emergency. Or that there's a virus on your computer. Some scammers say there's a problem with one of your accounts and that you need to verify some information.

Others will lie and say you won money in a lottery or sweepstakes but have to pay a fee to get it.

#### 3 Scammers PRESSURE you to act immediately.

Scammers want you to act before you have time to think. If you're on the phone, they might tell you not to hang up so you can't check out their story.

They might threaten to arrest you, sue you, take away your driver's or business license, or deport you. They might say your computer is about to be corrupted.

#### 4 Scammers tell you to PAY in a specific way.



They often insist that you can only pay by using cryptocurrency, wiring money through a company like MoneyGram or Western Union, using a payment app, or putting money on a gift card and then giving them the numbers on the back of the card.

Some will send you a check (that will later turn out to be fake), then tell you to deposit it and send them money.



#### What To Do if You Were Scammed







Find out what to do if you paid someone you think is a scammer, or if you gave a scammer your personal information or access to your computer or phone.

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. And they're good at what they do. Here's what to do if you paid someone you think is a scammer or gave them your personal information or access to your computer or phone. If you paid a scammer, your money might be gone already. No matter how you paid, it's always worth asking the company you used to send the money if there's a way to get it back.

If You Paid a Scammer	
Did you pay with a credit card or debit card?	Contact the company or bank that issued the <u>credit card</u> or <u>debit card</u> . Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.
Did a scammer make an unauthorized transfer from your bank account?	Contact your bank and tell them it was an <u>unauthorized debit or</u> <u>withdrawal</u> . Ask them to reverse the transaction and give you your money back.
Did you pay with a gift card?	Contact the company that issued the <u>gift card</u> . Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.
Did you send a wire transfer through a company like Western Union or MoneyGram?	Contact the <u>Wire transfer</u> company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.  • MoneyGram at 1-800-926-9400  • Western Union at 1-800-448-1492  • Ria (non-Walmart transfers) at 1-877-443-1399  • Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144
Did you send a wire transfer through your bank?	Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.
Did you send money through a money transfer app?	Report the fraudulent transaction to the company behind the <u>money transfer app</u> and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

## ftc.gov/languages





## For Older Adults



National Consumer Protection Week • March 3-9 #NCPW2024

**NCPW Speaks Your Language** 

Scammers speak the language of *older adults*.

Start a conversation. Help stop scams:

ftc.gov/PassItOn

Grandma, I need money for bail.



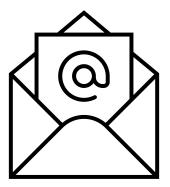
### Free printed publications

- English: ftc.gov/bulkorder
- Spanish: ftc.gov/ordenar



### Free Consumer Alerts by email

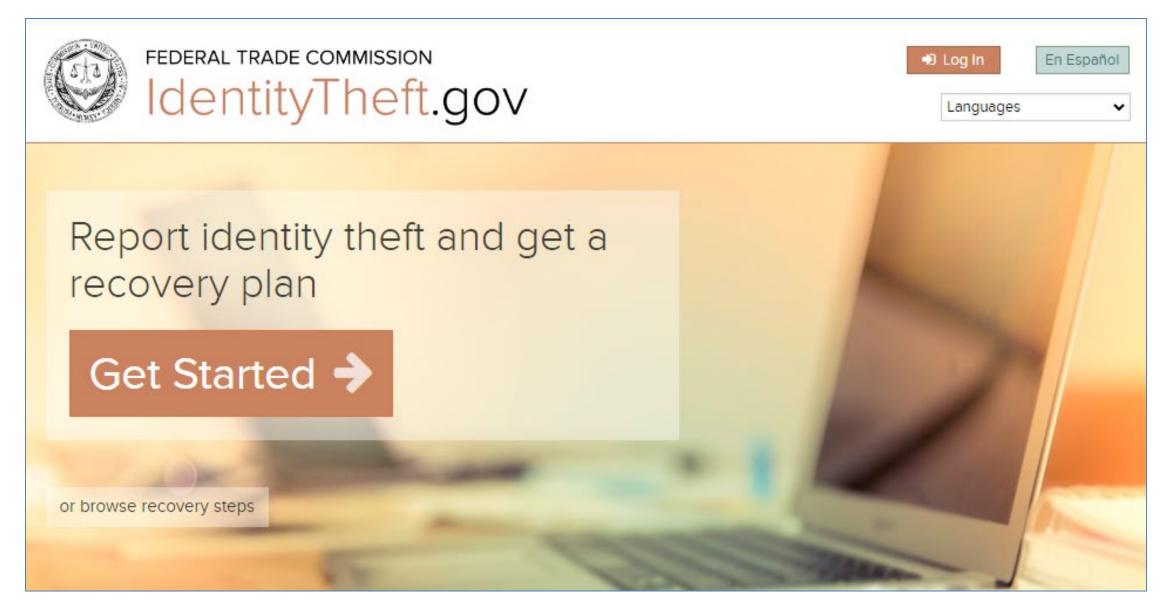
- English: ftc.gov/subscribe
- Spanish: ftc.gov/es/conectese



## ReportFraud.ftc.gov/ReporteFraude.ftc.gov



## IdentityTheft.gov/Robodeidentidad.gov





## Contacts

Patti Poss pposs@ftc.gov Alvaro Puig apuig@ftc.gov

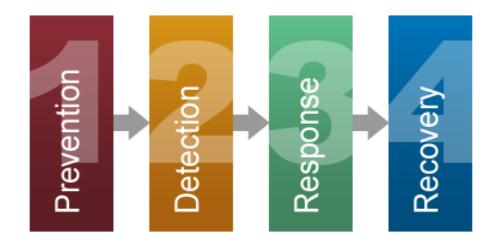
## **ABA Training Resources for Bankers**



## **ABA Online Certificates**

### **Certificate in Fraud Prevention**

- Introduction to Fraud Management
- Establishing a Fraud Prevention Program
- Types of Fraud and Prevention Strategies
- Operating a Fraud Prevention Program
- Maintaining a Compliant Fraud Prevention Program





## **ABA Online Certificates**

## **Certificate in BSA and AML Compliance**

- Introduction to BSA/AML
- Components of an AML Compliance Program
- SARs and Information Sharing
- Currency and Correspondent Banking Accounts
- Electronic Banking and Funds Transfer Activities
- Higher Risk Accounts and Activities
- BSA Requirements for Business Accounts
- BSA Requirements for Foreign Customers and Accounts
- International Partners in AML Policy
- Office of Foreign Assets Control (OFAC) for Compliance Professionals







## **ABA Financial Crimes Certification**

## **Certified AML and Fraud Professional (CAFP)**

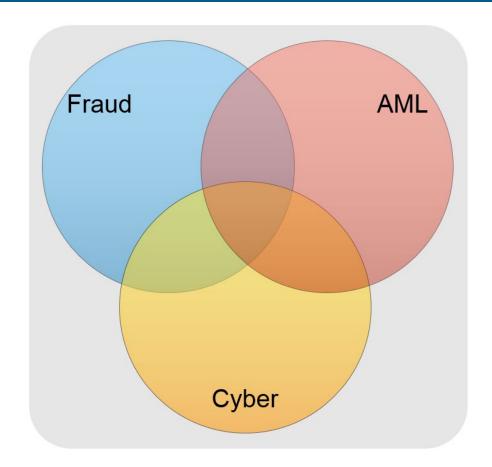




## **CAFP Fills a Specific Industry Need**



- Demonstrates holistic knowledge of the financial crimes lifecycle:
  - AML
  - Fraud
  - Cyber-enabled crime
- Focuses on U.S. banking laws, regulations, and guidance.
- Experienced-based approach demonstrating ability to handle day-to-day situations.





## **ABA Foundation Campaigns**







## Free Financial Education Materials











Facilitator guides

Presentation slides

Handouts

Social graphics

Videos



## Financial Education Programs

**ABA Foundation** 

THE SPIRIT OF BANKING

ABOUT THE FOUNDATION

FINANCIAL EDUCATION PROGRAMS

> Financial Education Webinars

Financial Literacy Programs

COMMUNITY DEVELOPMENT & AFFORDABLE HOUSING

COMMUNITY COMMITMENT AWARDS The ABA Foundation provides financial education programs and resources for bankers to help them strengthen the financial well-being of their communities. Every year, the Foundation works with nearly a thousand banks across the country to jumpstart the financial education of over a half million consumers.

#### **Get Smart About Credit**



Get Smart About Credit is a national campaign of volunteer bankers who work with young people to raise awareness about the importance of using credit wisely.

- List of Participating Banks
- More Get Smart About Credit
- Banks: Free Registration/Update Participation
- Community Members: Request a Presentation

#### Lights, Camera, Save!

Lights Camera Save! is a video contest that engages teens in educating themselves and their peers about the value of saving and using money wisely.





- · List of Participating Banks
- More Lights, Camera, Save!
- Lights, Camera, Save! Consumer Contest Site
- Banks: Free Registration

#### **Safe Banking for Seniors**



Safe Banking for Seniors is a national campaign that helps older customers and their financial caregivers understand and mitigate the risks of fraud and financial abuse.

- List of Participating Banks
- More Safe Banking for Seniors
- Banks: Free Registration/Update Participation
- Community Members: Request a Presentation

Register for free Aba.com/FinEd

### Aba.com/BanksNeverAskThat



**Protect Yourself** 

**Play Scam City** 

Take the Quiz

Watch the Videos

Español



Don't fall for fake. Take action to protect your hard-earned cash against phishing scams.

**TAKE THE QUIZ** 

Learn more



## **Staff Contact**

Sam Kunjukunju

VP, Consumer Education

202-663-5418

Skunjukunju@aba.com



# Thank you!

