
FBI
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

Complex Financial Crimes

Presented by:

Supervisory Special Agent Mary Gleason
Phoenix Field Office/Squad C-4
White Collar Crime
623-466-1014

FBI Priorities

1. Protect the United States from terrorist attack
2. Protect the United States against foreign intelligence operations and espionage
3. Protect the United States against cyber-based attacks and high-technology crimes
4. Combat public corruption at all levels
5. Protect civil rights
6. Combat transnational/national criminal organizations and enterprises
7. Combat major white-collar crime
8. Combat significant violent crime
9. Support federal, state, local and international partners
10. Upgrade technology to successfully perform the FBI's mission

Types of White Collar Crime

- Health Care Fraud
- Corporate Fraud
- Investment (Securities/Commodities) Fraud
- Financial Institution Fraud/Bank Fraud
- Mortgage Fraud
- Mass Marketing Fraud
- Antitrust Matters
- Bankruptcy Fraud
- Credit Card/Check Fraud
- Fraud Against the Government

2022 IC3.gov Data

IC3 BY THE NUMBERS[16]

$10.3 Billion
Victim losses in 2022

2,175+
Average complaints received daily

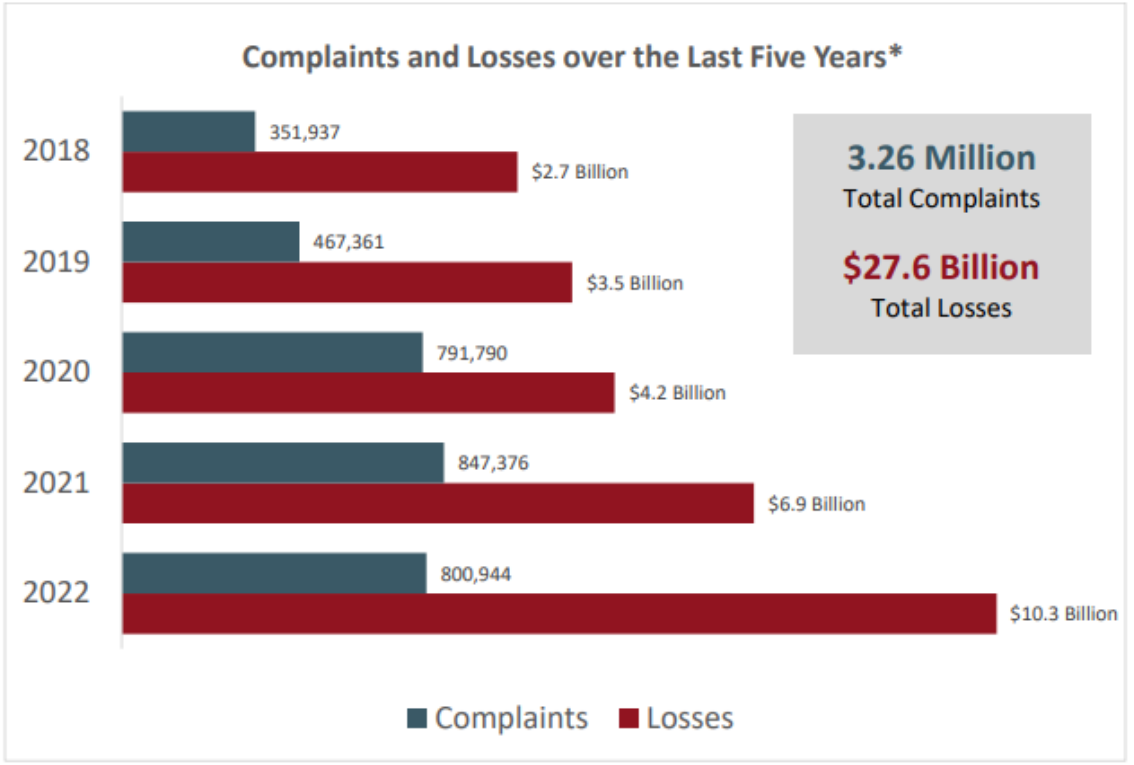
651,800+
Average complaints received per year (last 5 years)

Over 7.3 Million
Complaints reported since inception

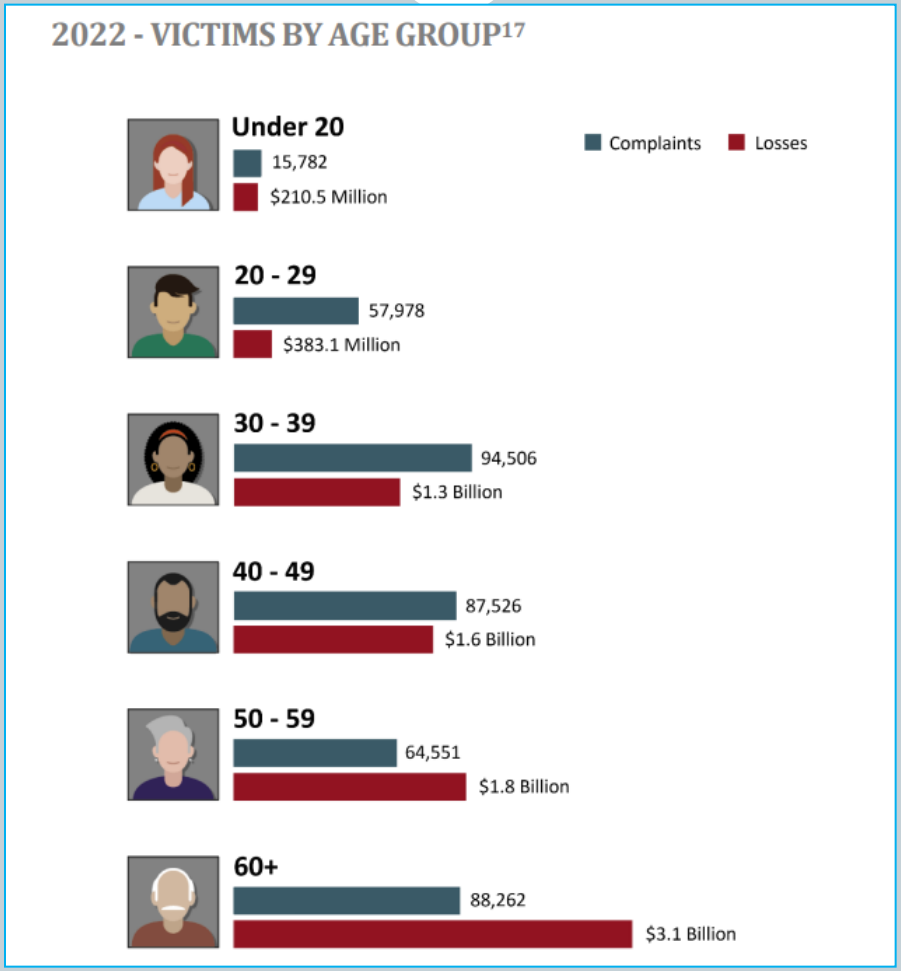
IC3 Complaint Statistics

LAST FIVE YEARS

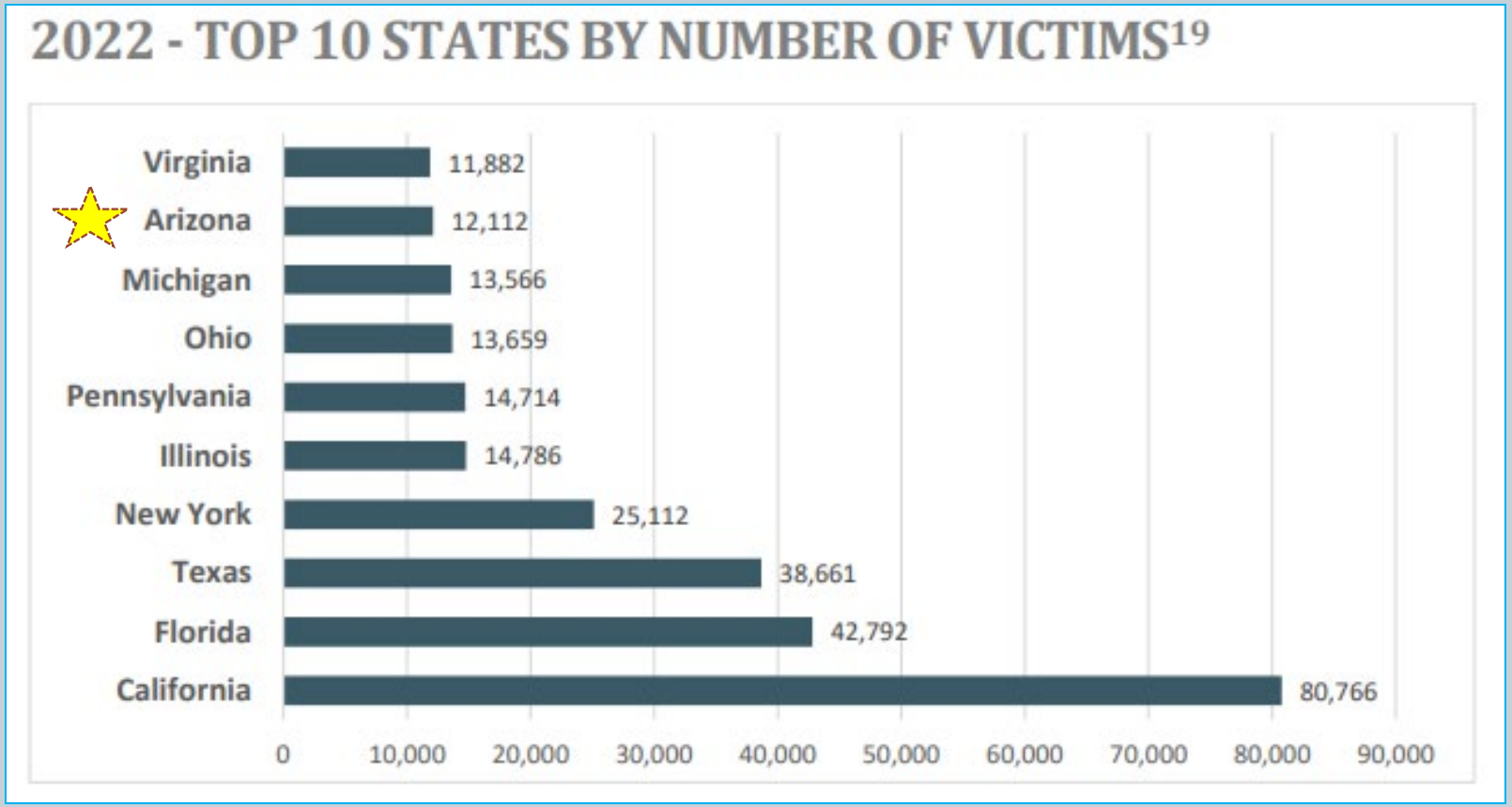
Over the last five years, the IC3 has received an average of 652,000 complaints per year. These complaints address a wide array of Internet scams affecting victims across the globe.[3]



2022 IC3 Data



2022 IC3


2022 - TOP 10 STATES BY NUMBER OF VICTIMS[19]
Virginia
11,882
Arizona
12,112
Michigan
13,566
Ohio
13,659
Pennsylvania
14,714
Illinois
14,786
New York
25,112
Texas
38,661
Florida
42,792
California
80,766
0
10,000
20,000
30,000
40,000
50,000
60,000
70,000
80,000
90,000

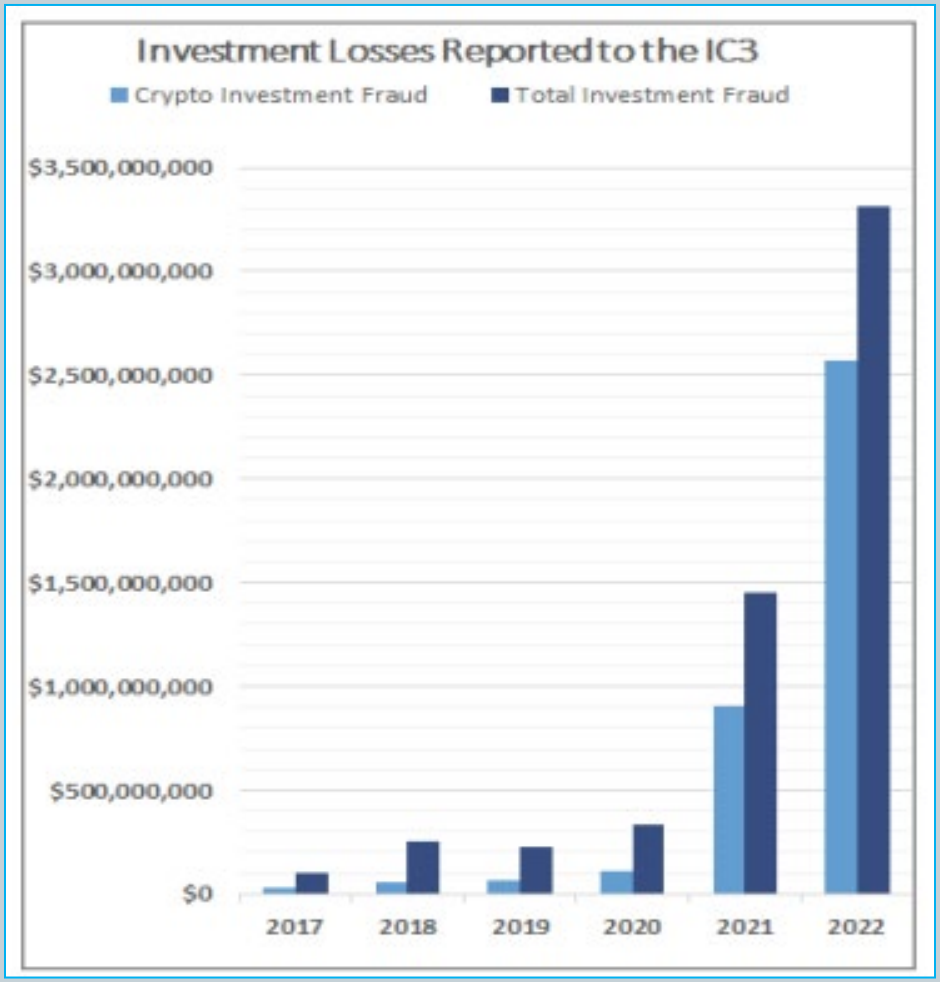
2022 IC3


2022 - TOP 10 STATES BY VICTIM LOSS (IN MILLIONS)[20]
Arizona
$241.1
Alabama
$247.9
Pennsylvania
$250.9
Illinois
$266.7
New Jersey
$284.6
Georgia
$322.6
Texas
$763.1
New York
$777.0
Florida
$844.9
California
$2,012.8
$0
$500
$1,000
$1,500
$2,000
$2,500

IC3 Crime Types

By Victim Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$3,311,742,206	Lottery/Sweepstakes/Inheritance	$83,602,376
BEC	$2,742,354,049	SIM Swap	$72,652,571
Tech Support	$806,551,993	Extortion	$54,335,128
Personal Data Breach	$742,438,136	Employment	$52,204,269
Confidence/Romance	$735,882,192	Phishing	$52,089,159
Data Breach	$459,321,859	Overpayment	$38,335,772
Real Estate	$396,932,821	Ransomware	*$34,353,237
Non-Payment/Non-Delivery	$281,770,073	Botnet	$17,099,378
Credit Card/Check Fraud	$264,148,905	Malware	$9,326,482
Government Impersonation	$240,553,091	Harassment/Stalking	$5,621,402
Identity Theft	$189,205,793	Threats of Violence	$4,972,099
Other	$117,686,789	IPR/Copyright/Counterfeit	$4,591,177
Spoofing	$107,926,252	Crimes Against Children	$577,464
Advanced Fee	$104,325,444		
*Descriptors***			
Cryptocurrency	$2,496,196,530	Cryptocurrency Wallet	$1,349,090,883

IC3 Data


Investment Losses Reported to the IC3
Crypto Investment Fraud
Total Investment Fraud
$3,500,000,000
$3,000,000,000
$2,500,000,000
$2,000,000,000
$1,500,000,000
$1,000,000,000
$500,000,000
$0
2017
2018
2019
2020
2021
2022

Crypto Investment Scams

Potential Signs of a scam:

- Statements of “guaranteed returns” with “no risk”
- Advertised investments include cryptocurrencies and real estate
- Fake testimonials, often from celebrities

FBI Phoenix Success!!

THE UNITED STATES DEPARTMENT of JUSTICE

FOR IMMEDIATE RELEASE
April 3, 2023
www.justice.gov

CRM
202-514-2007
TTY 866-544-5309

Justice Department Seizes Over $112M in Funds Linked to Cryptocurrency Investment Schemes

WASHINGTON – The Department of Justice announced today that it has seized virtual currency worth an estimated $112 million linked to cryptocurrency investment scams.

Seizure warrants for six virtual currency accounts were authorized by judges in the District of Arizona, the Central District of California, and the District of Idaho.

Spear Phishing

- Use of social engineering (via email or phone) to surreptitiously obtain information
- Medicare/doctor's office employee
- Employee from your bank
  - Attempt to obtain account information as well as PII
- Employee from your own company
  - Attempt to obtain sensitive company information

Warning Signs

- Offer sounds too good to be true
- Seller using high pressure sales tactics
- Seller asking for information that is usually considered personal (e.g. social security number, credit card information, etc.)
- Investment offer unsolicited

Tips to Protect Yourself

Things you should do:

- Insist on learning full name, address, contact info, etc.
- Insist that all information is sent in writing
- Research all solicitors through BBB, state AG's office, and/or consumer protection service
- Register with the FTC's "Do Not Call" registry
- Only give out your personal info when necessary
- Regularly check your credit with one or more of the three credit reporting agencies
- Properly dispose of documents which contain PII (e.g., shred instead of throwing in trash)

Tips to Protect Yourself cont'd

Things you should NOT do:

- Do NOT make any payments to either secure a prize or improve your chances of winning a prize
- Do NOT be intimidated into making hasty financial decisions by high-pressure sales tactics
- Do NOT provide anyone with your sensitive personal or financial information
- Do NOT deposit checks and wire back any fees using the check proceeds until the checks have fully cleared
- Do NOT be lured by offers that are simply too good to be true … they almost certainly are

Close, but no cookie…
Can you spot the difference?

- CUSTOMERSERVICE@AMAZON.COM
- CUSTOMERSERVICE@AMAZoN.COM
  - There is a zero instead of an O in the word Amazon in the second email address

- customercomplaintdepartment@apple.com
- customercompliantdepartment@apple.com
  - Transposed the I and the A in the second email

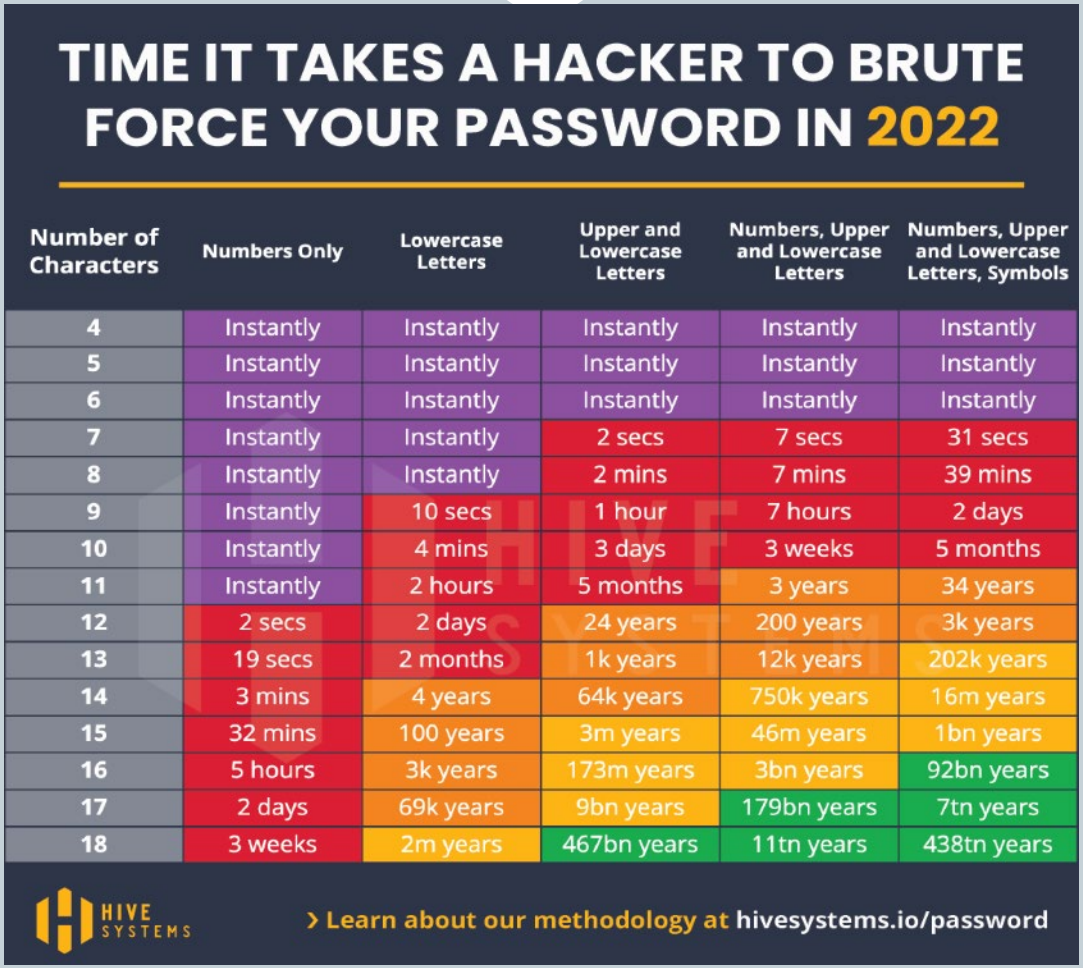
- returndepartment@WaImart.com
- returndepartment@Walmart.com
  - In the first email, there is an uppercase I instead of an L in the word Walmart

What Can You Do?

PASSWORD DISCIPLINE

- **Use long passwords**
- **Don’t reuse passwords for more than one account**
- **Consider changing passwords frequently**
- **Consider using a Password Manager**

Prevention Tip: Create Strong, Unique Passwords



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

Review and Monitor Financial Statements

Under federal law, each credit bureau is required to provide consumers

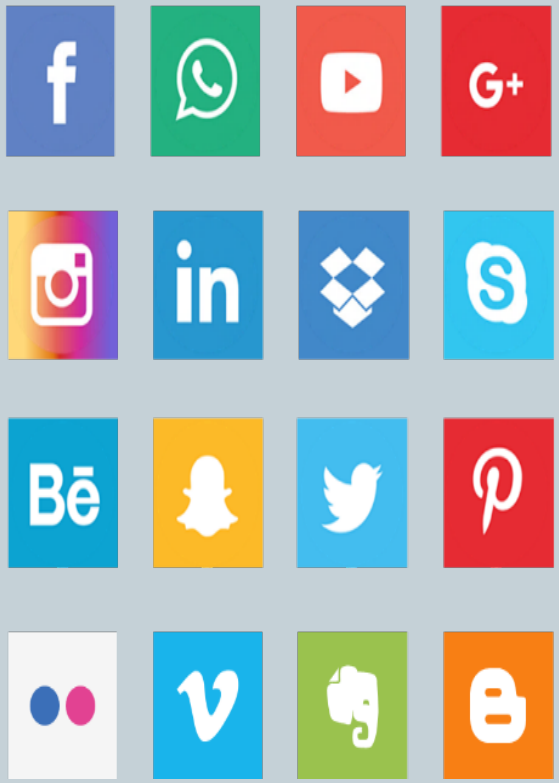
one free report

each year

AnnualCreditReport.com

1-877-322-8228

Be mindful with Social Media



- Keep accounts private and review connections
- Be wary when sharing personal information
- Check app settings

If you Are a Victim

WHAT TO DO IF YOU ARE A VICTIM

Immediately contact your bank and initiate a recall.

Contact your local FBI Office, 800-CALL-FBI.

Report it to www.ic3.gov

Change email passwords and check your email account for any changes to your mailbox rules, such as Mail Forward, Delete, CC, or BCC.

Change all e-banking and/or other pertinent passwords.

National Elder Fraud Hotline

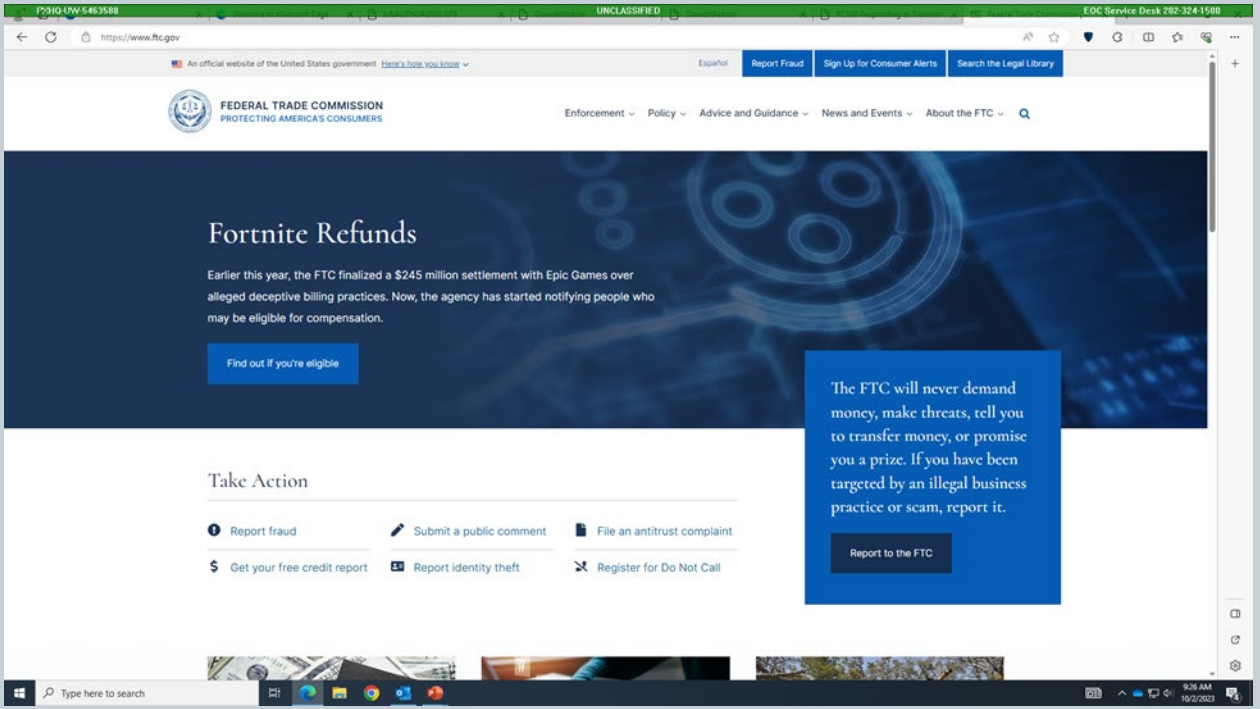
The National Elder Fraud Hotline aids victims of elder fraud. This hotline is staffed by professionals who know how to support victims of fraud. Case managers will help victims through the reporting process at the federal, state, and local levels.

To reach the National Elder Fraud Hotline, call:

833-FRAUD-11

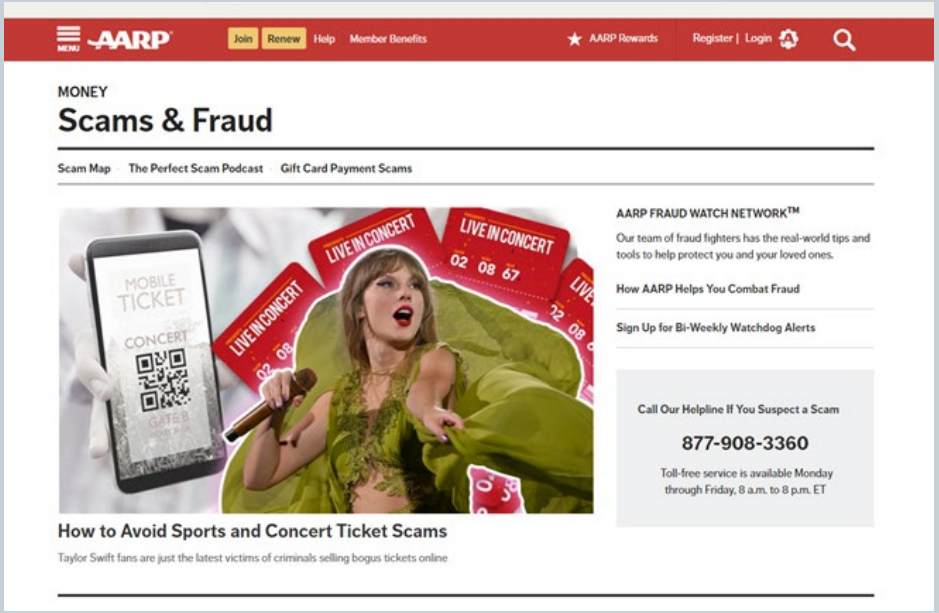
Federal Trade Commission

The Federal Trade Commission website features a page that provides information on what to do if you get scammed. www.ftc.gov



AARP Fraud Watch Network

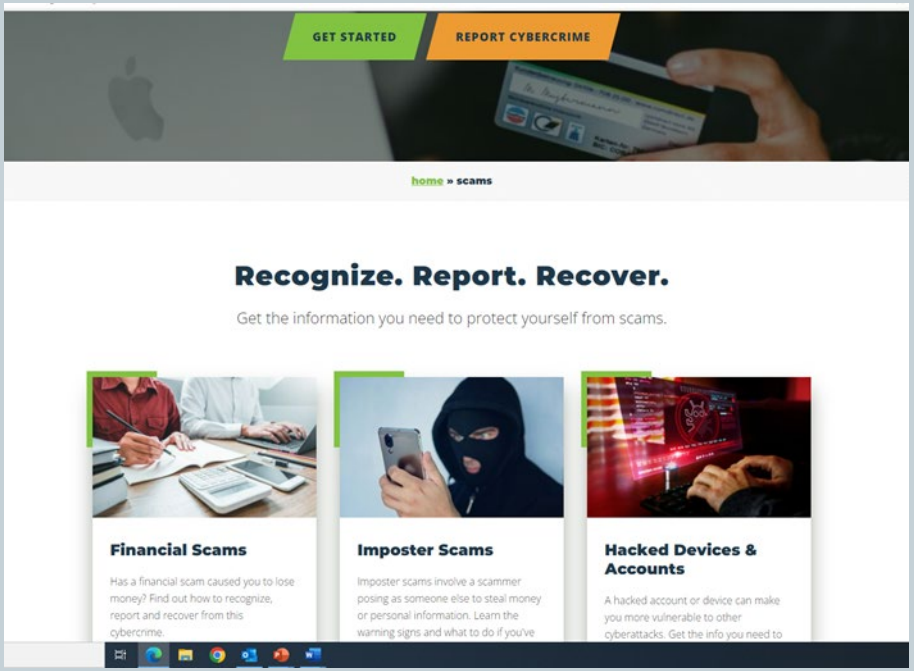
- Peer Support Groups
- Fraud prevention
- Scam tracking map



- www.aarp.org

Cybercrime Support Network

FightCyberCrime.org helps users learn how to recognize, report, and recover from cybercrime, online fraud, and scams.



Q & A

- "Judge a man by his questions rather than his answers."

  ~ *Voltaire*

- "If there are no stupid questions, then what kind of questions do stupid people ask? Do they get smart just in time to ask questions."

  ~ *Scott Adams*

Closing Thoughts

SSA Mary F. Gleason
Phoenix Field Office/Squad C-4
Complex Financial Crimes

623-466-1014

mfgleason@fbi.gov


FBI
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION