Top Financial Scams by Generation

Melissa Trumpower, BBB Institute for Marketplace Trust
Michael Carroll, International Association of Financial Crimes Investigators
Gauri Sharma, ABA
Sam Kunjukunju, ABA Foundation

Housekeeping

- Slides will advance automatically
- All attendee lines are muted
- Use the chat feature to ask questions
- Today’s presentation is being recorded
- Presentation will be posted online within one week at www.aba.com/seniors

Staff Contact

- Samuel Kunjukunju
- Director, Bank Community Engagement
- 202.663.5418
- Skunjukunju@aba.com

Agenda

- Better Business Bureau Scam Tracker 2019 Risk Report
  - Riskiest Scams by age
  - Susceptibility by age
  - Median losses by age
- Debit Card & Imposter Scams
- ABA Training Resources
- ABA Foundation Campaign
- Q&A

BBB Institute for Marketplace Trust

Mel Trumpower
Executive Director

New Risks and Emerging Technologies

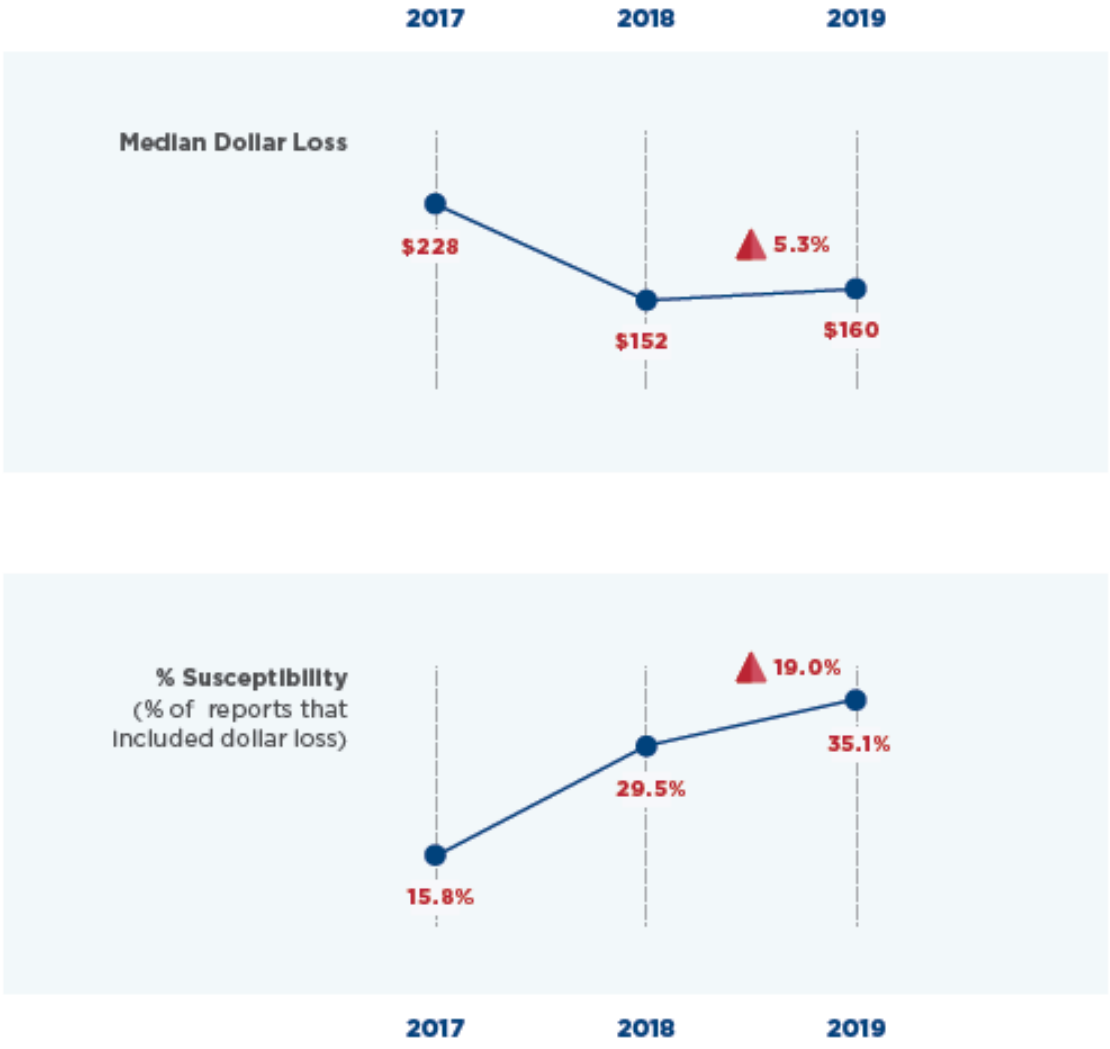
2019 BBB Scam Tracker Risk Report

BBB INSTITUTE for MARKETPLACE TRUST™

- Crowd-sourced
- Searchable
- 21.8% of people say it helped them avoid losing money

BBB Risk Index

Compared with 2018, 2017



2019 10 Riskiest Scams

1. Employment
2. **Cryptocurrency**
3. Online Purchase
4. Fake Check/Money Order
5. Advance Fee Loan
6. Romance
7. Home Improvement
8. Investment
9. Tech Support
10. Travel/Vacation/ Timeshare

#1 Riskiest Scam: Employment

#1 for ages 18-54, men, women, students, and military spouses

More risky than 2018:

- 9.3% of all reports
  (vs 9.1% in 2018)
- 17.7% susceptibility
  (vs 13.7% in 2018)
- $1,500 median loss
  (vs $1,204 in 2018)

#2 Riskiest Scam: Cryptocurrency

#2 for ages 25-44 and men

0.7% of all reports
(vs 0.3% in 2018)

68.5% susceptibility
(vs 63.6% in 2018)

$3,000 median loss
(vs $900 in 2018)

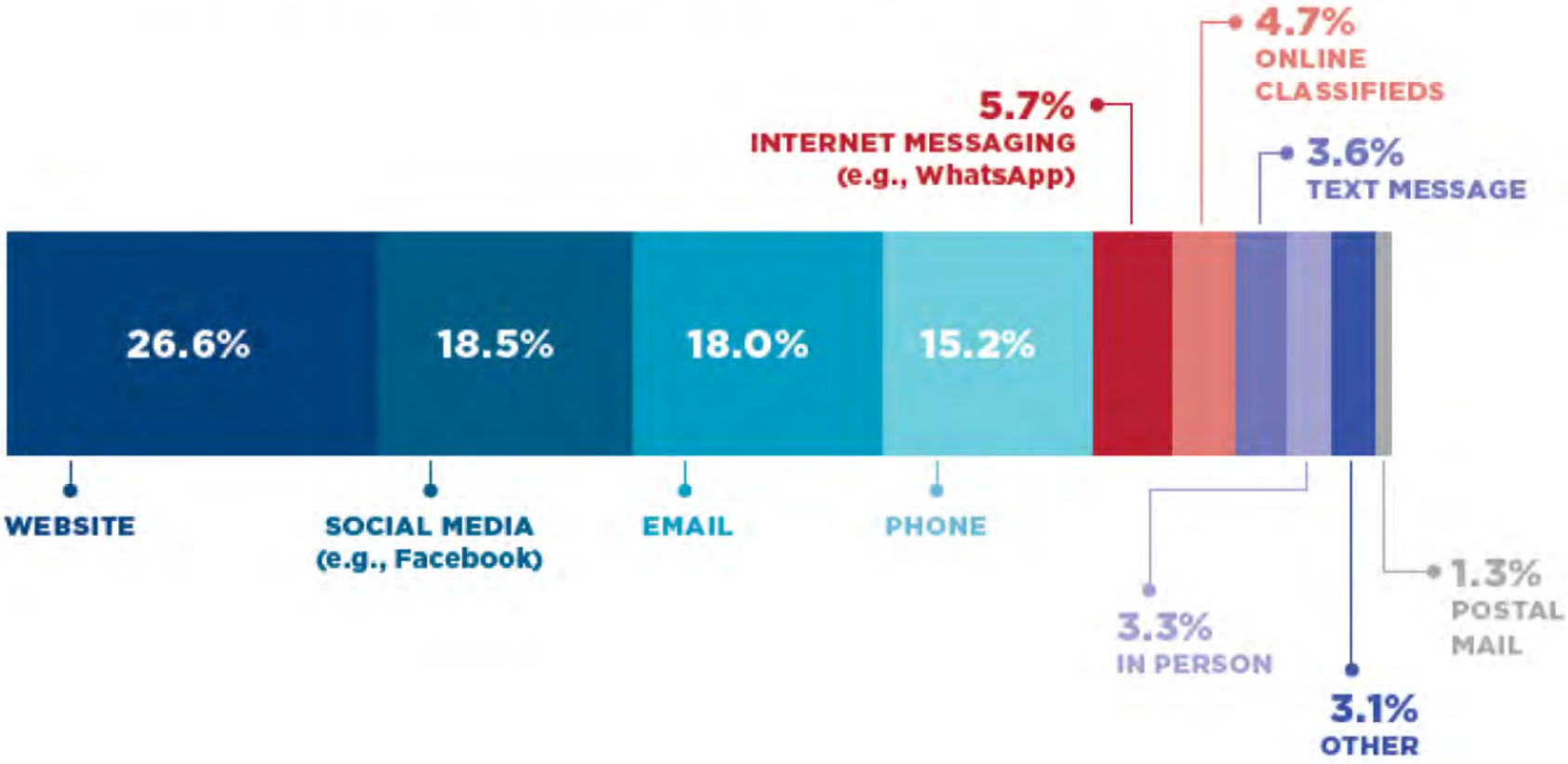
#3 Riskiest Scam: Online Purchase

Most common scam: 24.3%
(vs 20.6% in 2018)

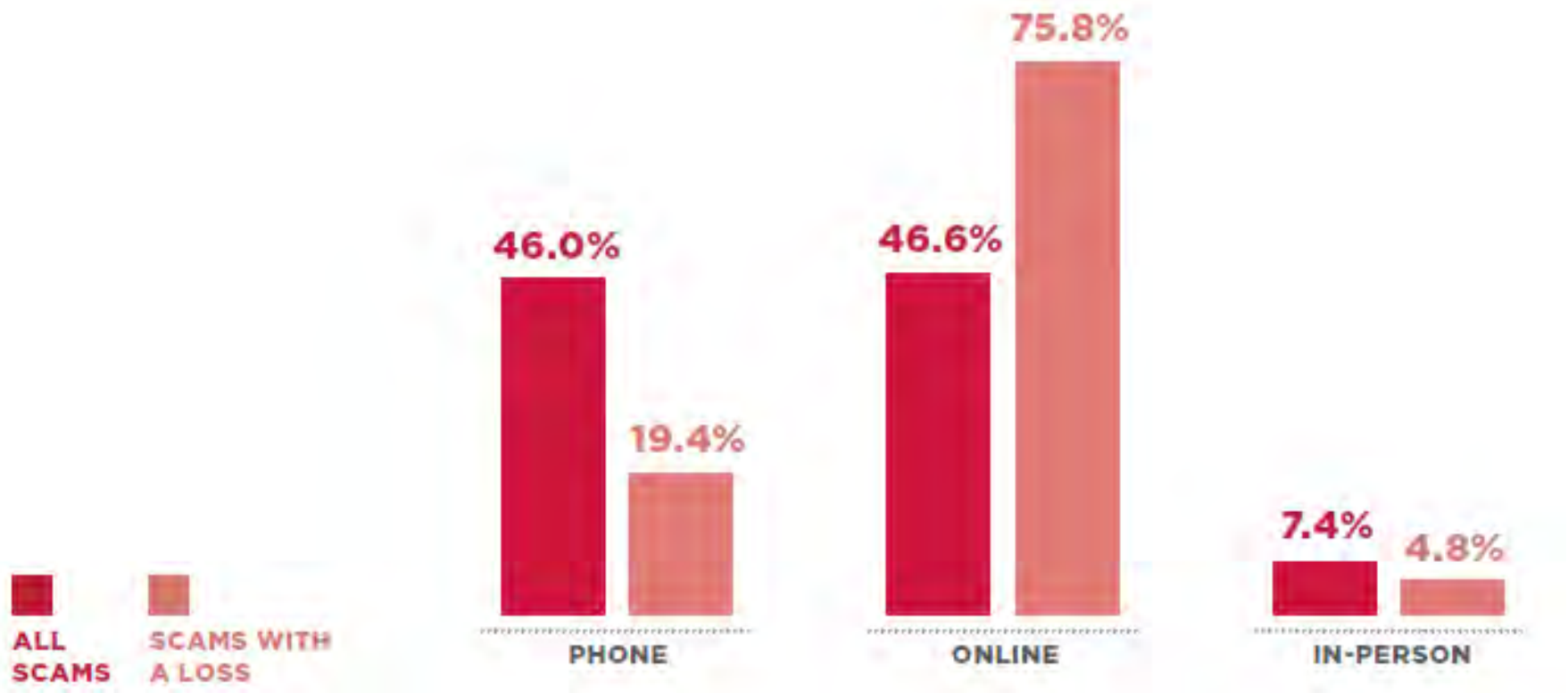
Highest susceptibility: 81.2%
(vs 75.2% in 2018)

Median Loss: $76 (vs $75 in 2018)

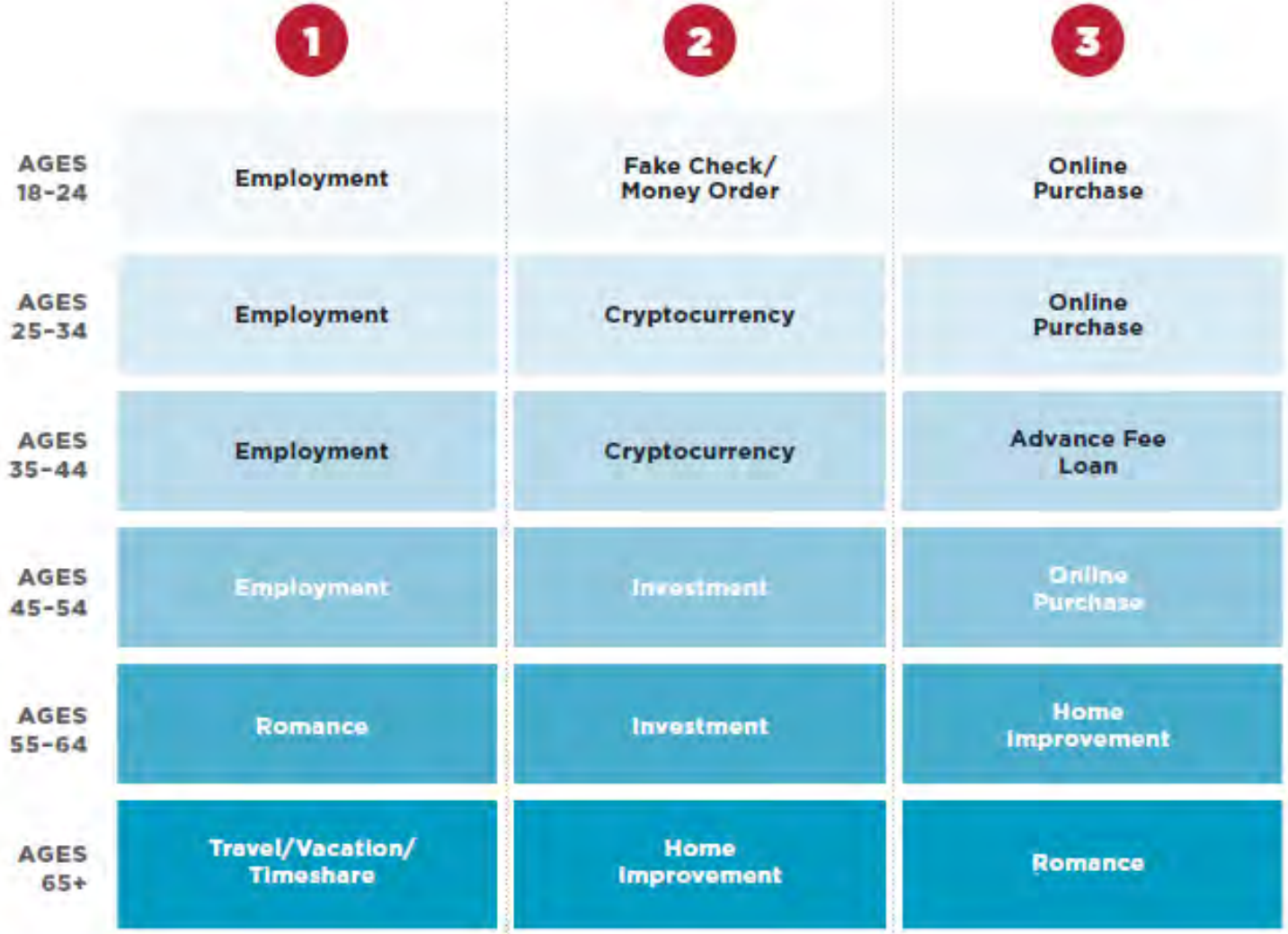
Means of Contact with $ Loss



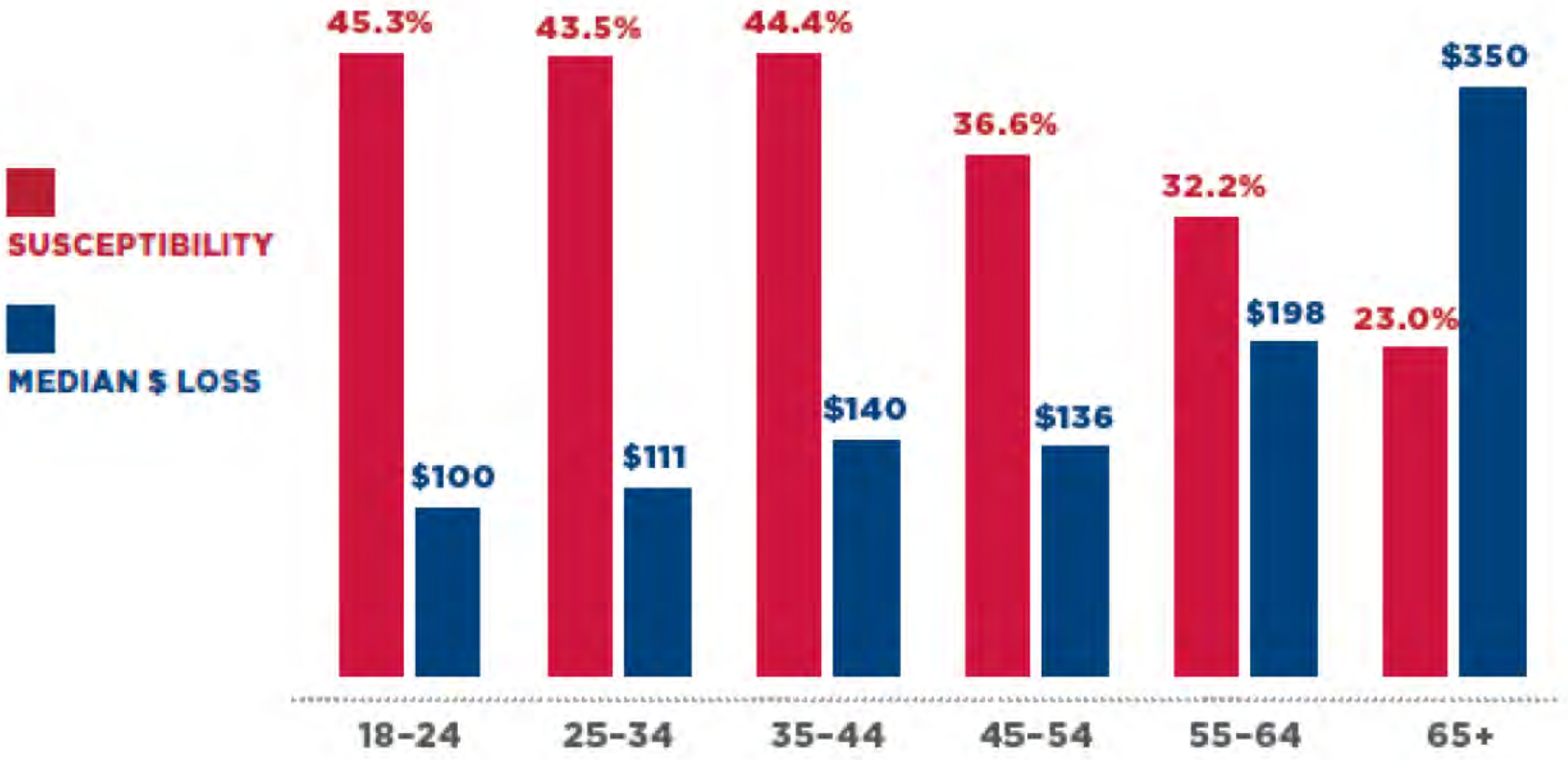
Means of Contact:
All Scams vs. Scams with $ Loss



Riskiest Scams by **Age**



Susceptibility & Median Loss by **Age**

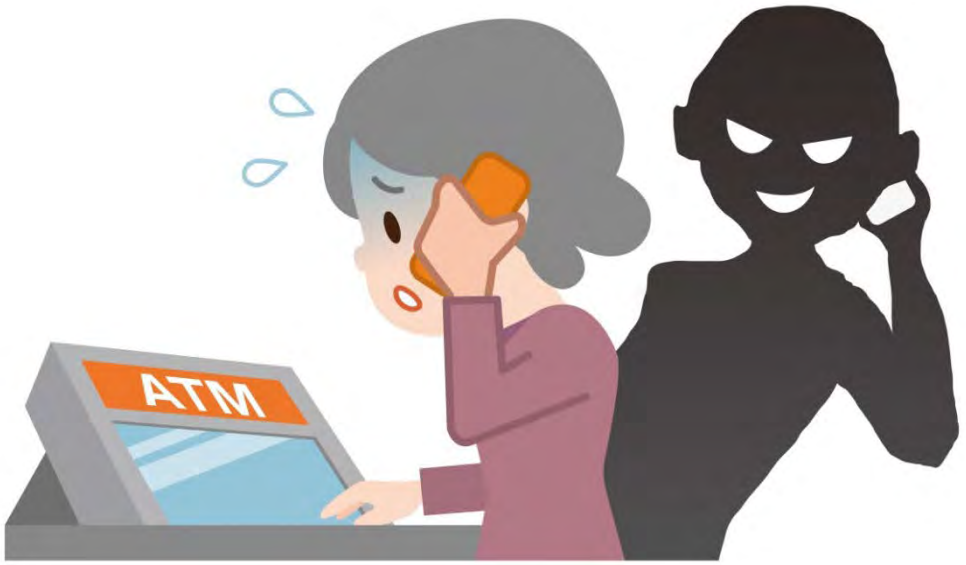


Seniors Lose More Money to Scammers

Investment Scam: **$15,000** vs $2,550

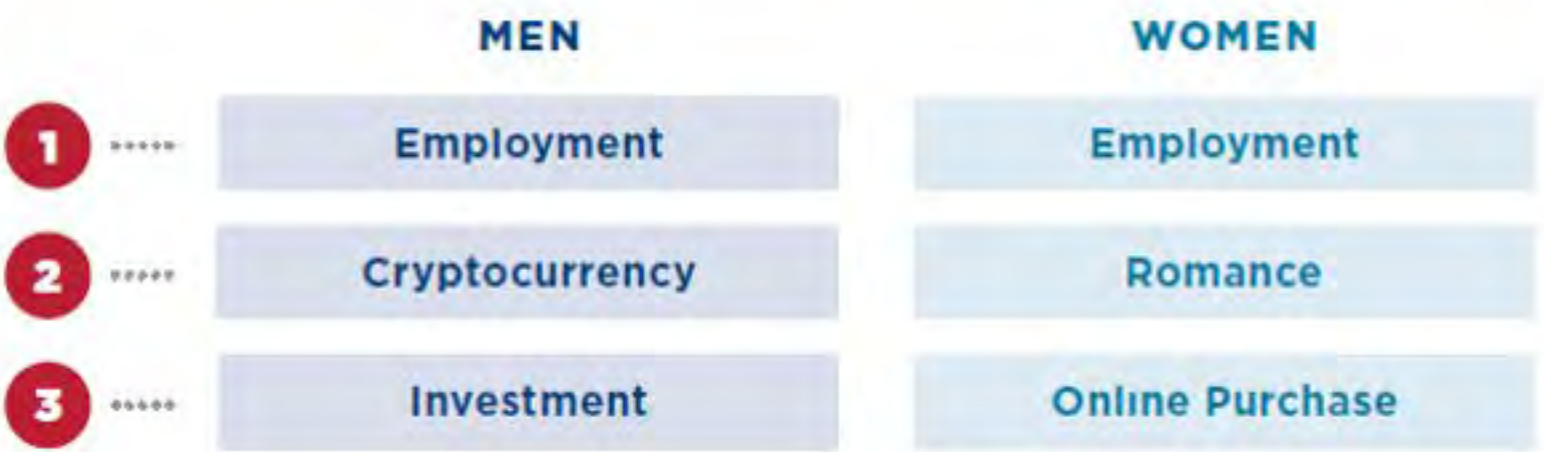
Travel/Vacation Scam: **$6,475** vs $1,097

Overall Median Loss: **$350** vs $160

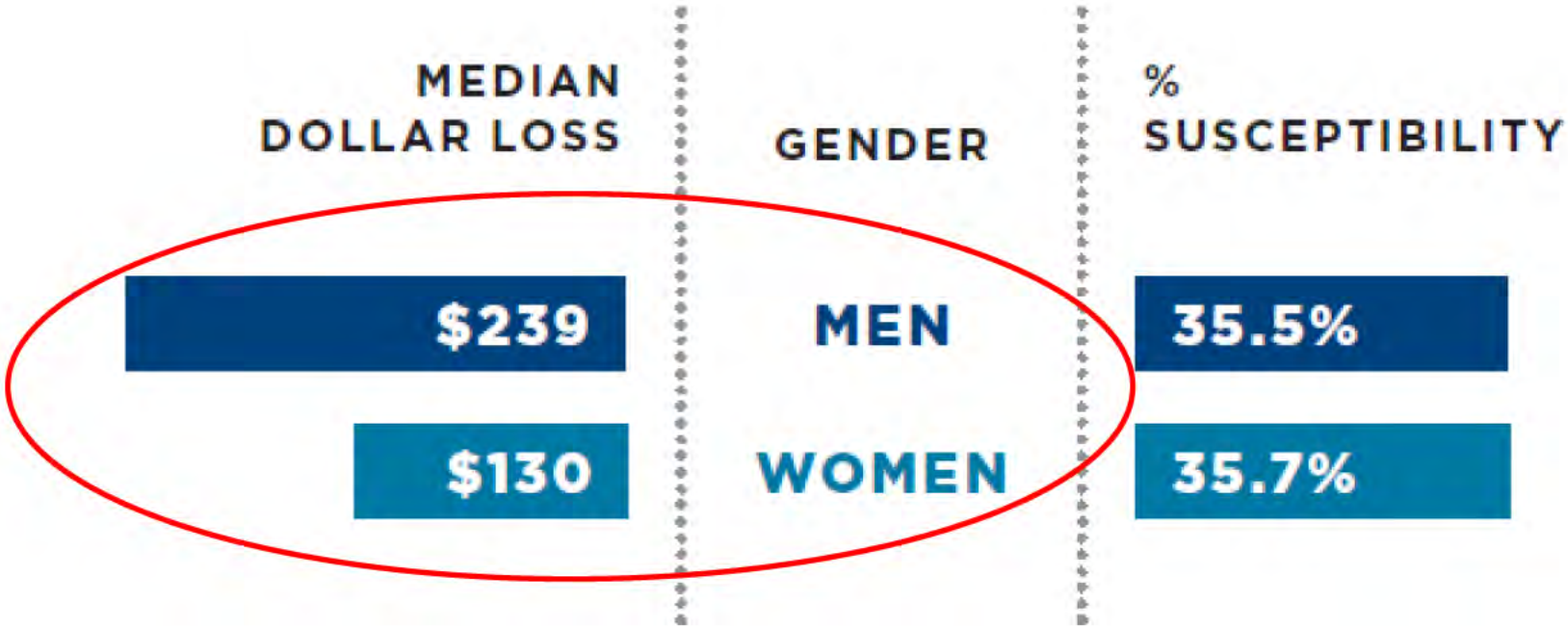


BBB
Start With Trust

Riskiest Scams by **Gender**



Susceptibility & Median Loss by **Gender**



Spotlight: Military / Veterans

3 Riskiest Scams

Service members, spouses and veterans lose more money to scammers.

	MILITARY SPOUSES	VETERANS	NON-MILITARY
1	Employment	Travel/Vacation/ Timeshare	Employment
2	Government Grant	Employment	Cryptocurrency
3	Online Purchase	Online Purchase	Online Purchase

Median Reported $ Loss in 2019:

Service members are also **more likely to lose money to scammers than non-military consumers.** 46.2% versus 35.2%.

Spotlight: **Students**

3 Riskiest Scams

	STUDENT	NON-STUDENT
1	Employment	Employment
2	Fake Check/Money Order	Online Purchase
3	Online Purchase	Cryptocurrency

3,404 students reported a scam to BBB in 2019.

47.7% reported losing money to a scam versus 34.2% for non-students.

$100 median reported loss.

Vast majority of scams with a loss happen online 76.8% for all 18–24 year olds.

Most Impersonated Companies

1	Social Security Administration	1,963
2	Publishers Clearing House	444
3	Microsoft	367
4	U.S. Internal Revenue Service	251
5	Apple	244
6	Amazon	194
7	Medicare	193
8	Walmart	156
9	Cash Advance/Advance America	125
10	Better Business Bureau	111
11	Facebook	107
12	U.S. Treasury	60
13	Paypal	56
14	Dominion Energy	54
15	Capital One	33

Tips for Business Owners

- Train and inform your employees.
- Verify invoices and payments.
- Know who you're dealing with.
- Keep digital data safe and have a cybersecurity plan.

BBB
Start With Trust

Report to help others

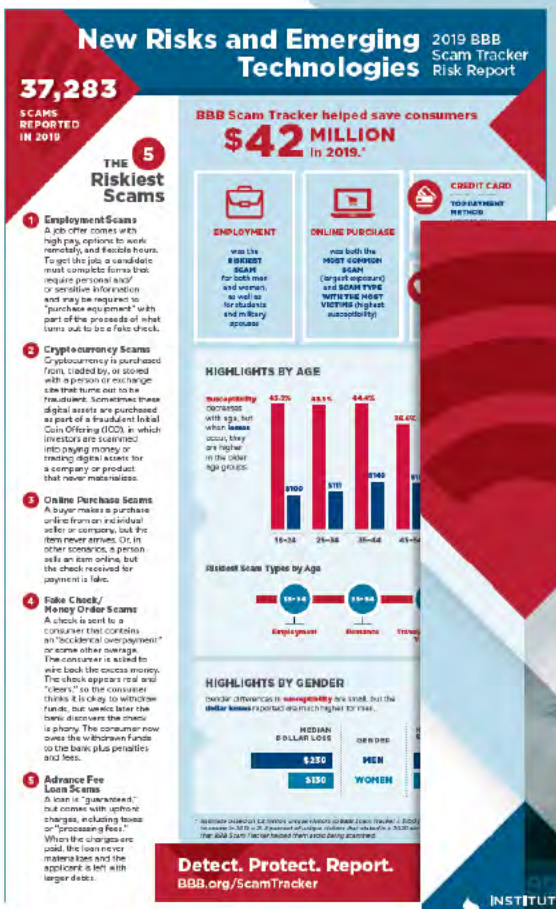
"I didn't want anyone else to go through this."

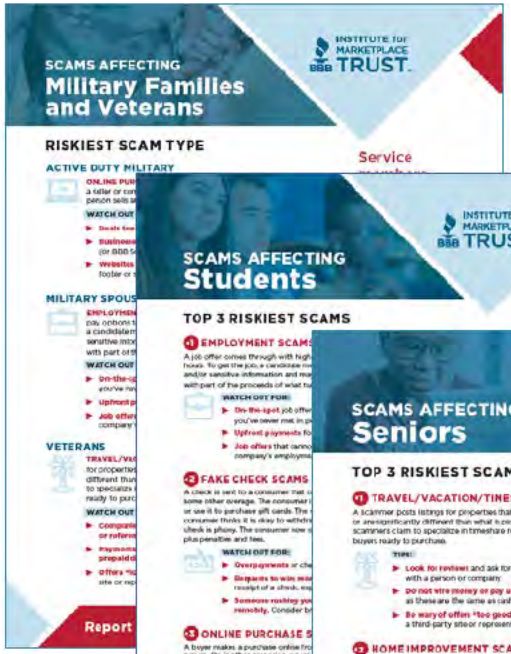
"If these people can share their story, then I can too. I can help by warning others."

"If this helps someone, it was worth it."

More Resources

BBB.org/ScamTracker





Thank you!

International Association of Financial Crimes Investigators

Michael Carroll
President

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

OVERVIEW OF DEBIT CARD SCAMS AND IMPOSTER SCAMS

Michael Carroll

Analyst – US Postal Inspection Service

Chicago Division

IAFCI International President

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

WHO WE ARE …

- 6,000 Members across the globe
- (31) Chapters in the United States
- (9) Chapters Internationally

- Membership comprised of approximately:
  - 1/3 law enforcement
  - 1/3 banking/financial investigators
  - 1/3 retail investigators

- A leader in certifications in the area of fraud, financial, digital forensics and cybercrime investigation

POINTS OF DISCUSSION

- Overview of Debit Card Scam: "Crackin Cards"
- Overview of Imposter Scams and Use of Gift Cards
- IAFCI Projects
- Student Guide – Frauds and Scams Targeting College Students
- PowerPoint presentation for college police to use at orientation on frauds and scams targeting college students.
- Fake Facebook/Instagram page linked to webpage; guardyourstah.org
- TikTok Video

WHAT IS "CRACKIN CARDS"?

- "Crackin cards" is a bank fraud scheme which appears to have originated with Chicago street gangs.
- Suspects **use social media to recruit** individuals to give up their debit card and PIN number in return for monetary gain.
- Account holders – mostly young adults ages 18 - 25, are recruited, enticed, tricked, bribed, or voluntarily agree to **give up their debit card and PIN** to a "recruiter."
- Suspects utilize a cardholder's debit card and PIN to deposit altered stolen checks from the mail or counterfeit checks, into an account holder's bank account.
- Once deposited, these checks temporarily inflate the available balance of the account.

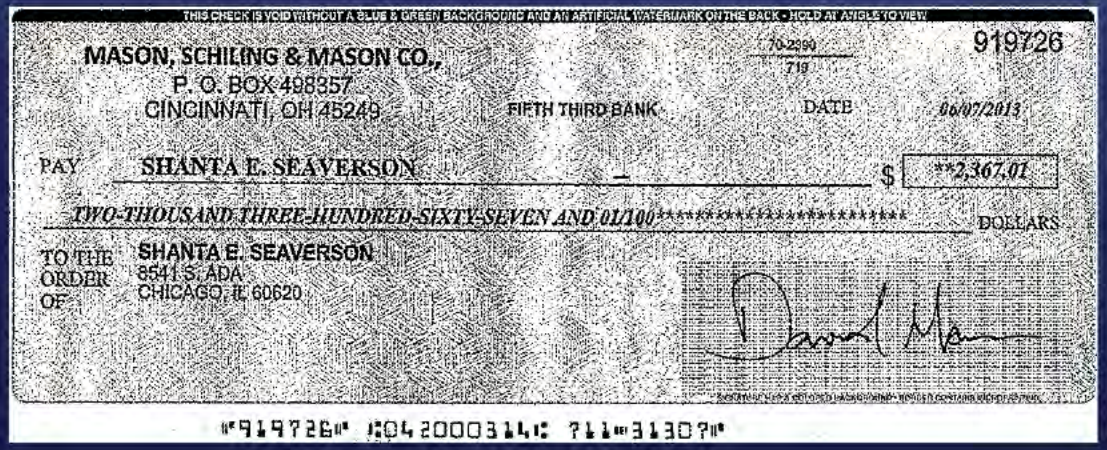
ONCE ACCOUNTHOLDER GIVES DEBIT CARD AND PIN TO RECRUITER

- After the deposits are made, funds are usually withdrawn the next day.
- Suspects use cardholder's debit card and PIN to remove funds from the account via ATM withdrawals, debit card purchases of gift cards or money orders, or by making point of sale cash purchases at a currency exchange (check cashing establishment).
- Deposited checks are then returned to the financial institution "not paid" because of various reasons – account closed, stolen, counterfeit, etc.
- However, the recruiter has already depleted the funds from account.
- Most account holders believe they will be paid for giving up their debit card and PIN to a "recruiter." But, the **account holder never gets paid!**

BACK TO THE FUTURE

- Checks stolen or altered are made payable to person recruited, who will either open an account or use an existing account.
- Not all financial institutions use positive pay to include the payee.
- After the check is deposited, several weeks can go by until the payee contacts sender asking about payment.
- Check sender contacts their bank and learns payee altered check and made it payable to someone else.
- Check sender's bank contacts bank of first deposit, learns most funds withdrawn and affidavit forgery process starts.

COUNTERFEIT CHECK DEPOSITED VIA ATM – PAYABLE TO ACCOUNT HOLDER BUT PHOTO IS OF RECRUITER; CHECKS ARE OF GOOD QUALITY



THIS CHECK IS VOID WITHOUT A BLUE & GREEN BACKGROUND AND AN ARTIFICIAL WATERMARK ON THE BACK • HOLD AT ANGLE TO VIEW

MASON, SCHILLING & MASON CO.,
P. O. BOX 498357
CINCINNATI, OH 45249

FIFTH THIRD BANK

70-2990
719

919726

DATE 06/07/2013

PAY SHANTA E. SEAVERSON $ **2,367.01

TWO-THOUSAND THREE-HUNDRED-SIXTY-SEVEN AND 01/100********** DOLLARS

TO THE ORDER OF SHANTA E. SEAVERSON
8541 S. ADA
CHICAGO, IL 60620

"919726" ⑆042000314⑆ 711-3130?"

Digital Video Snapshot

Site: FTCH/02842 Hyde Park
Camera Group: 02842 Hyde Park
Camera Name: ATM 4486
6/11/2013 11:20:21 AM (Central Daylight Time)

Capture Size: 352 x 240 pixels
Recorder Network Name: MNGS0814B215
Recorder Serial Number: GS0814B215
Recorder Station ID: 1796

North Brevard County Hospital District dba

PARRISH MEDICAL CENTER

951-4 NORTH WASHINGTON AVENUE
TITUSVILLE, FLORIDA 32796-2184

Regions Bank
111 NorthOrange Ave,
Orlando, FL 32801
Member FDIC

63-466/631

CHECK DATE: 06/06/18
CHECK NO: 437887

AMOUNT
***0.00

ID NO. 86-0033427
NOT VALID AFTER 90 DAYS

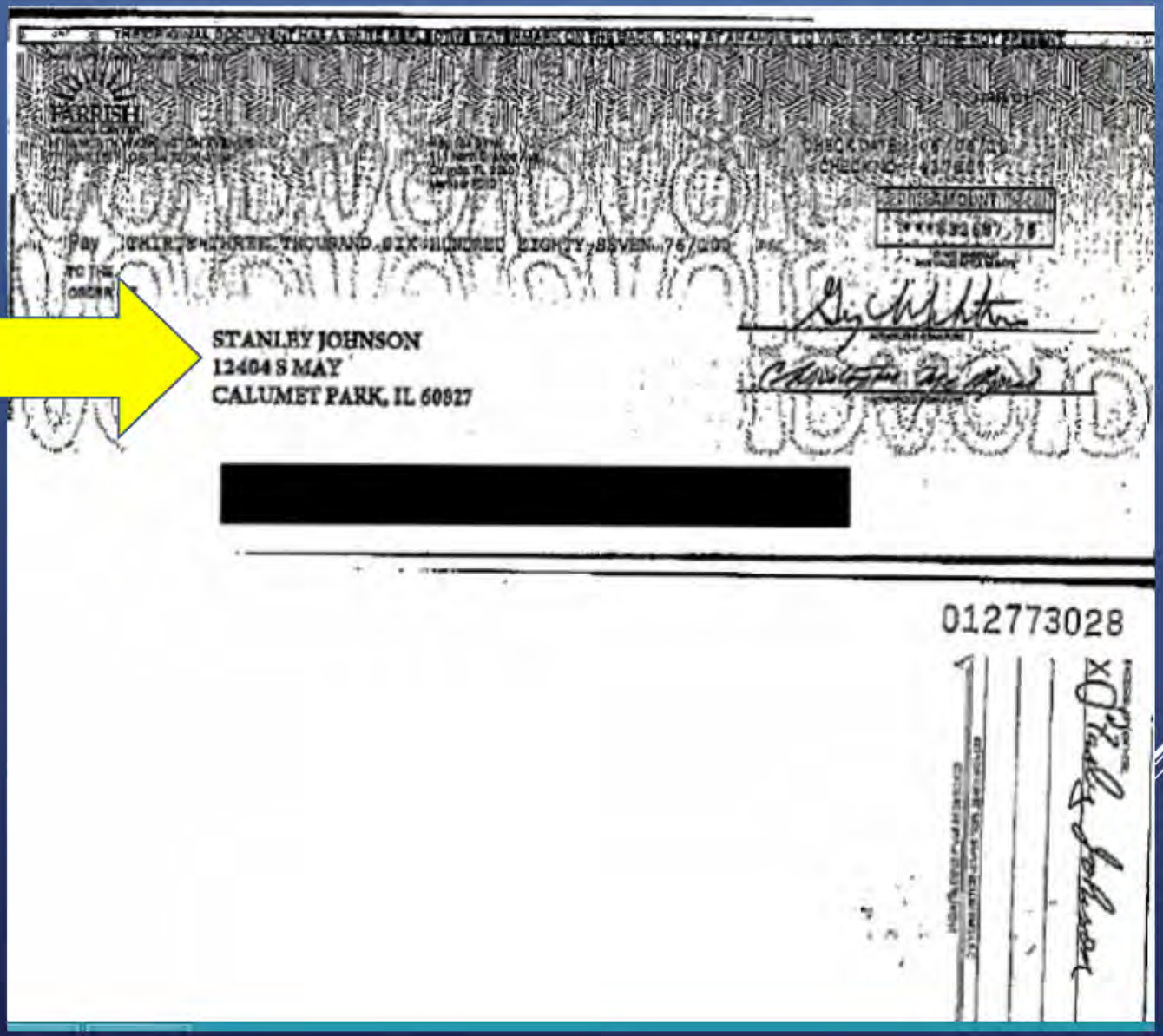
Pay ***** VOID *****

TO THE
ORDER OF

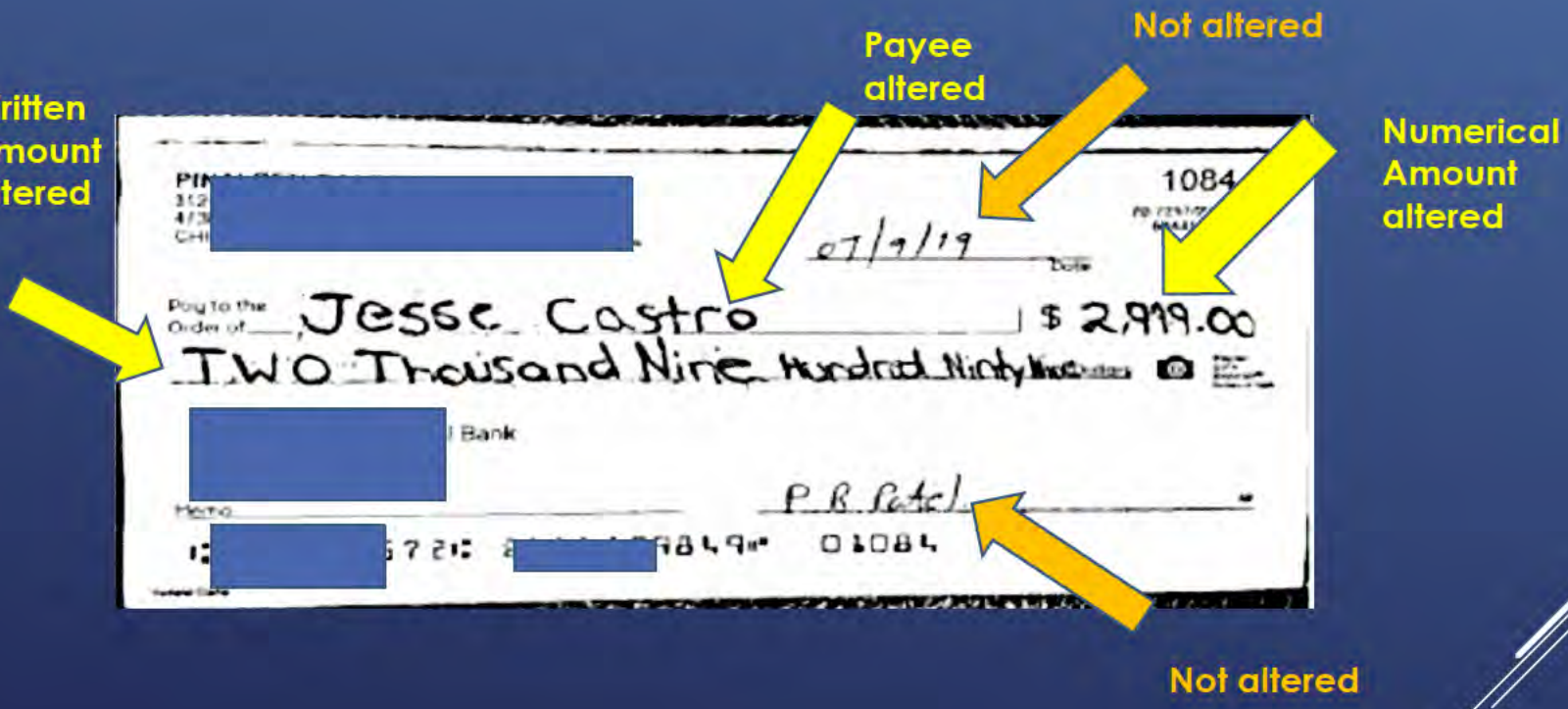
MEDLINE INDUSTRIES
DEPT CH 14400
PALATINE, IL 60055-4400

NON-NEGOTIABLE

Altered


PARRISH
STANLEY JOHNSON
12404 S MAY
CALUMET PARK, IL 60827
[redacted]
012773028

CHECK MADE PAYABLE TO ELECTRIC COMPANY



YOUNG ADULTS RECRUITED THROUGH VARIOUS MEANS

- **Social Networking** – Craigslist, Facebook, Twitter, Instagram or other social networks
- **College Campuses** – recruiters will even go as far as renting apartments for the sole purpose of recruiting students with bank accounts
- Recruit at **Bars, Restaurants, Clubs**, even outside **7/11** convenient stores
- Recruit a family member or friend of a friend of a friend (**anyone willing to give up their debit card and PIN**)

Leave me your number if you want some legit extra cash – the recruiter will then meet the account holder and pick up their Debit Card and PIN. Recruiter **promises cash, but NEVER RETURNS!**

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

USING SOCIAL MEDIA TO RECRUIT: SHOW THE MONEY, FANCY CARS, NICE TOYS, NICE LIVING STYLE, GUNS AND DRUGS


Antonio Chavis
18 hrs
Who tryna make some money dm me ASAP I got sumn for u
9
1 Comment
Like
Comment
Share
Pretty Bambii Me
Like · Reply · 18h
Write a comment...


Malik Webber
June 27 at 9:58 PM
Who got citi bank 3500 same day💯
3
Like
Share

HARDER TO IDENTIFY

CARD CRACKING TRENDS:

- Harder to identify suspect(s)
- Moving to mobile deposits
- Transfers to accounts via person-to-person payments, e.g. Zelle, Venmo, etc.
- Harder to link IP address or phone number
- Financial institutions are linking same devices to accounts
- Account holders are doing more of the work – making deposits and withdrawals

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

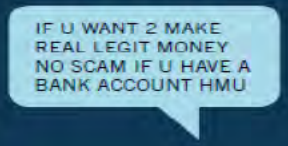
INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

CARD CRACKING

Responding to an online solicitation for 'easy money' and providing a debit card for withdrawal of fake check deposits

A TYPICAL CARD CRACKING SCENARIO

1. A fraudster sends you a social media message to "make quick cash"



2. Enticed by the promise of money, **YOU** provide the scammer a debit card, PIN or online credentials—giving them direct access to account

3. The fraudster deposits a fake check in your account

4. Money is withdrawn immediately at an ATM

5. The fraudster gives the account holder a kickback

6. **YOU** call the bank to report a lost or stolen card, or compromised credentials

7. Bank reimburses the stolen funds to **YOU**

8. **YOU** are now a **CRIMINAL ACCOMPLICE**

American Bankers Association

IMPOSTER SCAMS

- Imposter Scams was the **number one fraud reported** to FTC's Consumer Sentinel in 2019.
- People reported **losing more than $667 million to scammers**, mostly through gift cards.
- Social Security imposters were the top government imposter scam reported. There were 166,190 reports about the Social Security Scam, and the median loss was $1,500.
- Phone calls were the number one way people reported being contacted by scammers.

TOP IMPOSTER SCAMS

- Grandchild in distress – 65%
- IRS Scam - 15%
- Tech Scam -10%
- Sheriff/Police Warrant – 5%
- Utility Shut Off Scam - 5%

Two Recent scams are becoming very popular - Social Security Scam and Payroll Scam.

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

THE GRANDPARENT SCAM

- You receive a phone call from your "Grandchild" and **there is an emergency**
- Scammer may refer to your grandchild by name or a name very similar or even trick you into saying your grandchild's name
- They **need money sent immediately** and they **don't want you to tell anyone**

HOW DO THESE SCAMMERS KNOW THE NAMES OF YOUR FRIENDS OR RELATIVES?

In most cases they don't. For instance, the scammer may say "Hi grandma," hoping that they actually have a grandson. If she replies, "David, is that you?" the scammer will say "Yes!"

Or "grandpa, this is your favorite grandson" or "grandma this is your oldest grandson," hoping the grandparent will reply "Is that you Johnny?"

WHAT DO THESE SCAMMERS USUALLY SAY?

- They might say something like, "I'm in Canada and **I'm trying to get home, but my car broke down** and I **need money right away** to get it fixed."
- Or, they may **claim to have been mugged**, or been in a car accident,
- May claim to have been **arrested in another country** and need money for bail,
- **Need to pay customs fees** to get back into the United States from another country.

THE GRANDPARENT SCAM

- They may also pose as an **attorney or law enforcement official** contacting grandparent on behalf of grandson
- Pose as **friend of grandson** who was in a bad car accident and cant talk
- Calling from the **American Embassy** or **State Department**
- No matter the story, they **always want you to send money immediately**. There is always a sense of urgency.
- **And don't tell mom or dad!!**

IRS IMPERSONATOR SCAM

- Receive call from a person purporting to be with IRS. Person **demands immediate payment** without first having mailed a bill.
- Demand that you **pay taxes** without giving you the opportunity to question or appeal the amount they say you owe.
- **Threaten to bring in local police** or other law-enforcement groups to have you arrested for not paying.
- Require you to use a specific payment method for your taxes, such as a wire transfer, ACH, cash and GIFT CARDS.

TECH SUPPORT SCAMS

- You receive a call from a person who claims to represent a reputable tech company, such as Apple, Dell, or Microsoft. They tell you that **they noticed a fraudulent charge for a tech support product**, and they owe you a refund.

- However, to receive your refund, they'll **ask you to share sensitive personal information**. They may also ask you to log in to specific accounts or **grant them access to your computer**. In some cases, they even insist that the only way for you to get your money back is to purchase pre-paid debit cards or gift cards and give them the card numbers.

TECH SUPPORT SCAMS CONTINUED

- Often the scammer will create a sense of urgency—the computer is sending error messages, **they've detected a virus**, or your computer is about to crash and **you'll lose all your data**!
- You are told only a tech **support employee can fix the problem**, and you're asked to allow access to your machine.
- Once access is granted, the caller will often run a "scan" and claim your computer is infected with viruses. The **scammer then offers to fix the problem...for a fee**.

UTILITY SHUTOFF SCAMS

- The callers claim to be billing representatives from your utility company.
- They tell you that to avoid an immediate shutoff, **you need to settle an overdue bill** by providing them with your credit card number, debit card number or purchase gift cards and read off number on back.
- They may use "spoofing" software that lets them falsely display the name and phone number of your utility company on your Caller ID.

WARRANT FOR ARREST SCAMS

- Victim receives a phone call or email from someone **claiming to be a Sherriff, policeman, lawyer or a bounty hunter**, saying they have a warrant for your arrest.
- The **fraudster can spoof the number** to appear to come from the local sheriff's office or jail.
- Fraudster tells potential victims **they have an outstanding warrant** for an unpaid debt, missed jury duty or some minor infraction and that a fine is due. The fraudster then **convinces victim to make the payments** by wiring funds or purchase gift card and read off number on back.

SCAMMERS WANT YOU TO SEND MONEY THROUGH VARIOUS WAYS

- These scammers ask you to send money through services such as **Western Union** and **MoneyGram** because they can pick it up quickly, in cash.
- **ACH transfer** or US currency sent to money mule/re-shipper
- Current Trend – **Gift Cards!!!**
- And now, in some cases, **cryptocurrency**

CURRENT TREND – PURCHASE GIFT CARDS

- Top five gift cards purchased relating to Imposter Scams:
  - iTunes Gift Cards
  - Target Gift Cards
  - Best buy Gift Cards
  - Steam Gift Cards
  - EBay Gift Cards

WHY GIFT CARDS?

- The fraudster convinces the victim of an imposter scam to purchase gift cards for money owed.
- Usually in amounts from $2000 to $6000, bought in increments of $500
- The fraudster convinces victim that paying by gift card is just like paying by cash, **gift cards are easier and quicker to process**, or gift cards are just like a voucher that is accepted by IRS, tech company, or whatever the imposter scam might be.

GIFT CARDS

- The fraudster convinces that in order to verify the purchase, or for quicker payment so law enforcement don't arrest you, **read the numbers off the back of the card.**
- This allows the fraudster to add gift card number to app on phone and make purchases.
- Victim purchases gift card in Chicago and reads off numbers to fraudsters and purchase next day in Buffalo, NY.
- To convince the victim of legitimacy, victims are instructed to purchase gift cards and mail them directly to IRS office in Washington DC. Of course, the funds have already been removed from card.

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

IRS SCAMS

- A victim (Frisco TX) was contacted by phone from a suspect who identified himself as being from the IRS. The suspect advised the victim she was under investigation and owed several thousand dollars. The suspect was able to get the victim to initially wire $5,896 to them, then was able get the victim to purchase $5,000 in Apple gift cards and $4,000 in Best Buy gift cards. The images one the right are the suspects who redeemed the Best Buy gift cards in and around the Chicago, IL area.

GRANDPARENT SCAM

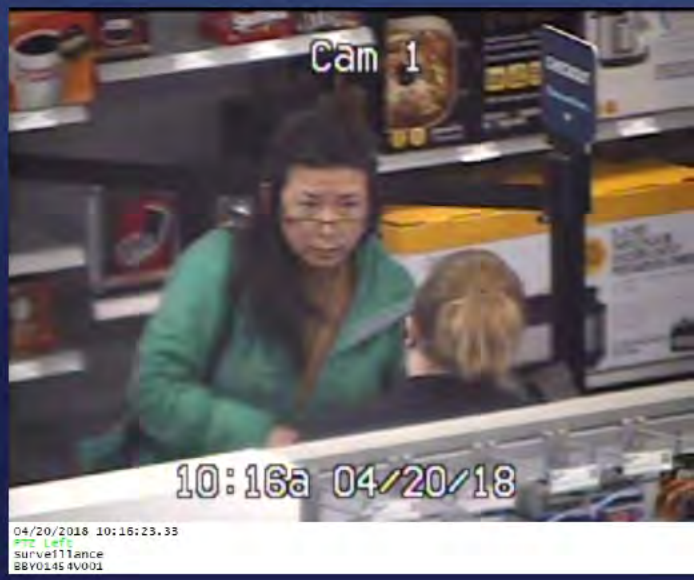
- An elderly female in White Bear Lake, MN fell victim to the grandparent bail scam and provided a Target gift card number for $1,250 to caller on 12/14/17. The gift card was soon redeemed by pictured male at a Houston, TX Target. Male also used another $1,750 gift card of unknown origin. Purchased $3,000 worth of EBay gift cards ($200 each).

WARRANT FOR ARREST SCAM

Said cards were obtained through a phone scam involving an **FBI and DEA agent impersonator**. The suspects called a local doctor and told him he had a **warrant for his arrest for violating a drug law** and that he had to post a federal bond. The victim purchased several gift cards and gave the numbers to the suspects over the phone.

TECH SCAM

- Following a victim sending $2,000 in gift cards swindled from a computer repair scam, the pictured female was seen in a Portland area Best Buy (Beaverton) exchanging them for Nike, Sephora and Nordstrom gift cards.



SOCIAL SECURITY SCAM

- On 09/05/19 and 09/06/19, an elderly victim received calls from an unknown subject posing as a SSA (Social Security Admin) rep. and then he received a call from a subject posing as a DEA agent. Both numbers are VOIP (voice over internet protocol).
- **The victim was told that his SSA benefits were being cancelled** and the DEA had issued a warrant related to drug offenses.
- The victim was convinced to withdraw $25k cash and mail it via FedEx First Overnight to a Walgreens store (FedEx pickup depot) located at 10660 Eastex Hwy Houston TX 77093.
- The package containing the $25k cash was picked up on 09/07/19 at 0850 hours by an unknown male wearing a neon green shirt, glasses and a long beard. The subject picking up the package walked from the rear of the store, no vehicle was captured on any of the store's exterior cameras.

ADDITIONAL IAFCI INDUSTRY GROUPS

- Auto Finance Coalition
- Bust Outs/Synthetic Identity Fraud
- BSA/AML
- Cyber Fraud
- Mortgage Fraud
- Retail Organized Crime Coalition ROCC
- **Identity Crimes/Scams/Elder Abuse**
- New Groups
  - Human Trafficking , SAPTA

IDENTITY CRIMES/SCAMS/ELDER EXPLOITATION WORKING GROUP

- Phil Bartlett, Inspector in Charge, New York Division United States Postal Inspection Service PRBartlett@uspis.gov
- Missy Coyne, Special Agent – National Insurance Crime Bureau - NICB - mcoyne@nicb.org
- Brian O'Connor, Detective, Cambridge (MA) Police Department - boconnor@cambridgepolice.org
- Michael Carroll, Contractor/Analyst, US Postal Inspection Service - mpcarroll@uspis.gov

IDENTITY CRIMES/SCAMS/ELDER EXPLOITATION INDUSTRY GROUP

- Over 210 members on our distribution list and growing.
- Meet bi-monthly on the 3rd Tuesday of the month via teleconference
- Breakout session Monday, August 24 at IAFCI Training Conference on current fraud trends and scams.

PAST ACTIVITY OF OUR GROUP

- Crackin Cards" Brochure for students
- Fraud Guide for Investigators
- A Guide for Clerks, Cashiers, Tellers and Sales Personnel
- Elder Fraud Guide for Investigators
- Scam Guide for College Students
- PowerPoint to go with the Scam Guide for College Students

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

Scamming College Students

How to avoid being scammed

1. Don't share your debit card information or PIN with anyone.
2. Don't deposit funds from an unknown source into your account. –This scam relies on you depositing a counterfeit check into your bank account .
3. Don't be a party to a criminal scheme. It's illegal to defraud a bank.

For more information on this and other scams go to postalinspectors.uspis.gov

You don't have to be a genius to know, there's no such thing as a "free lunch." If it sounds too good to be true—it is!

Crackin' Cards Scam

Know How to Protect Yourself

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

FRAUD AND SCAMS TARGETING COLLEGE STUDENTS

Students Guide to Fraud Scams

Table of Contents

Types of Scams

BEHAVIOR BLACKMAIL SCAM

- College students are extorted for money in return for maintaining their reputation on campus.
  - Students are caught on video doing something inappropriate and the blackmailer threatens to publish the video or unsavory information on social media unless payment is made immediately.

PREVENTION TIPS

- With the prevalence of a phone in every hand and a multitude of social media apps, students should be aware that every action can make its way to the internet with the click of a button.
- Keep apps and privacy settings set to the strictest levels possible.
- **Do not share compromising photos** even with people you are in a relationship with – not all relationships last forever or end on amicable terms. Do not save intimate photos on your device.
- Be mindful of others who may be impaired and act inappropriately – be respectful and don't take or post pictures of them online. The internet is forever and your lapse in judgment today can come back to haunt you in the future.

RESHIPPING SCAM / WORK FROM SCHOOL SCAM

- A scheme involving **bogus job offers**, **fraudulent credit card orders, and the reshipping of illegally obtained products**. Victims are recruited online through job boards and popular employment websites.
- **Don't give out personal information** to a person or company you don't know.
- **Be suspicious** of any offer that doesn't pay a regular salary or involves working for an overseas company.
- Check out the company with the FTC, Better Business Bureau or State Attorney General.

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

RIDE SHARE SCAMS

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

RIDE SHARE SCAMS PREVENTION TIPS

Whether you are riding with Uber, Lyft, Via, or any of the other Transportation Network Companies (TNCs) the company will provide you with valuable information to ensure you enter the correct vehicle. Information includes:

- Vehicle make and model
- First name of the driver and photo
- Vehicle license plate number

If any of the observed details do not match those on the app, do not enter the vehicle.

TIPS CONTINUED

- Where you live is an important piece of information and you may not want to share this information with others. Instead of being dropped off directly in front of your apartment, house or dorm, select a drop off location adjacent to your residence.

- If you notice a cleaning fee charge ($100-$300) for no legitimate reason (you did not make a mess or vomit in the vehicle), immediately access the company website, select the trip in question and select the help section. There you will find a link titled "Dispute Cleaning Fees." You should also contact your credit card company and dispute the charge.

Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

COLLEGE SCAM GUIDE TIPS

- **Get your free credit report at annualcreditreport.com.** Each year you may receive 1 free credit report from each of the 3 credit reporting agencies (Trans Union, Equifax or Experian). Upon receipt, check for unauthorized accounts, inquiries and unknown addresses.
-
- **Know who you are paying**, via person to person payments, e.g., ZELLE, Venmo, etc. Pay and receive money only with people you know. Don't pay strangers with P2P (Person to Person). Most "person to person" transactions are instantaneous and irreversible.

- **Do not pay for merchandise online or via the phone using a debit card**. Debit cards are vulnerable because they are linked to a bank account. You have a far better chance of resolving a fraudulent transaction when paying with a credit card rather than with a debit card. Also do not provide your debit/credit card numbers over the phone, via emails or on websites unless you initiated the call or order.

DISTRIBUTION OF GUIDE

- IAFCI Public and Members Website
- New York University
- IACLEA website
- San Diego Financial Literacy Center (Twitter and Website)
- USPIS HQs Twitter Account
- LinkedIn
- College Confidential (student forum)
- Fordham University
- Jace's (Interns Twitter account) – retweeted
- Northeast Area Update for USPS (segments of the Guide were used in an upcoming article)
- New York Post (Reporter retweeted)
- New York Times (Reporter retweeted)

CURRENT PROJECTS

Crackin Cards

- Questions to ask accountholder to obtain guilt, knowledge, intent – a confession.
- Bogus Facebook page linked to webpage **Guardyourstash.org**
- TikTok video
- Imposter Scams awareness videos
- Podcasts

If any members have any suggestions for future projects for the group, please let us know

DEBIT CARD FRAUD "CRACKIN CARDS"

- Many of the young account holders recruited are college students.
- Account holders can be arrested on local state or federal charges for knowingly giving up their debit card and PIN for financial gain.
- Account holders can also be responsible for reimbursing their financial institution for funds taken from their account.
- Account holders can have their credit history destroyed and may not be able to open bank account, obtain credit cards or loans.
- Prevention and awareness is the key.

WORKING ON QUESTIONS TO ASK ACCOUNT HOLDER

- Questions to ask account holder who claims that debit card and PIN are lost or stolen.
- Questions to ask account holders when claiming they did not know check they deposited to their account was stolen/counterfeit.
- Sample question to ask if interviewing account holder in-person:
  - If account holder claims the debit card was in their purse or wallet, ask them what else was in the purse or wallet that was stolen. Later in interview, ask for one of the items they claimed was in the stolen purse or wallet, such as a license, SS Cards, etc.

DEBIT CARD FRAUD "CRACKIN CARDS"

- Setting up Facebook/Instagram page.
- Share a message that if you have bank account and want to make easy money: message me or "hit me up" link, which directs them to our new webpage.
- Right now it is www.guardyourstash.com.
- When they go to this page there will be a statement advising people that giving up your debit card and PIN or allowing someone you don't know to deposit check(s) to your account is a scam. You can destroy your credit forever, be prosecuted and face jail time. Also include prevention material and videos

HTTPS://MICHAELCARROLL3853.WIXSITE.COM/GUARDYOURSTASH

Guard Your Stash

HOME | WHAT TO LOOK FOR | PREVENTION VIDEOS | CONTACT

Don't Be a Fool

If someone on social media tells you of a great way to make money by giving up your debit card and PIN or letting them put a check in your account, DON'T DO IT. It's a SCAM and you will be left *owing* your bank money, destroying your credit for life, along with *criminal charges* and *jail time*.

For more information on the debit card scam and other frauds and scams, go to www.iafci.org

Promote the cash – the recruiter provides email or phone number to contact to learn the next step

TIKTOK

- Looking at college students willing to be recorded and placed on TikTok, advising others of various scams
- 25 second video clip from our intern
- Learned of scam – giving up your debit card or PIN can lead to destroying your credit, criminal charges and jail time
- **https://vm.tiktok.com/bqR8us/**

CONSUMER FRAUD VIDEO

- Prepared 3 scripts on imposter and lottery scams for training purposes to store clerks, money exchangers and tellers.
- Purpose is to identify the scam and train employees on questions to ask when victim approaches counter to purchase $5000 gift cards, withdraws $1000 on daily basis or wires out $1000 weekly to various individuals.
- Reaching out to 3rd party vendor to provide real actors to play victims and employees. Presently working on finishing 3rd script and getting cost for producing short video.

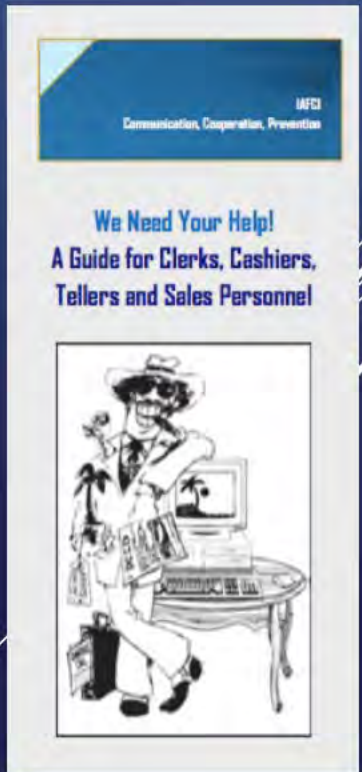
Collectively Combating Financial and Cyber Fraud Globally!

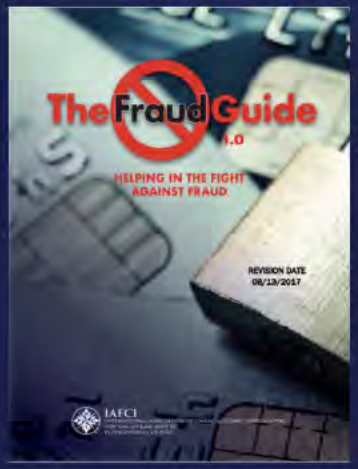
IAFCI

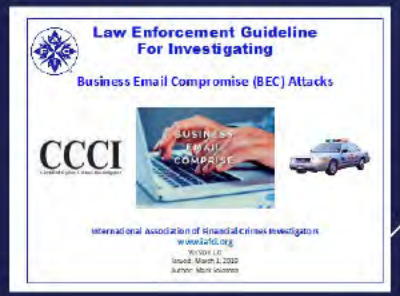
INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

IAFCI PUBLICATIONS & TRAINING MATERIALS

Our memberships is not only committed to training its members, we believe that sharing information with others will help prevent fraud as well as help investigators develop the best techniques to investigate their cases.







Collectively Combating Financial and Cyber Fraud Globally!

IAFCI

INTERNATIONAL ASSOCIATION OF FINANCIAL CRIMES INVESTIGATORS

Contact Information

- Michael Carroll
- Fraud Analyst
- U.S. Postal Inspection Service
- Phone – 312-983-7885
- Cell – 312-509-3809
- mpcarroll@uspis.gov

ABA Bankers Association

Gauri Sharma
Vice President, Professional Certifications

ABA Training & Professional Resources

Certificate in BSA and AML Compliance

- ***Introduction to BSA/AML***
- ***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***
- ***Components of an AML Compliance Program***
- ***International Partners in AML***
- ***Office of Foreign Assets Control (OFAC) for Compliance Professionals***

https://www.aba.com/training-events/online-training/certificate-in-bsa-and-aml-compliance

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***

https://www.aba.com/training-events/online-training/certificate-in-fraud-prevention

ABA Training & Professional Resources

Certified AML and Fraud Professional (CAFP) Certification

Position Yourself as a Financial Crimes Leader

Earning this credential enhances your professional reputation and value by recognizing:

- Your practical experience in complying with U.S. laws and regulations and your ability to respond to a wide variety of financial crimes threatening your institution.
- Your proven knowledge in program design and governance, regulatory requirements, detection, prevention and reporting, and understanding of existing and emerging money laundering and fraud risks.

ABA Training & Professional Resources

Two powerhouse organizations at the forefront of financial crimes–the American Bankers Association and American Bar Association–partner to deliver this premier educational event that has become a trusted resource for insights, expertise and tactics to protect your bank.

https://www.aba.com/training-events/conferences/financial-crimes-enforcement-conference

Community Outreach Materials for Seniors

- **Safe Banking For Seniors**
  - National banker driven educational campaign
  - Turnkey materials to deliver community presentations on:
    - Identifying and **avoiding scams**
    - Preventing **identity theft**
    - Choosing a financial caregiver
    - Acting as a responsible financial caregiver
- Register for **free** at www.aba.com/seniors

SAFE BANKING FOR SENIORS®

Older Americans Benchmarking Report

- Bank services and programs for older adults.
- How banks are responding to fraudulent activity.
- The ways banks are training and educating their employees.

- Visit: www.aba.com/seniors


Online Dating Scams
Has an online love interest asked you for money?
That's a scam.
Scammers know millions of people use online dating sites. They are there, too, hiding behind fake profiles.
Signs of a Scam
Professes love quickly. Claims to be overseas for business or military service.
Asks for money, and lures you off the dating site.
Claims to need money — for emergencies, hospital bills, or travel. Plans to visit, but can't because of an emergency.
COSTLIEST SCAM
REPORTED TO THE FTC IN 2019
$201 million lost
REPORTED MONEY LOSSES INCREASED 6X SINCE 2015
What to do
1 Slow down — and talk to someone you trust. Don't let a scammer rush you.
2 Never transfer money from your bank account, buy gift cards, or wire money to an online love interest. You won't get it back.
3 Contact your bank right away if you think you've sent money to a scammer.
4 Report your experience to:
• The online dating site
• Federal Trade Commission: ftc.gov/complaint
• Federal Bureau of Investigation: ic3.gov
Learn more at ftc.gov/imposters and aba.com/engagement
ABA FOUNDATION


FAKE CHECK SCAMS
Did someone send you a check and ask you to send some money back?
THAT'S A SCAM.
MAYBE:
You win a prize and are told to send back taxes and fees.
You get paid as a "secret shopper" and are told to wire back money.
You sold an item online and the buyer overpays.
IN ALL CASES:
You get a check.
They ask you to send back money.
THAT'S A SCAM.
IF IT'S A FAKE CHECK, WHY IS MONEY IN YOUR ACCOUNT?
Banks have to make deposited funds available within days. It's the law. But uncovering a fake check can take weeks. By then, the scammer has your money. And you have to repay the bank. Remember — just because the check has "cleared" does not mean it is good.
WHAT TO DO:
Be wary. Talk to someone you trust and contact your bank before you act.
Never take a check for more than your selling price.
Selling online? Consider using an escrow or online payment service.
Never send money back to someone who sent you a check.
Spot this scam? Tell the Federal Trade Commission: ftc.gov/complaint
ftc.gov/ScamAlerts
ABA FOUNDATION
aba.com/Consumers


Phishing: Don't Take the Bait
Phishing is when you get emails, texts, or calls that seem to be from companies or people you know. But they're actually from scammers. They want you to click on a link or give personal information (like a password) so that they can steal your money or identity, and maybe get access to your computer.
The Bait
Scammers use familiar company names or pretend to be someone you know.
They ask you to click on a link or give passwords or bank account numbers. If you click on the link, they can install programs that lock you out of your computer and can steal your personal information.
They pressure you to act now — or something bad will happen.
Avoid the Hook
Check it out.
• Look up the website or phone number for the company or person who's contacting you.
• Call that company or person directly. Use a number you know to be correct, not the number in the email or text.
• Tell them about the message you got.
Look for scam tip-offs.
• You don't have an account with the company.
• The message is missing your name or uses bad grammar and spelling.
• The person asks for personal information, including passwords.
• But note: some phishing schemes are sophisticated and look very real, so check it out and protect yourself.
Hi Ms. Fizh,,
Protect yourself.
• Keep your computer security up to date and back up your data often.
• Consider multi-factor authentication — a second step to verify who you are, like a text with a code — for accounts that support it.
• Change any compromised passwords right away and don't use them for any other accounts.
Report Phishing
• Forward phishing emails to spam@uce.gov and reportphishing@apwg.org.
• Report it to the FTC at ftc.gov/complaint.
For more information, visit ftc.gov/phishing aba.com/phishing
ABA FOUNDATION


LOOK BEFORE YOU LEAP
Is a Joint Bank Account Right for Me?
Joint accounts may be a great way to share financial responsibilities (income & expenses).
OTHER REASONS PEOPLE CHOOSE JOINT BANK ACCOUNTS
Extra pair of eyes
Assist with managing money
Post-death distributions
WHAT YOU NEED TO KNOW
The other account holder could withdraw money out of the account without your consent or knowledge.
IRS
You may become responsible for paying taxes on the account.
Your funds could be taken if the other account holder is sued.
SAFER ALTERNATIVES TO JOINT BANK ACCOUNTS
View-Only Account
Convenience Account or Special Financial Power of Attorney
Payable Upon Death Form
If you are considering a joint bank account talk to your banker about the alternatives.
AARP Real Possibilities
ABA FOUNDATION


Money Mule Scams
If someone sends you money and asks you to send it to someone else, STOP. You could be what some people call a money mule — someone scammers use to transfer and launder stolen money.
Scammers often ask you to buy gift cards or wire money. They might recruit you through online job ads, prize offers, or dating websites.
Scammers:
Send you a check
Tell you to send some of the money to someone else
When you later find out the check was bad, you could be stuck covering the entire amount of the check, including what you sent. And that might overdraw your account.
HOW TO AVOID A MONEY MULE SCAM:
Never use your own bank account, or open one in your name, to transfer money for an employer.
Never pay to collect a prize or move any money out of your "winnings."
Never send money to an online love interest, even if he or she sends you a check first.
WHAT TO DO if you spot this scam:
Break off contact with the scammers and stop moving money for them.
Tell your bank and the wire transfer or gift card company — right away.
Report it to the Federal Trade Commission at ftc.gov/complaint.
Criminals are good at conning people into helping them move money. Don't do it. You could lose money and get in trouble with the law.
ftc.gov/ScamAlerts
ABA FOUNDATION
aba.com/Consumers

American Bankers Association

Banking Topics | Training & Events | Member Tools | News & Research | Advocacy | About Us | SIGN IN

Home > Advocacy > Community Programs > Safe Banking for Seniors

Safe Banking for Seniors

Safe Banking for Seniors

- SAFE BANKING FOR SENIORS FAQS
- SAFE BANKING FOR SENIORS FINEDLINK
- SAFE BANKING FOR SENIORS CONSUMER RESOURCES

Safe Banking for Seniors (SBFS) is a free national program, sponsored by the ABA Foundation, that provides bankers with the tools and resources necessary to help older adults, their families and caregivers prevent elder financial abuse and exploitation. The program consist of four turn-key modules with presentations, activity sheets, resource sheets, and guides to help bankers connect with their local communities to share about: identifying and avoiding scams; preventing identity theft; choosing a financial caregiver; and acting as a responsible financial caregiver. Now, also available in Spanish!

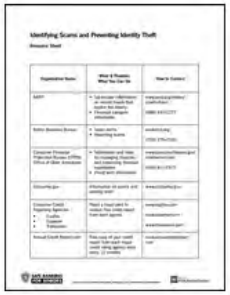
FREE REGISTRATION/UPDATE PARTICIPATION

Banks of all sizes can access Safe Banking for Seniors materials for free simply by registering for the program. Within 24 hours of registration, bankers will receive a link to all Safe Banking for Seniors resources, including presentation lessons, participant activities, communications tools and promotional materials. The list of program participants is shared with State Bank Associations, policymakers and consumers.

Presenter's Guides

Presentation Slides

Activity Sheets



Resource Sheets

Register for free at www.aba.com/seniors

Staff Contact

- Samuel Kunjukunju
- Director, Bank Community Engagement
- 202.663.5418
- Skunjukunju@aba.com