Fraud Awareness Seminar

presented by:

Gregory Matuson- Chief Operating Officer

Joseph Badecki- Security Officer

Danette McDevitt- Director of Operations

September 2022

New Data Shows FTC Received 2.8 Million Fraud Reports from Consumers in 2021

Reported fraud losses increase more than 70 percent over 2020 to more than $5.8 billion

February 22, 2022

Tags: Consumer Protection | Bureau of Consumer Protec https://www.ftc.gov/bureau-consumer-protection el Network

Newly released Federal Trade Commission data shows that consumers reported losing more than $5.8 billion to fraud in 2021, an increase of more than 70 percent over the previous year.

The FTC received fraud reports from more than 2.8 million consumers last year, with the most commonly reported category once again being imposter scams, followed by online shopping scams.

Prizes, sweepstakes, and lotteries; internet services; and business and job opportunities rounded out the top five fraud categories.

Of the losses reported by consumers, more than $2.3 billion of losses reported last year were due to imposter scams—up from $1.2 billion in 2020, while online shopping accounted for about $392 million in reported losses from consumers—up from $246 million in 2020.

Topics for Discussion

1. **Elder Abuse Scams:** Romance, Tech Support, Lottery/Sweepstakes/Inheritance, "Grandparent", Investment & Government Imposter Scams. Targeting Consumers > 60 YOA since they are more financially stable, trusting, and less likely to report crimes.
2. **Business Email Compromises:** type of email cyber crime scam targeting businesses of all sizes, across every industry. Growing GLOBAL problem.
3. **Check Fraud:** Specifically counterfeit and altered checks.

Elder Abuse Scams

By the numbers:

2021

- 92,371 Victims
- $1.7 Billion Losses
- 74 Percent Increase in losses from 2000
- $18,246 Average dollar loss per victim
- 3,133 Victims losing more than $100k

FBI's 2021 Elder Abuse Scams

In Pennsylvania alone, victims lost more than three times the $23.3 million reported in 2020.

OVER 60 VICTIM LOSSES BY STATE*		
Rank	State	Loss
1	California	$427,263,948
2	Florida	$224,205,716
3	New York	$188,052,904
4	Texas	$159,614,547
5	New Jersey	$87,546,156
6	Pennsylvania	$77,027,656

DO's & Don'ts
to Fight Elder Abuse Scams

Training and Awareness is

DO:

- ✓ **Stop and notify us**

  Before withdrawing funds to pay for any of the above

- ✓ **Stay up-to-date on the latest scams**

  Visit our Website

Don’ts to Fight Elder Abuse Scams

- ✗ Pay bills in cash or send cash to the IRS; a legitimate organization will never ask for cash payment
- ✗ Send money to someone you don’t know using apps like Venmo or CashApp
- ✗ Purchase gift cards to send to strangers as a form of payment
- ✗ Return an overpayment that someone made to you
- ✗ Send money to a romantic acquaintance you don’t trust or have never met
- ✗ Deposit cash elsewhere to protect your funds at SSB from being compromised- we would never instruct you to do so
- ✗ Pre-pay taxes or fees to receive lottery winnings

Business Email Compromises

FBI states BEC have increased by 65% between 2019 & 2021

- Between June 2016 - July 2019, the FBI's Internet Crime Complaint Center (IC3) received **241,206 complaints** from domestic and international victims, amounting to **$43 billion in total exposed dollar loss.**
- **It is a GLOBAL PROBLEM!!!**
- In 2021 **Thailand and Hong Kong** banks were the primary recipients of illegal funds acquired through BEC attacks.
- **China**, the previous top destination, emerged third in 2021, followed by **Mexico and Singapore.**

Most Common BEC scams:

1. **CEO Fraud:** Attackers pose as the CEO or Executive and email an employee requesting funds to be transferred to an account controlled by them. They stress "*immediate*" action and are "*not available*" for a conversation.

2. **Email Account Compromise:** An employee's email account is hacked and used to request payments to vendors or change banking information. Payments are then sent to fraudulent bank accounts owned or controlled by the attacker.

3. **False Invoice Scheme:** Attackers target suppliers through this tactic. The scammer acts as if they are the supplier and request fund transfers to fraudulent accounts.

#BECareful

Defending against BEC attacks

- Use multi-factor authentication to account changes.
- Verify emails originate from the purported sender by checking the legitimacy of the sender's email and URLs.
- Subtle misspellings of domain names and email addresses.
- Avoid sharing sensitive details such as login credentials and personal identifiable information (PII)via email messages.
- Use secondary channels to confirm transaction information and instructions they receive via emails.
- Use existing contact information NOT the number in the email.
- These tend to increase before a holiday weekend.

Check Fraud

- Association of Financial Professionals (AFP), post-pandemic figures: **"In 2020, Checks and Wire transfers continued to be the payment methods most impacted by fraud activity.**
- Different approaches to check fraud. On-US & Transit:
  1. **Altered Checks**: intercepted or stolen. Both Personal and Business checks - that have the Payee &/or Amount altered.
  2. **Counterfeit checks**: Legitimate customer information copied to new check stock. Predominantly Business checks – with Payee &/or Amount changed.
- Mobile & Banking Apps are factors with this increase in fraud cases.
- Since April 2020: 200% increase in mobile banking, when the pandemic and lockdowns began.

Factors Driving this Increase

- ***Stimulus*** – Stimulus funds have dried up, fraudsters are turning to checks.
- ***Social Media*** – Creating a booming black market for stolen checks.
- ***New Accounts*** -Fraudsters open new accounts and exploit mobile deposit.
- ***Scams*** – Scams are rising, driving more check fraud attempts.
- ***Mail Theft*** – Checks are being stolen from the mail, then washed and deposited.

Local News
U.S. Mail Thefts of Checks

Local News
U.S. Mail Theft of Checks

Mail Theft On the Rise in Our Region
5 months ago
youtube.com

Pennsylvania authorities announce arrests in **mail** theft...
1 year ago
youtube.com

Postal Worker In Critical Condition After Being Struck B...
3 years ago
youtube.com

Bucks County Authorities Investigating **Mail** Theft
8 months ago
msn.com

Philly USPS Postal Worker Appears to Watch as Man Wal...
5 months ago
nbcphiladelphia.com

Suspects in Pennsylvania **mail** theft ring 'washed' **stolen** chec...
1 year ago
youtube.com

Thieves Use **Stolen Mail** in 'Check Washing' Scheme
5 months ago
nbcphiladelphia.com

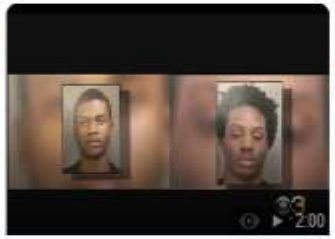
Delco **Mail** Thieves Use Chemicals to Create Blank...
1 year ago
youtube.com

Senators Want Postal Service to Secure Blue Mailboxes After...
2 months ago
nbcphiladelphia.com

Suspects in Pennsylvania **mail** theft operation 'washed' **stolen**...
1 year ago
fox29.com

Mailed Checks Being **Stolen** and Found on Dark Web
5 months ago
youtube.com

Estimated $50,000 worth of antiques **stolen** from...
11 months ago
youtube.com



Upper Darby Police Arrest 2 Men Accused Of Running **Stolen**...
5 months ago
youtube.com

Texas Postal Contractors Arrested, Charged After 8,000...
9 months ago
youtube.com

Mail Theft Investigation Underway In Bucks County
8 months ago
philadelphia.cbslocal.com

Thieves Continuing to Steal Items From the **Mail**
4 months ago
youtube.com

Senators Demand Answers Regarding Ongoing **Mail** Theft
2 months ago
nbcphiladelphia.com

USPS Worker Struck By **Stolen** Vehicle In Southwest Philly,...
3 years ago
philadelphia.cbslocal.com

Scammers File Fraudulent Claims With **Stolen** Personal...
1 year ago
youtube.com

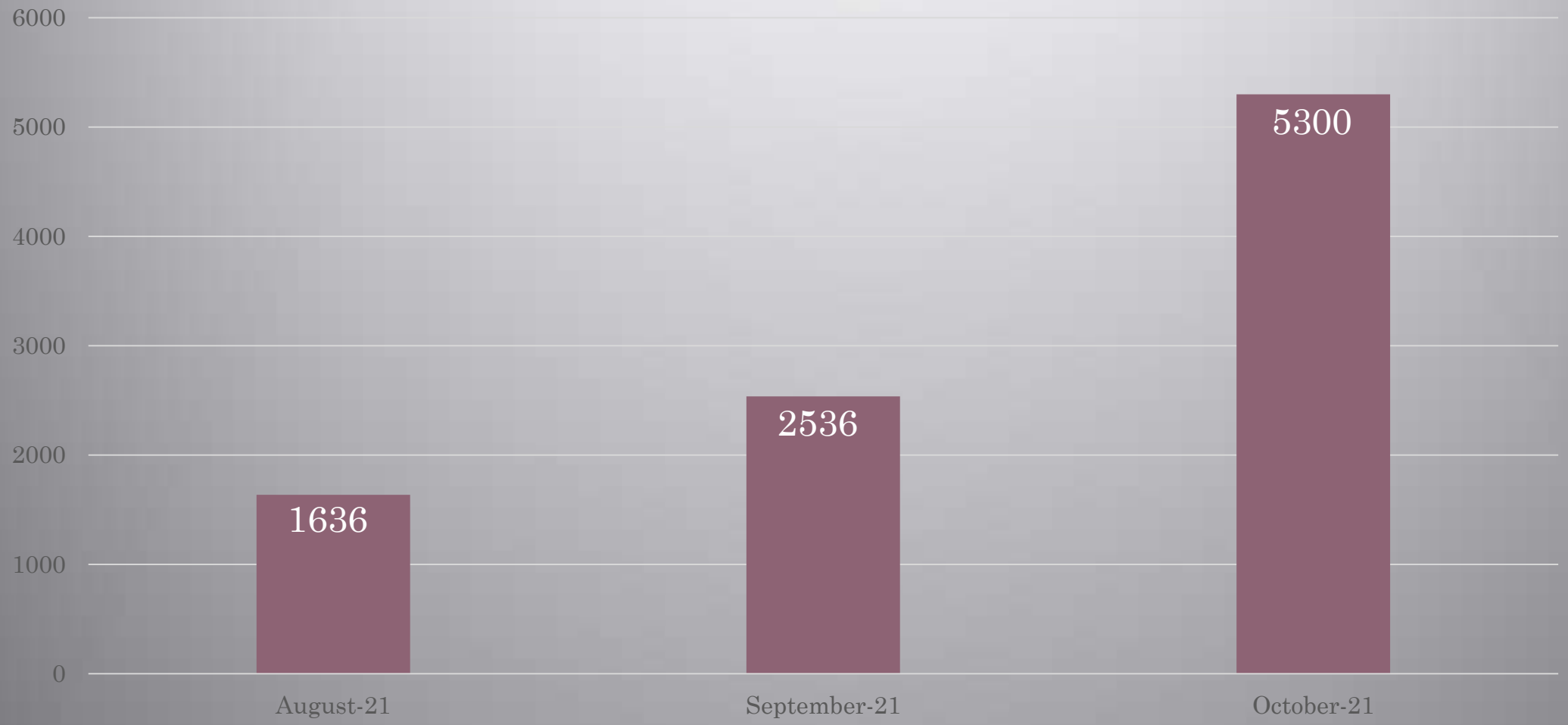
Fox News Flash top headlines for February 22
5 months ago
foxnews.com

Yeadon **mail** theft ring presser
1 year ago
facebook.com

American Bankers Association Reported

Stolen Checks Being Sold on Social Media Increased Dramatically in Last Year

632 in October 2020

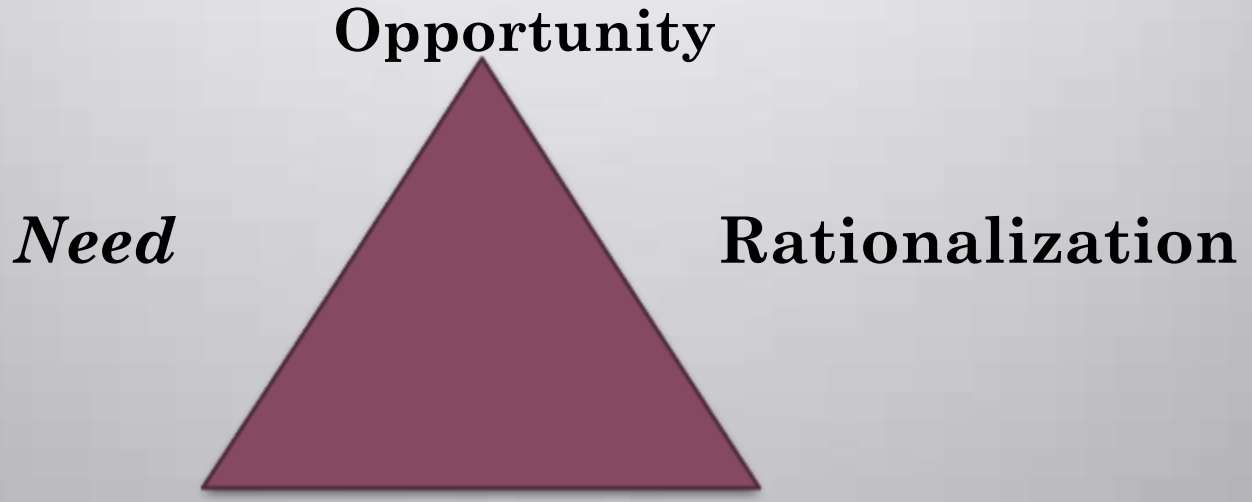


*Georgia State University's evidence Based Cybersecurity Research Group

American Banker Association Reports

Picture of USPS Master Keys For Sale Online - $2,000, Stolen Checks Go For $175

Fraud Triangle:



- Criminologist Edwin Sutherland coined the term “White-Collar Crime” in 1939
- David Cresey, Sutherland’s student at Indiana University, concentrated on embezzlers or “Trust Violators.”
- Devised Fraud Triangle: Opportunity, Need/Pressure, and Rationalization

What Can We Do to Combat Check Fraud

- Sturdy Savings Bank is:
  - Increasing awareness to our Employees and Customers.
  - Enhancing our Positive Pay Platform and offering it for FREE to our business Customers.
  - Investing in Fraud Detection Software

- What can Customers do:
  - Use electronic payments.
  - Checks mailed should be delivered inside the Post Office or handed to your mail carrier. Do not leave in your mailbox or use postal boxes.
  - Review your accounts daily.
  - Enroll in Positive Pay (Benefits include: account remain open, no disruption to daily business)

Fraud Deterrents & Security Features

- E-statements
- Positive Pay
- Online Banking (OLB) Notifications
- Online Banking (OLB) Alerts
- Card Transaction Review Centers

E-Statements

- Request E-Statements to prevent information from being stolen in the mail
- Easier for record retention
- Quicker statement access
- Accessed through your OLB so a password is necessary to access

Positive Pay

How it works

- Business provides details for each check written
- Bank verifies information provided to check image when it is received for payment
- Bank provides business customer with daily exception list; items that do not match
- Customer accepts or declines to pay the item

Positive Pay

Pros

- Secure your bank assets
- Increase your control
- Effective fraud protection tool

Cons

- Requires work on the part of the business owner
- Bank returns the item if you miss the review deadline

OLB Security Preferences- Notifications

Protect Access to your Online Banking portfolio

- Set Up Secure One Time Access Code
- Change Passwords often
- Encourage use of Complex Passwords
  - I love the OC Chamber! They are the best!

Ilt0CC!Trtb!

OLB Security Alerts

Set up Alerts to notify of online changes or specific transaction alerts

- When an external transfer is authorized
- When a recipient is added
- When a computer/browse is registered
- When my Login ID is changed
- When a micro deposit is created
- When the forgot password process is attempted unsuccessfully
- When an Invalid Secure Access Code is submitted
- When my login ID is disabled
- When my Login ID is locked out

Business Card Transactions

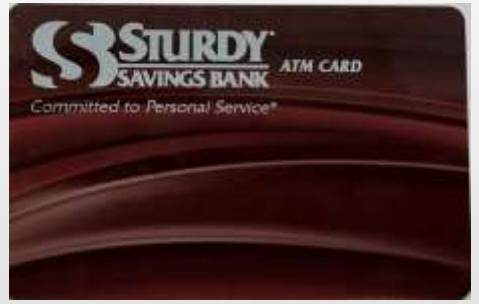
Fraud Detection Centers – monitors transaction activity

- Fraud Centers will reach out to your phone number on file if they see unusual activity. Be sure to answer your phone.
- Enter phone number in your mobile device as a contact including your bank name and Fraud Center

SSB Fraud Detection Center – 800-262-2024 & 973-682-2652

Lost or Stolen Cards – 800-472-3272

Card Monitoring Service



- Control your card through your mobile device
- Allows you to turn your card off and on
- Immediate notification on transaction types and amounts that you choose
- Set transaction thresholds on your mobile device or computer
- Limit merchant types
- Limit locations such as domestic vs. international

Closing Remarks

Philadelphia Business Journal (Sept 15, 2022)

Your banking partner is one of your best resources in helping protect your business against fraud and addressing it if your business falls victim. Therefore, it's important to have a strong relationship with your bank and trust that they have your best interest in mind. Your bank should not only offer anti-fraud monitoring systems and fraud prevention services, but also stay abreast of the latest tools and technologies that can help secure your business and make proactive recommendations. Lastly, your banking partner should be easily accessible if fraud does occur if you see suspicious activity on your account or if you have a question.

With fraud schemes evolving at a rapid pace, it's important that business owners continue to educate themselves and their employees on ways to protect themselves and the business. The right banking partner can help not only inform your fraud protection plan, but also inform your employee education and keep you abreast of the type of schemes they are seeing.

While many businesses can't stop accepting or issuing checks to protect their business, there are other proactive steps they can take to ensure they are handling checks in the safest manner possible. It is never too late to improve your processes and your organization's defenses against fraud.