Combatting Financial Fraud: Strategies for Banks and Businesses

Presented by:

Missouri Chamber of Commerce and Industry

Missouri Bankers Association

Agenda

- Welcome – Kara Corches, President & CEO, Missouri Chamber of Commerce and Industry; and Jackson Hataway, President & CEO, Missouri Bankers Association
- Overview of Webinar Details
- Presentation on check fraud and other fraud – Carol Barnett, Senior Vice President, Compliance Services, Missouri Bankers Association
- Presentation by Diane Klocke, Special Assistant United States Attorney, U.S. Attorney's Office, St. Louis
- Q&A
- Presentation on Beneficial Ownership Registry – Carol Barnett
- Q&A
- Wrap-up

Webinar Details

- **Presentation materials were emailed to registrants**
- **Ask questions using the Q&A feature**
- **Asking questions verbally will not be available, as all participants are muted**
- **The webinar is being recorded, and the recording will be available from the Chamber for Chamber members, and from the MBA for MBA members**
- **The information presented in this webinar does not constitute legal advice; attendees should consult legal counsel for specific application of concepts that are presented**

The Fraud Landscape

- **Fraud, including check fraud, is the largest source of illicit proceeds in the United States and represents one of the most significant money laundering threats to the United States. The U.S. Treasury Department reported that check fraud has increased 385% since the pandemic.**
- **Despite the declining use of checks in the United States, criminals have been increasingly targeting the U.S. Mail since the COVID-19 pandemic to commit check fraud. The United States Postal Service (USPS) delivers nearly 130 billion pieces of U.S. Mail every year to over 160 million residential and business addresses across the United States. From March 2020 through February 2021, the USPIS received 299,020 mail theft complaints, which was an increase of 161 percent compared with the same period a year earlier.**
- **Additionally, the United States Postal Service (USPS) reported 38,500 high volume mail theft incidents from mail receptables (including blue USPS collection boxes) from October 2021-October 2022 and over 25,000 such incidents in the first half of Fiscal Year 2023. While mail theft often consists of mail being stolen from USPS mailboxes or personal mailboxes, USPIS reported 412 mail carriers were robbed on duty between October 2021-October 2022 and 305 were robbed in the first half of Fiscal Year 2023.**

The Fraud Landscape

- **Criminals committing mail theft-related check fraud generally target the U.S. Mail in order to steal personal checks, business checks, tax refund checks, and checks related to government assistance programs, such as Social Security payments and unemployment benefits.**
- **Criminals will generally steal all types of checks in the U.S. Mail as part of a mail theft scheme, but business checks may be more valuable because business accounts are often well-funded, and it may take longer for the victim to notice the fraud.**
- **There have been cases of Postal Service employees stealing checks at USPS sorting and distribution facilities. However, according to USPIS, mail theft-related check fraud is increasingly committed by non-USPS employees, ranging from individual fraudsters to organized criminal groups comprised of the organizers of the criminal scheme, recruiters, check washers, and money mules.**

What Happens When Checks Are Stolen?

The Financial Crimes Enforcement Network (FinCEN) identified three primary outcomes after checks were stolen from the U.S. Mail:

- **44 percent were altered and then deposited**
- **26 percent were used as templates to create counterfeit checks**
- **20 percent were fraudulently signed and deposited**

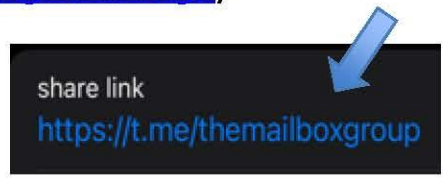
What Happens When Checks Are Stolen?

- After stealing checks from the U.S. Mail, fraudsters and organized criminal groups may alter or "wash" the checks using chemicals to remove the original ink on a check, replacing the payee information with their own or fraudulent identities or with business accounts that the criminals control. During check washing, these illicit actors also often increase the dollar amount on the check, sometimes by hundreds or thousands of dollars. Washed checks may also be copied, printed, and sold to third-party fraudsters on the dark web and encrypted social media platforms in exchange for convertible virtual currency.
- In some cases, victim checks are also counterfeited using routing and account information from the original, stolen check. Illicit actors may cash or deposit checks in person at financial institutions, through automated teller machines (ATMs), or via remote deposit into accounts they control, and which they often open specifically for the check fraud schemes.
- Criminals may also rely on money mules and their pre-existing accounts to deposit fraudulent checks. A money mule is a person (whether witting or unwitting) who transfers or moves illicit funds at the direction of or on behalf of another. Homeless individuals and college students are often targets.
- Once the checks are deposited, the illicit actors often rapidly withdraw the funds through ATMs or wire them to other accounts that they control to further obfuscate their ill-gotten gains.

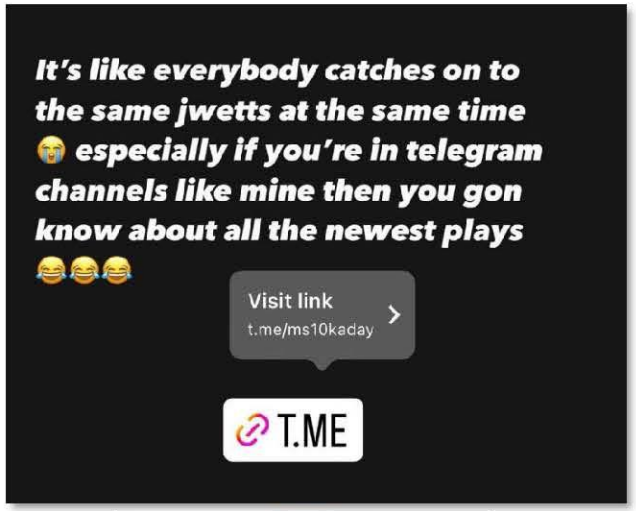
Telegram and the Check Fraud Landscape

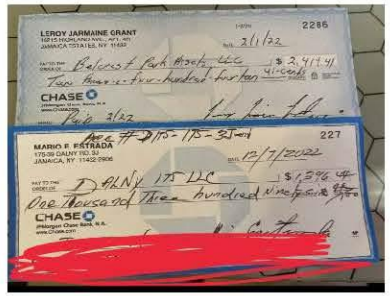
DOES NOT ACCEPT US LEGAL PROCESS

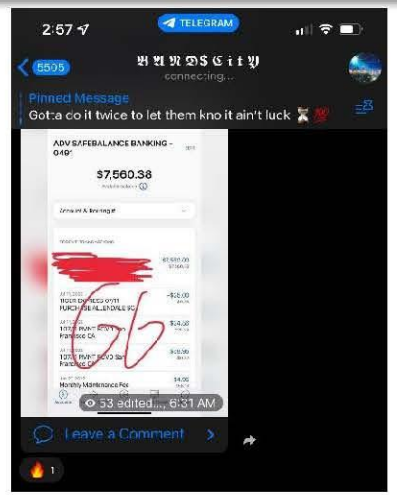
- Telegram has over **700 million** monthly active users and is one of the **10 most downloaded apps** in the world (https://telegram.org/)
- **Share link**



- "Channels" and "Chats" where like minded individuals can connect anonymously to discuss ANYTHING such as: fraud, guns, drugs & other illicit activities
- Telegram offers encrypted messaging – need the physical phone/device to access the encrypted messages







Some cell phone extractions may not capture Telegram messages/data.

Telegram

According to a report issued by Recorded Future, a threat intelligence company, their fraud intelligence team analyzed nearly one million stolen bank check images that were posted on over 700 Telegram sources the first half of 2024 revealing these major check fraud statistics and trends:

- **The check fraud ecosystem on Telegram is defined by rampant reposting – for every original and net-new check image, an average of six reposts of the check on other Telegram channels was observed**
- **Threat actors post stolen check images soon after stealing the checks – 50% of stolen check images are posted within eight days of when the check was signed, and 75% of stolen checks are posted to Telegram within two weeks**
- **Stolen checks impact all 50 states, including suburban and rural areas**

Who bears the loss from check fraud?

- **It depends – it's not an easy answer**
- **Laws and regulations have not evolved with technology**
- **Uniform Commercial Code and other laws can have an impact**
- **Altered Check – generally the depository bank**
- **Forged/counterfeit check – generally the paying bank**
- **Customer can be liable if the customer does not abide by the account agreement and does not exercise ordinary care**
- **Ultimately everyone pays – either through a direct loss, or in the reduction of services or higher costs because of losses**
- **The vast majority of the money is leaving the country (thwarting law enforcement efforts) and is used to further fund illegal activities**

Check Fraud Examples

A large check written by ABC Company was mailed to XYZ Company. Both of these companies are located in Missouri. The check was stolen somewhere along the line, likely from the mail. XYZ Company never received the check and contacted ABC Company about not receiving payment. ABC Company reviewed their statement and saw that the check was paid by their Missouri bank. Upon investigation it was revealed that the check was in fact deposited in a Georgia bank by "XYZ Company" – a phony company created by filing documents with the Georgia Secretary of State and opening a new account at the Georgia bank with those documents in the name of XYZ Company and depositing the check.

How to avoid: ABC Company could have used a wire transfer, ACH or other form of payment to pay XYZ Company instead of just mailing a check via regular U.S. mail. ABC Company could have sent the check as certified mail or used a carrier that would require a signature and/or address proof of delivery.

Check Fraud Examples

A Missouri business pays its workers by check every Friday. Many of the employees are new to the area or somewhat transient and do not have bank accounts. They go to the bank where the business has its bank account to cash checks at the bank as they are "on us" checks and the bank has been doing this for years for their long-standing business customer. Several fraudulent checks are cashed, that are identical counterfeits to legitimate checks. A Texas crime ring has obtained a real check, made counterfeit checks, and has hired people to pose as employees to cash the counterfeit checks using their real names and IDs, to receive a cut of the check proceeds, with the rest going to the crime ring.

How to avoid: Use other payment mechanisms to pay employees, increase security features on paychecks, work with the bank to implement Positive Pay or possibly provide a list of payees to the bank or come up with other solutions.

Check Fraud Examples

Homeless people are being recruited/coerced at various locations around Missouri. The fraudsters obtain a legitimate Missouri business check, and then create counterfeits. The homeless people are using their own name and ID to cash the "on-us" checks at banks where the businesses have accounts. Occasionally they will open an account.

How to avoid: Use positive pay so that only checks to approved payees will be paid by the bank.

Business Email Compromise/Account Takeover

- **Can result in fraudulent wire transfers or other payments from online banking**
- **Banks and business customers must implement stringent multi-factor authentication procedures, call-back procedures, other forms of verification to ensure transactions and requests are legitimate**
- **Implement security procedures to ensure accounts are only being accessed by authorized personnel**

Deepfake Fraud – synthetic media produced by GenAI. Deepfake videos replace a person's likeness with someone else's in existing images or videos or mimic a person's voice in deepfaked audio with striking accuracy

- **According to a report by the FS-ISAC Artificial Intelligence Risk Working Group, 1 in 10 companies have encountered deepfake fraud, and 6 in 10 executives say their firms have no protocols regarding deepfake risks**
- **Anyone's voice/image that exists in digital form can be cloned effectively**
- **Ways to combat: multi-factor authentication, fraud reduction processes such as callbacks, methods to determine "live person" interaction, possible biometric devices**

Presentation by Diane Klocke

- **Diane Klocke has been a Special Assistant United States Attorney with the U.S. Attorney's Office in St. Louis, Missouri since 2018. Diane is part of the White-Collar unit of the office, prosecuting crimes related to Social Security fraud, identity theft, bank fraud, tax fraud, and more. Prior to her work with the U.S. Attorney's Office, she worked for the Social Security Administration and a county prosecutor's office. She has been a practicing attorney for 15 years.**
- **Diane will share some real-life cases where businesses have been impacted by fraud.**

Fighting Check Fraud

- **Eliminate or reduce the use of paper checks, especially ones that are mailed and payments of large dollar amounts, by using ACH payments, wire transfers, and other digital payment methods such as real-time payments (FedNow, for example).**
- **Encourage customers of your business to pay you through digital methods instead of mailing checks to you.**
- **Use Positive Pay Solutions for checks you can't convert to electronic payments – this service may vary by bank, but it typically compares checks presented for payment against a list of checks issued by the business. The date, check number, payee, signature, and amount must all match for payment to proceed.**

Fighting Check Fraud

- **Implement security features on checks – watermarks, certain inks, microprinting and other security features on check stock make it much harder to alter checks or create counterfeit checks – criminals will look for the easiest checks to alter or counterfeit.**
- **If your business sends and/or receives large quantities of checks in the mail, use secure mailboxes for incoming mail and empty them as soon as the mail is delivered every day. If mailing checks, take them directly to the post office instead of leaving them in an outgoing mailbox for pickup or dropping them in a blue box, especially if it will not be picked up immediately.**
- **Verify the identity of anyone requesting a large payment by check to ensure that the payee's name and address are legitimate. If sending a large check, use a "proof of delivery" service or tracking mechanism.**

First Steps

- **Reconcile accounts frequently and notify the bank immediately of any discrepancies.**
- **Contact your bank about solutions to reduce the possibility of fraud.**
- **Verify any text or email or phone call supposedly from your bank – do not reply to the number in an unexpected text or click on a link in an unexpected email. Call the bank number you know and not any number in a random text or email.**
- **Educate employees and customers about fraud vulnerabilities and ways to protect themselves.**
- **Report fraud or fraud attempts immediately to your bank.**

ANY QUESTIONS?

Beneficial Ownership Reporting Requirements

Beneficial Ownership Summary

- In 2021, Congress passed (in a bipartisan effort) the Corporate Transparency Act in an effort to curb illicit finance. The law required the Financial Crimes Enforcement Network (FinCEN) to establish a beneficial ownership registry for many companies – for example a corporation, LCC or other entity created by filing a document with the secretary of state
- 23 types of entities are exempt, such as publicly traded companies and nonprofits
- Law enforcement has been requesting this type of registry to give them access to data regarding the true owners of businesses to help in their investigations and prosecutions of financial fraud
- Banks have separate requirements to gather information and keep records about beneficial owners of businesses

Beneficial Ownership Summary

- Compliance Dates – the registry was implemented January 1, 2024 and filing was required for any new businesses established on or after that date. Businesses in existence prior to January 1, 2024 must register by January 1, 2025. Information must be reported about the company itself and about the individuals who ultimately own or control it.
- Registration is free online at the FinCEN website. Bad actors are targeting businesses to "assist" in the filing, for a fee. Criminals can use this information to set up phony companies. Only use your trusted attorneys or accountants if you need assistance.
- For more information visit fincen.gov/boi

ANY QUESTIONS?