NELSON MULLINS

FINREG / FINTECH

CHECK FRAUD AND CHECK WARRANTY/LIABILITY IN BANKS

Key Concepts and Responsibilities

AGENDA

- Introduction to Check Fraud
- Types of Check Fraud
- Legal Framework
- Bank Liability
- Warranties in Check Transactions
- Risk Mitigation Strategies
- Conclusions

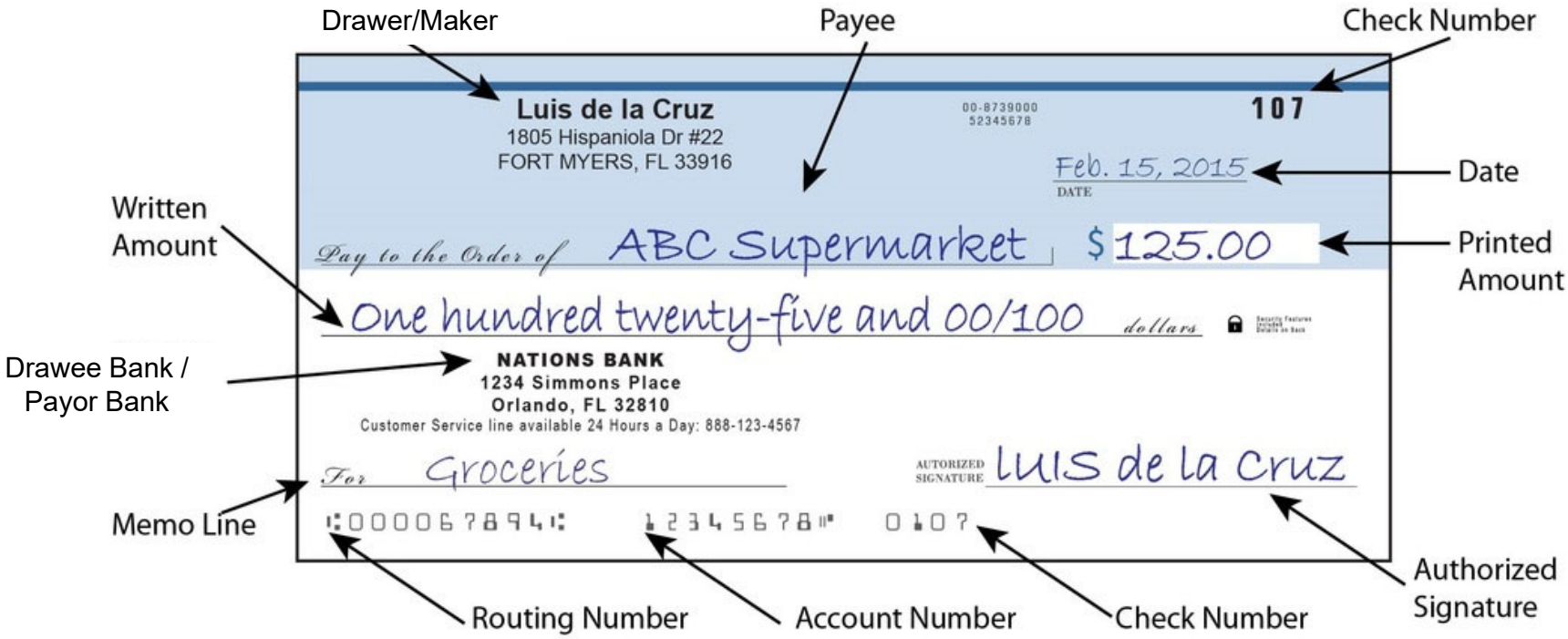
INTRODUCTION TO CHECK FRAUD

What is Check Fraud?
The illegal act of intentionally altering or falsifying a check to deceive a bank or customer.

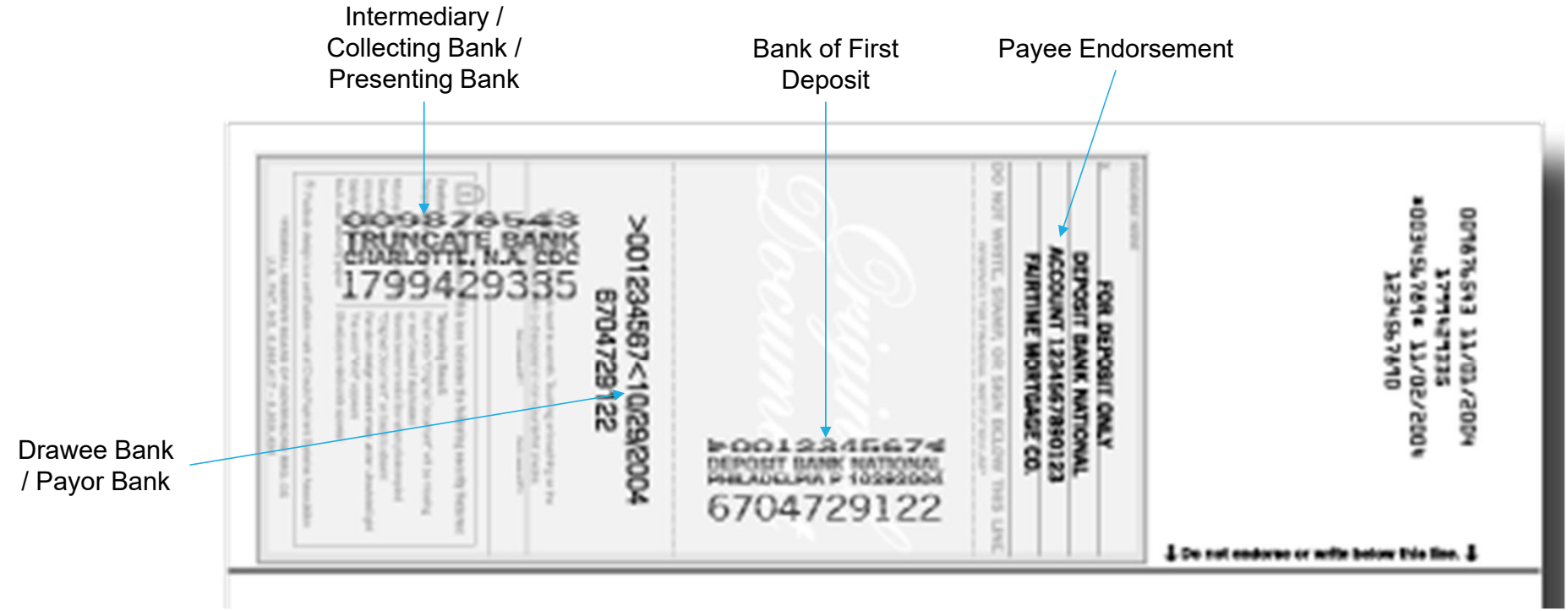
Impact on Banks and Customers:
Check fraud results in significant financial losses and damages the trust between banks and customers, as well as the hassle of "fixing" customer accounts.

Check fraud losses exceeded $20bn in 2023:
This trend accelerated with AI-based fraud. FinCEN reports a dramatic increase in check-fraud SARs, topping 500,000 in 2023.

PARTS OF A CHECK



THE BACK OF A CHECK



TYPES OF CHECK FRAUD

Forgery:
Signature forgery on checks.

Alteration:
Modifying the amount, payee, or other information.

Counterfeit Checks:
Completely fabricated checks designed to imitate legitimate ones.

Identity Theft:
Using stolen personal information to issue or cash fraudulent checks.

CHECK FORGERY

Definition:
Occurs when a person signs another individual's name on a check without permission.

Examples:
Employee forges employer's signature to embezzle funds. In-home caregiver steals a check and forges a payment to a landlord.

Detection:
Comparing the signature against those on file; using technology to identify irregularities. The days of comparing signatures by hand have passed, but new AI-based systems make this possible using technology.

CHECK ALTERATION

Definition:
Changing the check's original details, such as the payee or the amount.

Examples:
Using chemicals to wash off ink and rewriting new amounts. This can be as simple as adding a "1" at the beginning of a number and add "One Thousand" to the written amount.

Prevention and Detection:
Encouraging customers to use indelible ink pens and educating them about the risks. Encouraging business customers to use check-printing software and positive pay systems.

COUNTERFEIT CHECKS

Definition:
Creation of checks that "mirror" a real check using routing numbers and account numbers of a real account.

Examples:
Purchasing check stock at an office supply store and then printing checks with stolen routing numbers and account numbers.

Prevention and Detection:
One of the hardest to detect by a bank; but can be detected by a consumer when they receive a statement. Can be monitored by business customers or through positive pay systems.

LEGAL FRAMEWORK FOR CHECK FRAUD

Laws Governing Check Fraud:
Uniform Commercial Code (UCC) Articles 3 and 4, Regulation CC.

Responsibility:
Defines the obligations of banks and customers in cases of check fraud.

Protections for Banks:
Warranties under UCC that assign liability in fraudulent transactions.

PRESENTMENT WARRANTIES

Check presentment warranties refer to the guarantees provided when a check is presented for payment. The presenting bank warrants that:

- The check is not altered.
- The check has not been previously paid.
- The person presenting the check has the right to enforce it.

TRANSFER WARRANTIES

Check transfer warranties refer to the guarantees provided when a check is transferred to another party. The transferor warrants that:

- The transferor is entitled to enforce the check.
- All signatures on the check are authentic and authorized.
- The check has not been altered.
- The check is not subject to a defense or claim that can be asserted against the transferor.
- The transferor has no knowledge of insolvency proceedings against the maker or drawer.

ENDORSEMENT WARRANTIES

The bank of first deposit and each intermediary bank warrant that they have good title and that there are no forged endorsements.

Each intermediary bank is liable to the next bank in the "chain" of endorsements. (UCC 3-401 and 3-403).

FORGED MAKER CHECKS

A customer is generally not liable for a check drawn on the account if the customer did not sign the check or ***benefit from its proceeds***.

As against the depository bank, the drawee bank (the maker's bank) is generally liable for forged maker signatures since the drawee bank could best protect against the risk of a forged maker's signature.

The bank generally bears the risk since the check is "not properly payable." This can also happen if the check is counterfeit or if the bank agreed that more than one signature is required for a check to be payable. (This is the basic concept of UCC 4-401 – when a bank may charge its customer's account).

PAYOR BANK DEFENSES (FORGED MAKER)

The customer may have "ratified" a check by saying that they will "accept" the check or if they received the benefit of the check – such as payment of a mortgage.

Can also show that the customer previously let the forger write checks on the account – showing previous authorization.

The "*Repeat Wrongdoer Rule*" protects the bank from the same forger's actions if the customer previously received a statement showing a forgery and, after 30 days (or a shorter reasonable period) did not report the forgery. (UCC 4-406(d)).

The customer may also be blocked from contesting a check if a statement showing the check was provided and the customer did not report the fraud within one year (or a shorter period set by agreement with the bank). (UCC 4-406(f) and 4-103(a)).

FORGED PAYEE CHECKS

Depository and collecting banks warrant “good title” to a check and that no endorsement necessary to have good title has been forged.

The payor bank (drawee bank) is liable to its customer for forged payee checks.

As between the payor bank and the depository bank, the depository bank is liable for forged payee checks (since it is in the best position to protect against the fraud).

PAYOR BANK DEFENSES (FORGED PAYEE)

Generally, the Payor Bank must recredit its customer's account if it posted the check since the check was not "properly payable."

Since this fraud most commonly involves someone forging the payee's endorsement, the Payor Bank will make a warranty claim against the presenting bank. Depository and collecting banks are liable for improper endorsements. (UCC § § 3-401 and 3-403).

The Depository Bank can then seek redress against the customer whose account "received" the ill-gotten proceeds.

DEPOSITORY BANK DEFENSES (FORGED PAYEE)

Banks do not necessarily need to trust an affidavit. The Maker of the check may have falsified the affidavit.

If the Payor Bank would not be liable (untimely or repeat wrongdoer rule), then the Payor Bank suffered no loss and the Depository Bank is not liable. (Did the Payor Bank have a deposit account agreement with time periods?)

Was the Maker negligent by using a pencil? Did the Maker send it to someone with the same name as the payee? Was employee fraud involved?

Is the check a "double forgery?" – forged Maker and Payee? If so, the law generally treats the check as a forged Maker check.

Was the endorsement by an authorized signer of the payee (often the case on commercial checks)?

Did the actual payee endorse it in blank and create a "bearer check?"

CHECK CONVERSION

Checks are “converted” when it is paid on a forged endorsement.

To be “converted,” **the check must have been received by the payee and then stolen** – not just a forged payee.

Generally, the maker of the check brings suit against its payor bank under UCC 4-401.

Conversion is unique in that a payee that had the check stolen from it can bring suit against a collecting bank for conversion of the check.

Conversion is also unique in that the Payee can bring a claim against the payor bank on the amount of the check.

FICTITIOUS PAYEE

The Maker of the check may have written a check to a fictitious person – a person or company that does not exist.

If this is the case, an endorsement by anyone acting under that name is a valid, effective endorsement.

This is common when a crook "Jane Badapple" asks a victim to make a check out to "Jane Smith," her fictitious name. Anyone can legitimately endorse this check in the name of Jane Smith. This is the "***Imposter Rule***."

Similarly, if the "evil bookkeeper" makes a check out to "Jane Smith" not intending Jane Smith to have any interest in the check; then in such circumstances anyone can endorse the check in the name of "Jane Smith." This is the "***fictitious payee rule***."

If the depository bank/collecting bank acted negligently or knew of the fraud, then they cannot assert one of these rules.

ALTERED CHECKS

Altered checks start as a “real” check issued by the Maker of the check.

Not all check alterations are material – for example some banks will fix a non-existent date (i.e., February 30th checks) or alterations to a memo line.

Non-materials alterations also can occur on the Payee line if there is no material change (i.e., adding “Inc.” after the name of the payee company).

Generally, the Payor Bank cannot charge the customer’s account because the check is not properly payable. Generally, the depository bank will be liable for the loss – as it is in the best position to guard against the fraud. Also, depository and collecting banks always warrant that an item has not been altered.

ALTERED CHECKS (PAYOR BANK DEFENSES)

The Payor Bank can assert the Maker's negligence by, for instance, showing that the Maker left portions of the check incomplete, left inappropriate space on a line, or allow third parties to insert information (a friend or bookkeeper) onto the check.

If the Maker authorized a third party to complete the check, they are responsible for the writing by that third party.

The repeat wrongdoer rule applies to altered checks in the same way it applies to forgeries.

If the amount is altered, the bank can always enforce the original terms of the check, for instance, $700 can be charged to the account, even if "fifty" was added to make the amount seven hundred and fifty dollars.

AFFIDAVITS

Banks should always ask for an affidavit from the victim before they process a check fraud claim. This always helps drive home the seriousness to the victim (prevent false claims) and can be used against the other banks involved in the check-clearing process.

Have the customer review all statements and payments on the account to confirm if there is any other fraud (and to show that they did not report fraud if they later claim another loss).

Often, customers may have been engaged in "friendly fraud" and may have let another person have access to the checks. Once you present the affidavit, they may often remember that they encouraged or facilitated the fraud.

BEST PRACTICES

The only true way to stop Maker fraud, once it has occurred, is to close the account and open it under a new account number.

If a customer continues to experience repeated check fraud, the bank should carefully document its investigations and consider whether to suspend check-writing privileges on the account.

Commercial accounts can also be set for positive pay to avoid this type of fraud.

If you settle a check fraud claim where liability is not clear, work with the bank's attorneys to draft a settlement agreement. This is common when the bank and customer both claim the other acted negligently or where there is a dispute between the Payor Bank and the Depository Bank.

Always ensure that the bank is meeting its SAR filing requirements, as well.

THE MIDNIGHT DEADLINE

Often, the Payor Bank settles with the Depository Bank before they are aware of the check fraud. The Payor Bank does not make "***Final Payment***" until midnight on the next banking day of receipt. So, if a Bank receives a fraudulent check on Monday (not a federal holiday), the Bank has until midnight Tuesday to recoup the money from the Depository Bank or to refuse settlement. The Payor Bank has up until that time to refuse the settlement or recover the funds from the Depository Bank that presented the check for collection. ***This does not apply to counter-presented checks***.

After the midnight deadline, the check is "finally payable" and cannot be automatically returned. Any claims are simply warranty claims between the banks. For this reason, funds availability may be delayed by the depository bank because of the right of the bank to refuse or reclaim the funds until Final Payment is made.

CHECK KITING

Check kiting occurs when a fraudster makes use of the "float" period and opens accounts at two different banks. Checks from one bank are then used to "cover" the checks at the other bank.

- Fraudster writes $500 check on Bank A and deposits at Bank B.
- Fraudster writes $600 check on Bank B and deposits in Bank A, to "cover" the $500 check.
- Fraudster writes $700 check on Bank A and deposits in Bank B, to "cover" the $600 check.
- The kite continues until one of the banks detects the fraud.

Generally, the bank that first detects the kiting scheme and places a hold on the funds wins the battle between the banks as to who is liable.

BEST PRACTICES FOR RISK MITIGATION

Employee Training:
Regular training on detecting fraud and unusual check behavior. Especially focus on commercial banking representatives and educate on new typologies, like accounts payable fraud schemes.

Customer Training:
Conduct training of customers, particularly large dollar small businesses regarding check fraud. Be particularly careful with check-heaving businesses like car dealerships and attorney accounts. Encourage regular monitoring of accounts and prompt notification.

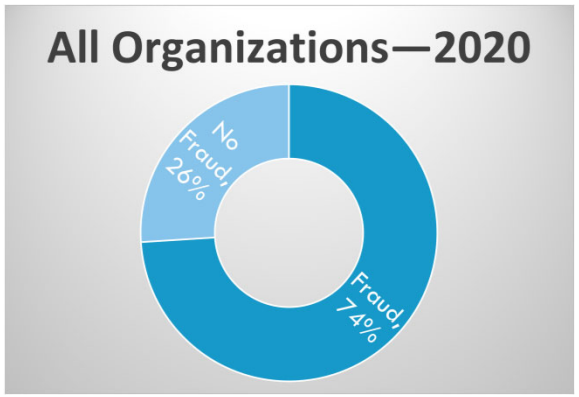
Enhanced Technology:
Every year, core systems are improving check fraud technology. Encourage customers to use remote deposit capture or mobile deposits. Encourage and incentivize positive pay for customers.

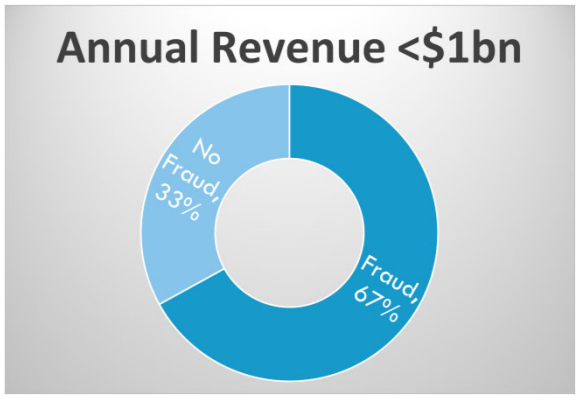
Business Email Compromise (BEC) and the Most Common Form of Fraud

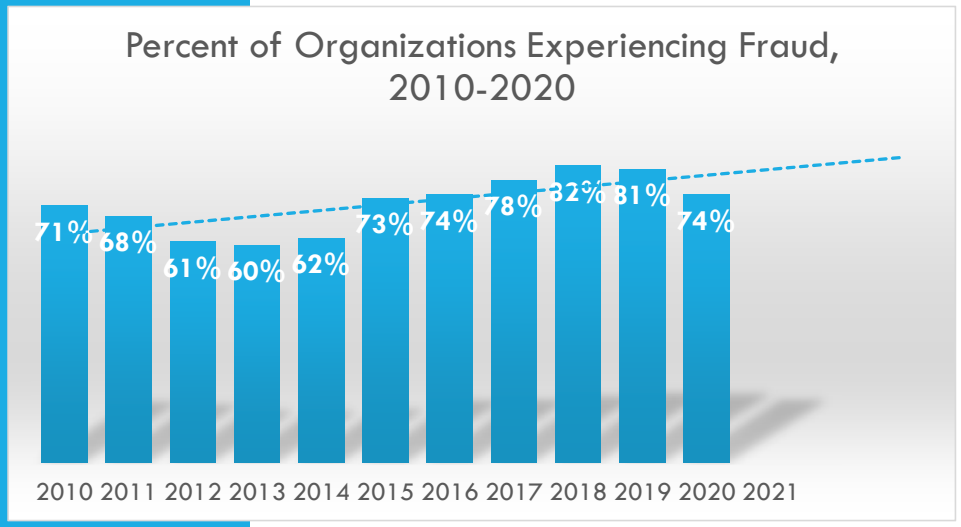
A CASE STUDY

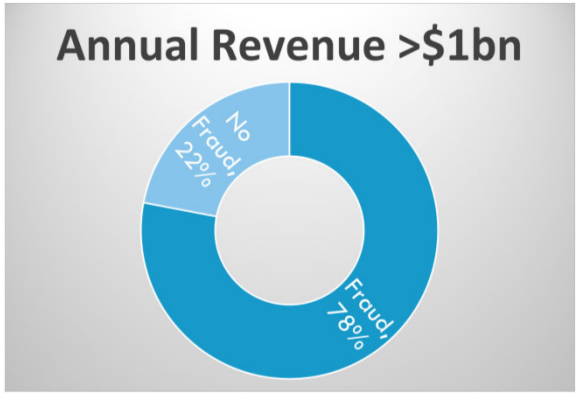
KEY STATISTICS WORTH KNOWING

Nearly 75% of all organizations were targets of a payment fraud attack in 2020.

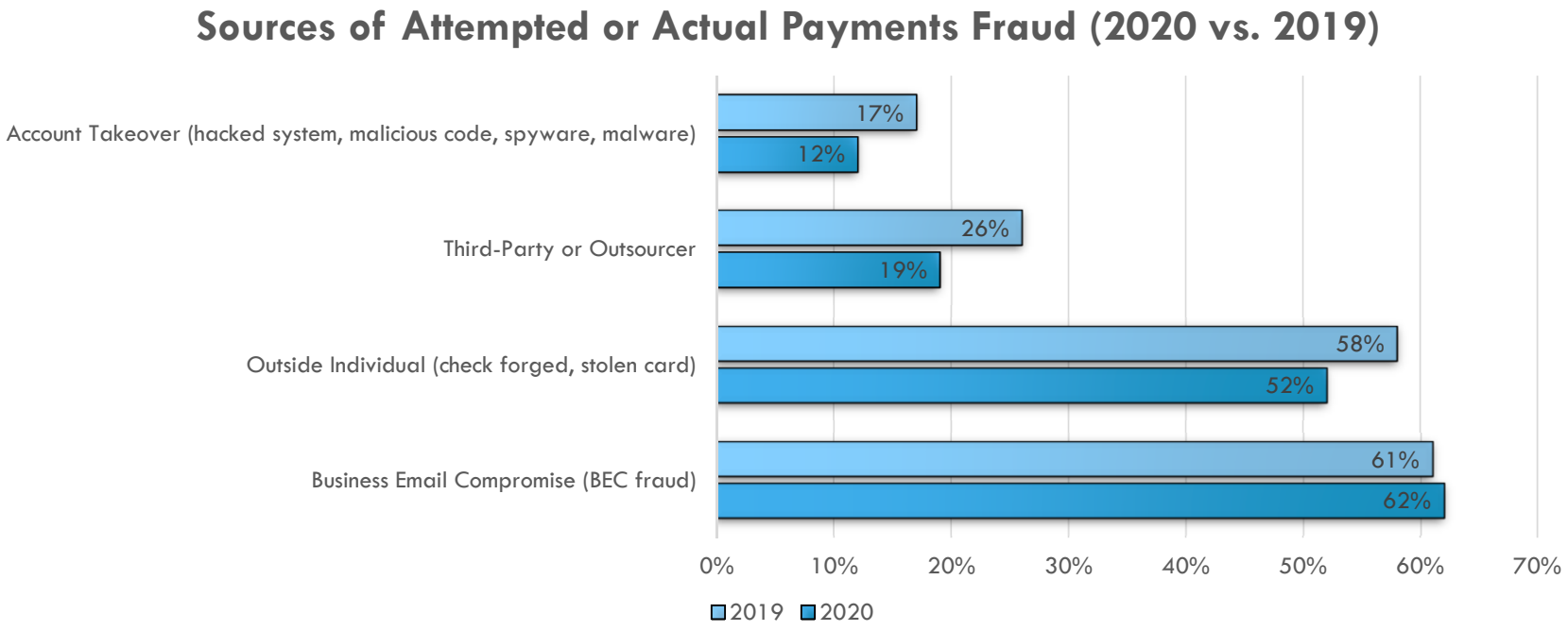




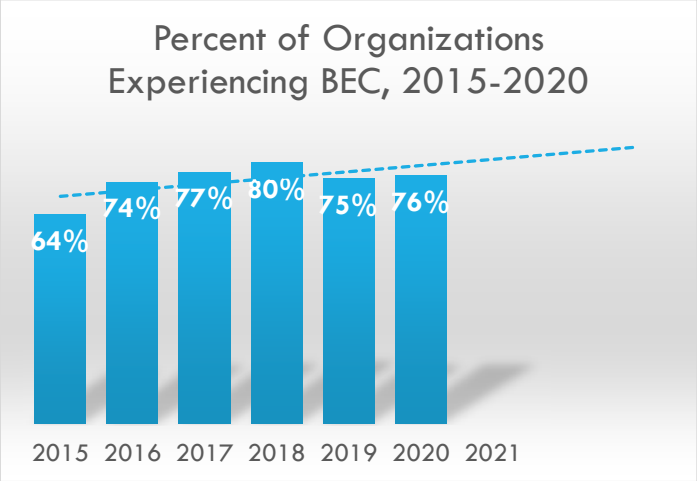




SOURCES OF PAYMENT FRAUD



THE FOCUS ON EMAIL FRAUD



	Less than 25 Instances Annually	26-100 Instances Annually	101-200 Instances Annually	200+ Instances Annually
Emails from 3rd parties requesting change of bank accounts, payment instructions, etc.	88%	9%	2%	1%
Emails from fraudsters pretending to be senior executives using spoofed email domains directing finance personnel to transfer funds to fraudsters' accounts	87%	9%	2%	2%
Emails from fraudsters impersonating vendors (using vendors' actual but hacked email addresses) directing transfers based on real invoices to the fraudsters' accounts	87%	11%	1%	1%

THE BEC STRATEGY

FBI Data:

- 4,620 Incidents per Month
- $728 million Exposed Losses per Month (US and Foreign)
- $281 million Exposed Losses per Month (Domestic)
- 1,927 Victims each Month

THE BOTTOM LINE

54% of Organizations reported Financial Losses as a result of Business Email Compromises

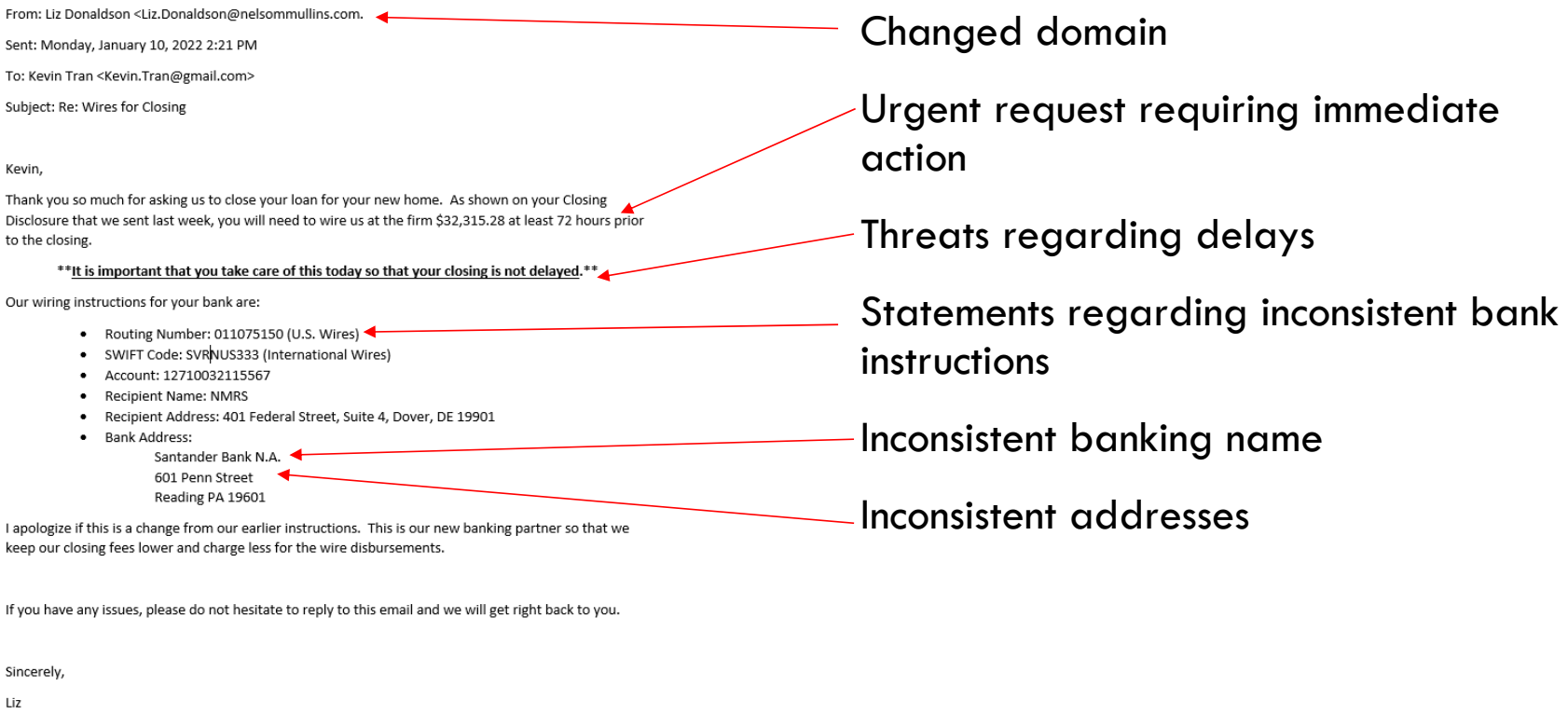
WAYS TO COMBAT PAYMENTS FRAUD BY EMAIL

End-User Education	Training on the BEC threat and how to identify spear phishing attempts
Company Policies	Implementing appropriate verification of any changes to existing invoices, bank deposit information, and contact information
Request Confirmations	Similar to banks, implementing a call back to an authorized contact at the payee organizations using an existing phone number from a system of record maintained by your organization
Stronger Internal Controls	Prohibiting payment initiations based on emails or other less secure messaging systems
Multi-Level Authorization	Requiring second person sign-off or senior management approval for transactions over certain thresholds
Two-Factor Authentication	Adding layers of security for access to company networks and network infrastructure that handles outbound payments
Color-Coded Emails	Adding systems that clearly flag that emails have originated from outside your organization.
Intrusion Detecting Systems	Adding systems that clearly flag emails where the sender is attempting to closely replicate an internal email address (e.g., replacing “Nelson” with “Nelsom”)
Email Restrictions	Flagging or prohibiting emails where the “reply” email address is different from the “from” email address shown in the email

BEC "RED FLAGS"

- Unexplained urgency
- Last minute changes in wire instructions or recipient account information
- Last minute changes in established communication platforms or email account addresses
- Communications only in email and refusal to communicate via telephone or online voice or video platforms
- Requests for advance payment of services when not previously required
- Requests from employees to change direct deposit information

SPOOFING LAW EMAIL ACCOUNT



From: Liz Donaldson <Liz.Donaldson@nelsommullins.com.

Sent: Monday, January 10, 2022 2:21 PM

To: Kevin Tran <Kevin.Tran@gmail.com>

Subject: Re: Wires for Closing

Kevin,

Thank you so much for asking us to close your loan for your new home. As shown on your Closing Disclosure that we sent last week, you will need to wire us at the firm $32,315.28 at least 72 hours prior to the closing.

It is important that you take care of this today so that your closing is not delayed.

Our wiring instructions for your bank are:

- Routing Number: 011075150 (U.S. Wires)
- SWIFT Code: SVRNUS333 (International Wires)
- Account: 12710032115567
- Recipient Name: NMRS
- Recipient Address: 401 Federal Street, Suite 4, Dover, DE 19901
- Bank Address:
  Santander Bank N.A.
  601 Penn Street
  Reading PA 19601

I apologize if this is a change from our earlier instructions. This is our new banking partner so that we keep our closing fees lower and charge less for the wire disbursements.

If you have any issues, please do not hesitate to reply to this email and we will get right back to you.

Sincerely,

Liz

POINTERS FOR TRUSTEES, ATTORNEYS, AND BUSINESS MANAGERS – SPREAD THE WORD!

Remember, the business is the front line. Business owners and staff have an affirmative duty to remain up-to-date regarding fraud schemes.

Business owners should be training staff on risks and ways to combat potential hackers and fraudsters.

Understand that **email is not a secure way of sending information**!

Consider using secure email systems instead of unencrypted emails to communicate with clients.

Have call back or multi-factor authentication to confirm payment instructions from client.

Maintain proper firewalls and anti-virus programs.

Avoid any storing of PCI-DSS (payment card data) on systems (or transmitting this information).

Make sure all software is updated and fully patched.

Maximize browser security.

Segregate accounting/online banking computers from social media or personal-use computers.

Implement strong password policies and robust IT security procedures.

Never wire funds based on email instructions, alone.

Immediately speak to the bank and a knowledgeable financial fraud and cybersecurity attorney if your business / firm / organization / general counsel's office is the subject of fraud.

Proactively consult with insurance providers regarding coverage for losses and obligations under cyber policies.

NELSON MULLINS

QUESTIONS OR FOLLOW UP?

Dowse B. ("Brad") Rustin IV

Chair, Financial Regulatory Practice

Brad.Rustin@nelsonmullins.com

202.689.2320 (DC)

864.373.2320 (SC)

www.nelsonmullins.com/people/dowse-rustin

ABOUT THIS PRESENTATION

Nelson Mullins Riley & Scarborough LLP ("Nelson Mullins") provides this material for informational purposes only. Certain images, courtesy ChatGPT4.0.

The material provided herein is general and is not intended to be legal advice.

Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations, and other legal issues unique to your circumstances.

Receipt of this material does not establish an attorney-client relationship.

Nelson Mullins is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case or engagement is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements or marketing materials.