Navigating the Landscape of Payments Fraud

Chris Selmi, *AAP, APRP*

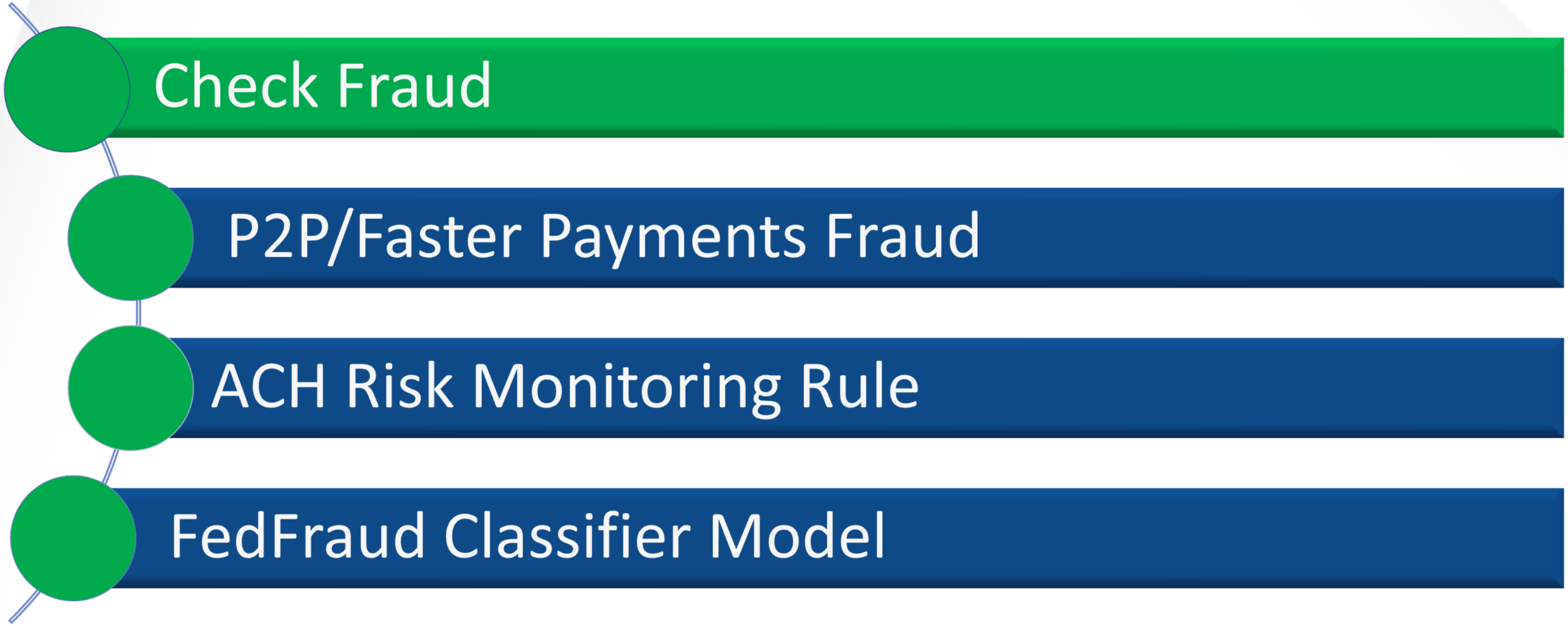
wespay

Shaping the Future of Payments

Agenda

- Check Fraud
- P2P/Faster Payments Fraud
- ACH Risk Monitoring Rule
- FedFraud Classifier Model

Agenda



- Check Fraud
- P2P/Faster Payments Fraud
- ACH Risk Monitoring Rule
- FedFraud Classifier Model

Check Fraud on the Rise

Check fraud losses are projected to exceed $24B in 2024

65% organizations reported check fraud in 2024, the most susceptible payment method

20% of organizations reported fraud due to interference with USPS (10% higher than in 2022).

70% of organizations have no immediate plans to discontinue use of checks

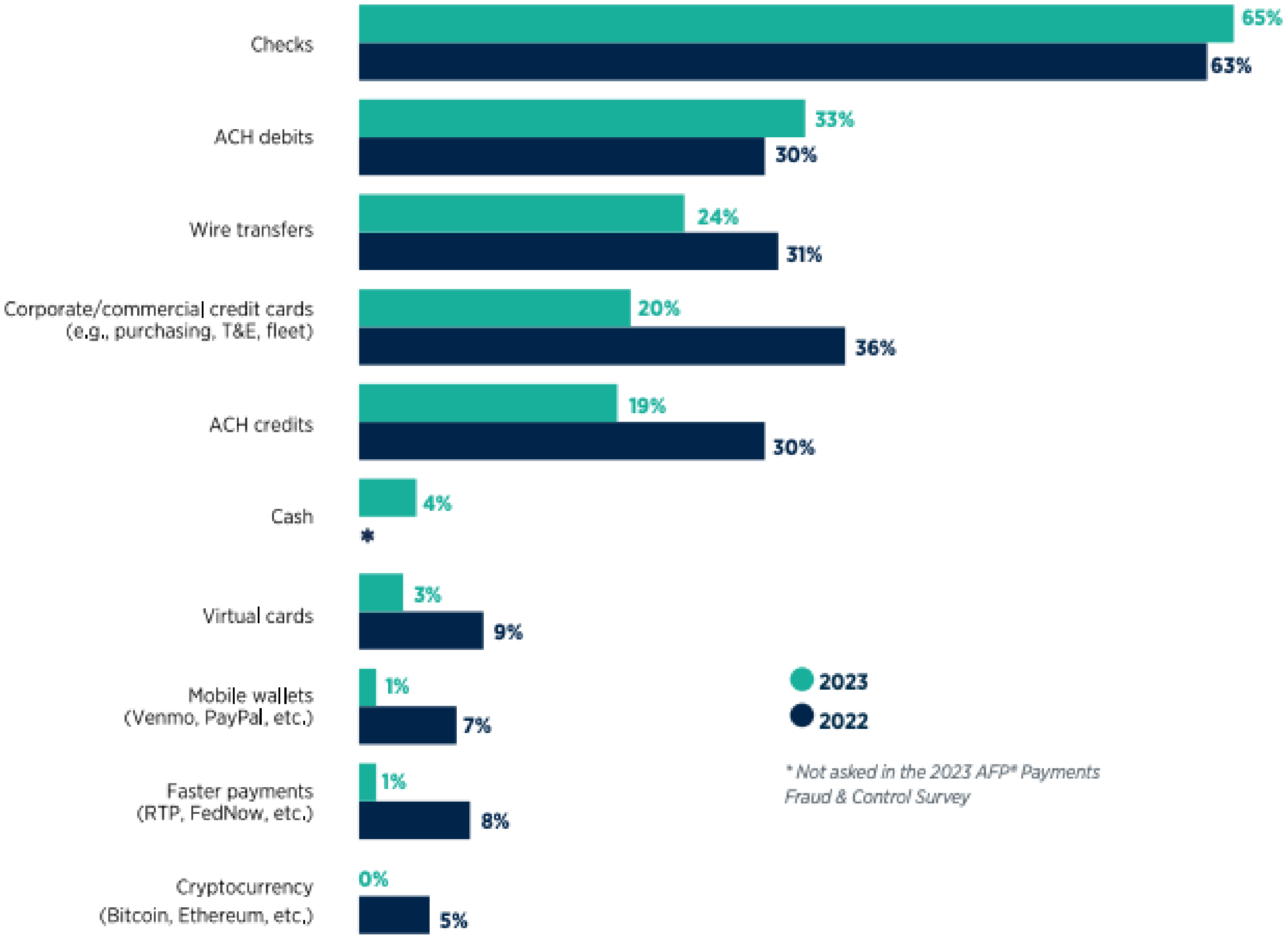
*Taken from 2024 AFP Payments Fraud and Control Survey

wespay

Check Fraud Statistics

- 90% of all forged checks are drawn on bank accounts that are less than one year old (AARP)
- 680,000 SARS were filed in 2022 related to check fraud (all-time high) (FinCEN)
- Mail theft is skyrocketing, from fewer than 60,000 complaints in 2018 to >250,000 in 2023 (CBS News)
- 1/3 of U.S. small businesses were victims of check fraud in 2023, with 65% of those reporting losses of >$50,000
- Check fraud losses are projected to exceed $24B in 2024

Payment Methods Subject to Attempted/Actual Fraud



** Not asked in the 2023 AFP® Payments Fraud & Control Survey*

Estimated Check Fraud Attempts

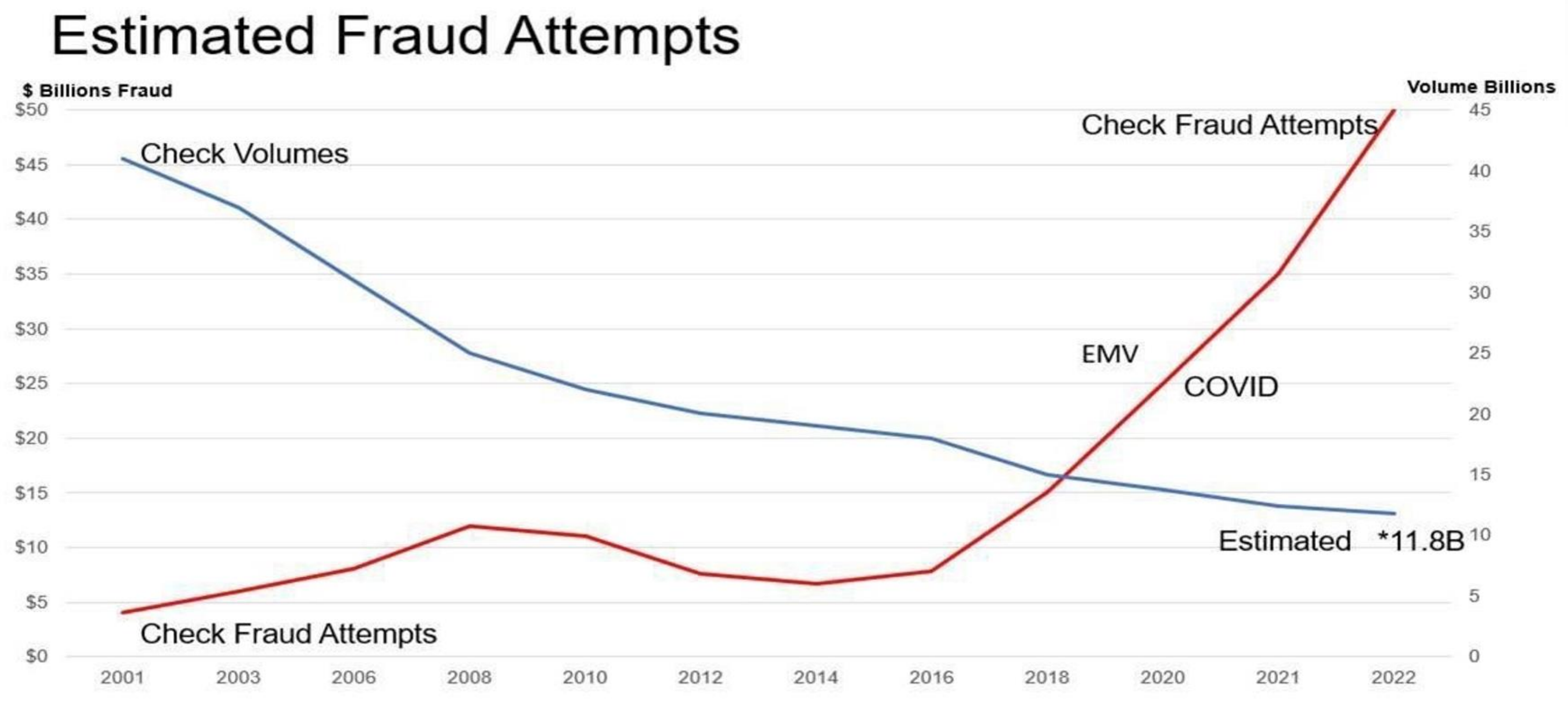


Chart created by OrboGraph: Sources: Multiple news publications, FED check volume research, additional 3rd party sources, internal resources

- Paper checks are one of the weakest points of financial systems
- Check fraud has dramatically increased since introduction of EMV chip cards and Pandemic

Alterations

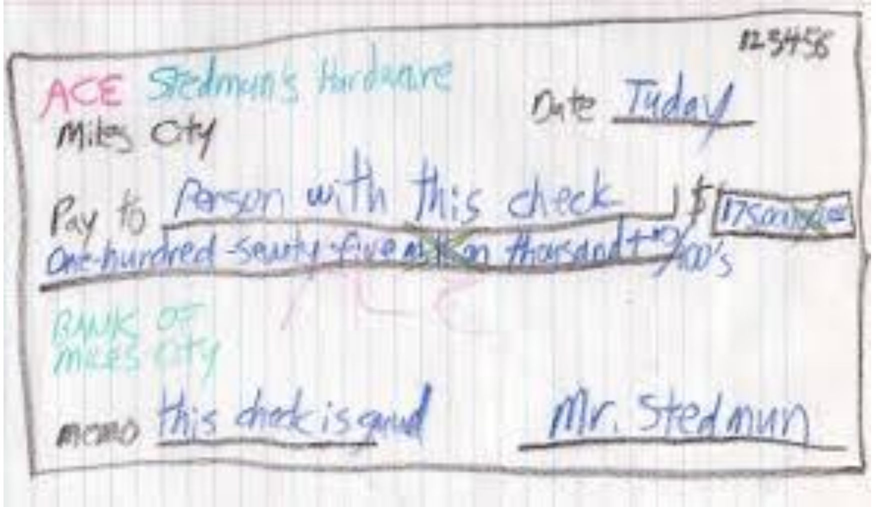
- Unauthorized change or additional of an amount, payee, or date, or an unauthorized addition of words, numbers, or other changes to an incomplete instrument, modified to benefit the perpetrator

- Methods of alteration
  - Check washing
  - Laser printer
  - Check imprinter
  - Typewriter
  - Handwriting
  - MICR line altered or damaged to delay clearing or return

Counterfeit Checks

- Counterfeit Checks: False checks drawn on valid accounts
  - Some security features are not captured by RDC

- Common characteristics
  - Poor quality paper stock
  - Misspelled printed information
  - MICR line missing, skewed, not machine readable
  - Fractional RTN different than MICR line
  - Check number in wrong position on MICR line



#23456

ACE Stedmun's Hardware
Miles City

Date Today

Pay to Person with this check $ 175,000.00

One-hundred -Seventy-five [illegible] thousand + 00/100's

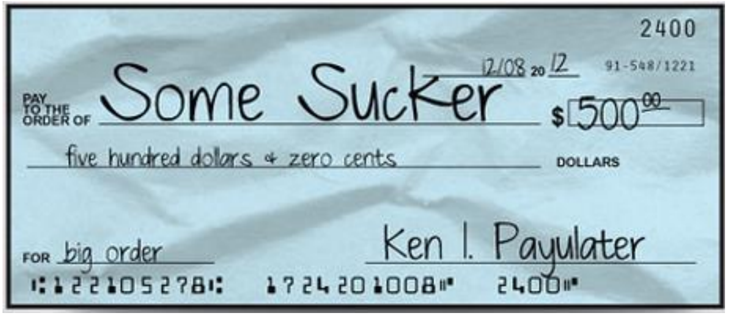
BANK OF
MILES City

memo this check is good

Mr. Stedmun

Forged Maker Signature

- Use of legitimate blank checks with a false imitation of the payor signature (unauthorized signature)
  - Forged/Counterfeit check
    - Return must be within UCC midnight deadline
  - Perpetrated by person known to payor
  - Check orders stolen from mailbox
    - Banks may combat in different ways such as different mailing/packaging, etc.



2400

12/08 20 12 91-548/1221

PAY TO THE ORDER OF Some Sucker $ 500^{00}

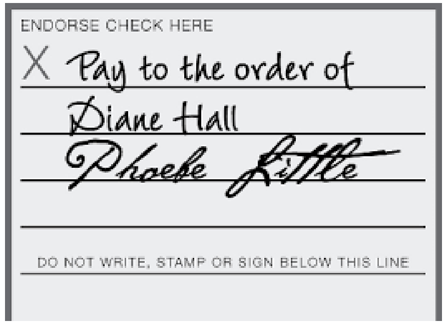
five hundred dollars + zero cents DOLLARS

FOR big order Ken I. Payulater

⑆122105278⑆ 1724201008⑈ 2400⑈

Forged Indorsement

- Check is payable to multiple parties
  - One party forges the indorsements of all payees and negotiates the check
- Check payable to a merchant or consumer
    - Check stolen and payee indorsement forged to negotiate the check
- Breach of UCC Transfer & Presentment warranties
  - Person transferring and/or presenting the item for payment is “entitled to enforce” the item
  - Liability lies with the Bank of First Deposit


ENDORSE CHECK HERE

X Pay to the order of

Diane Hall

Phoebe Little

DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE

Duplicate Deposits

- When fraudster using the same check to make multiple deposits via a remote deposit capture service
  - Higher risk for duplicate deposits via mobile RDC

- BOFD warrants that the item will not be deposited elsewhere. And if they do, BOFD is liable

Possible Risk Mitigation

- Know Your Accountholder
  - How long have they been a client?
  - Review past statements for returned items
  - How many times overdrawn?
    - NSF vs. UCF
  - How many checks deposited in the last week/month/year?
  - Place limits on high-risk transactions (i.e., remote deposits, transfers between FIs)
  - Use longer Reg CC hold times for new/frequently overdrawn/NSF accounts

- Presumption of Alteration
  - BOFD: Do your research before accepting a forged return

Possible Risk Mitigation

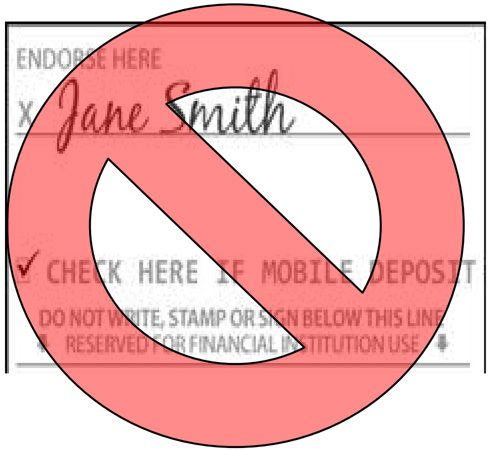
- Spot checking
  - Pull deposited items & check payee names, etc.

- Periodic review
  - Review deposit history for trends
  - Software can perform this using analytics

- What happens to the item and image?
  - Send a message with client responsibility
    - Secure source document
    - Destroy after elapsed time period

RDC Restrictive Endorsements

- Must be a physical endorsement
- Must contain a minimum of 2 elements:
  - Method of deposit (For Mobile Deposit Only)
  - Intended depository institution (To ABC Bank)

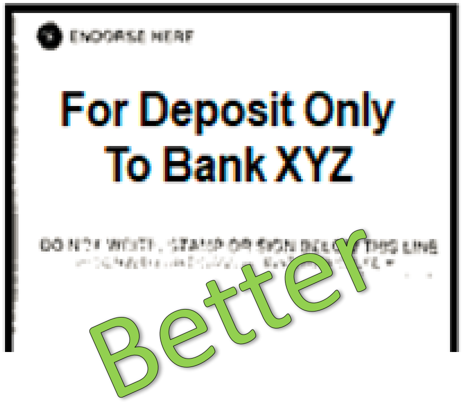


ENDORSE HERE

X Jane Smith

✓ CHECK HERE IF MOBILE DEPOSIT

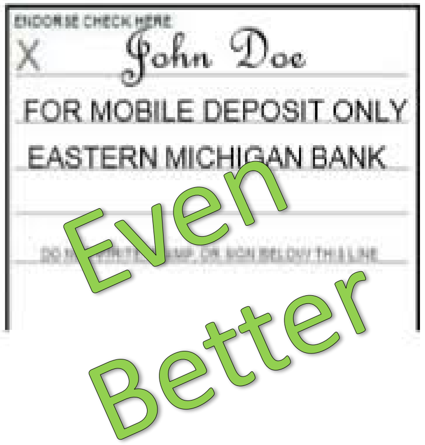
DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE
RESERVED FOR FINANCIAL INSTITUTION USE



ENDORSE HERE

For Deposit Only
To Bank XYZ

DO NOT WRITE, STAMP OR SIGN BELOW THIS LINE



ENDORSE CHECK HERE

X John Doe

FOR MOBILE DEPOSIT ONLY
EASTERN MICHIGAN BANK

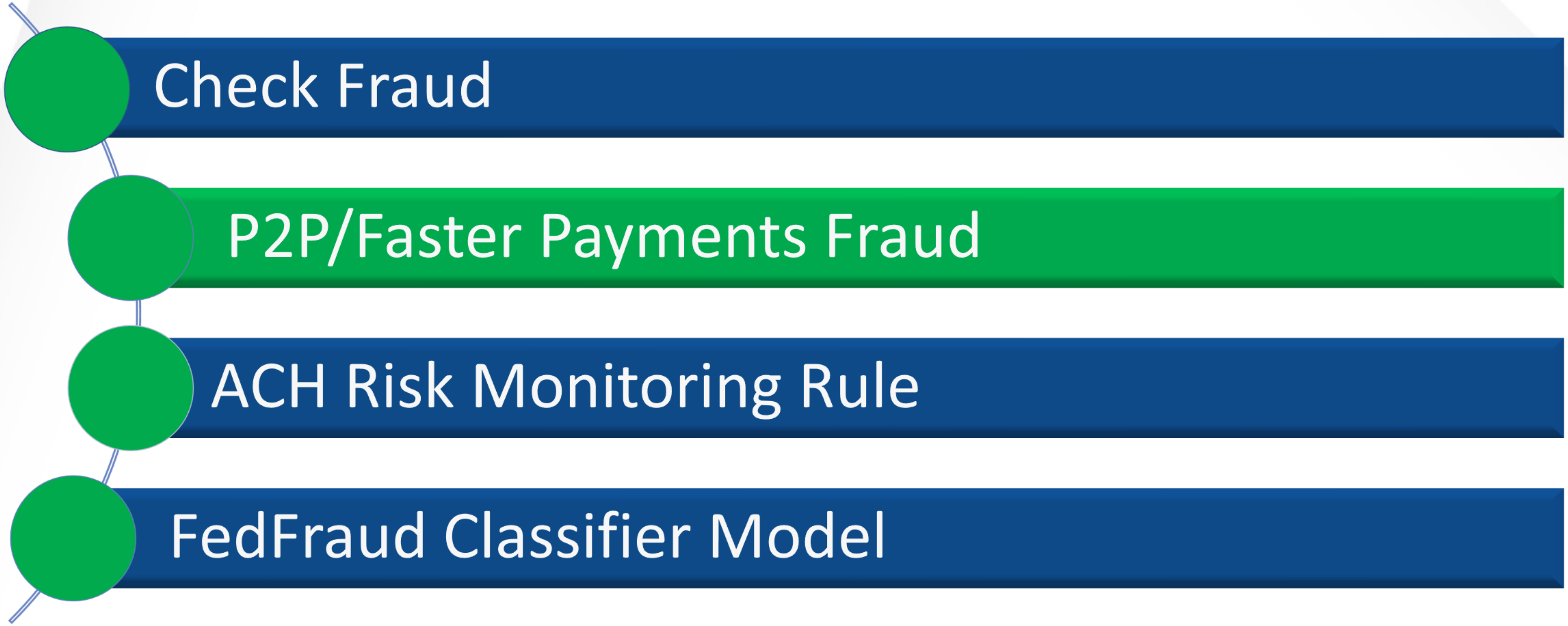
DO NOT WRITE, STAMP, OR SIGN BELOW THIS LINE

Even
Better

RDC Fraud Tactics

- **Image Analysis Technology** to detect signs of tampering
- **Duplicate Detection** to combat double deposit fraud across multiple branches/institutions
- **Transaction Limits and Hold Periods** especially for new customers or high-risk activity accounts
- **Geolocation and Behavioral Monitoring** using customer data to identify unusual deposit patterns

Agenda



- Check Fraud
- P2P/Faster Payments Fraud
- ACH Risk Monitoring Rule
- FedFraud Classifier Model

P2P Metrics

P2P fraud is increasing as payment options are accessible, fast and convenient

$1.4T P2P TRANSACTIONS WERE MADE IN 2023 (28.5% INCREASE OVER 2022) (FTC)

159M U.S. RESIDENTS MADE AT LEAST ONE P2P MOBILE PAYMENT IN 2023 (FTC)

CONSUMERS REPORTED LOSING **$2.7B** IN P2P FRAUD IN 2022 AND **$2.1B** IN 2023 (ACCORDING TO FTC)

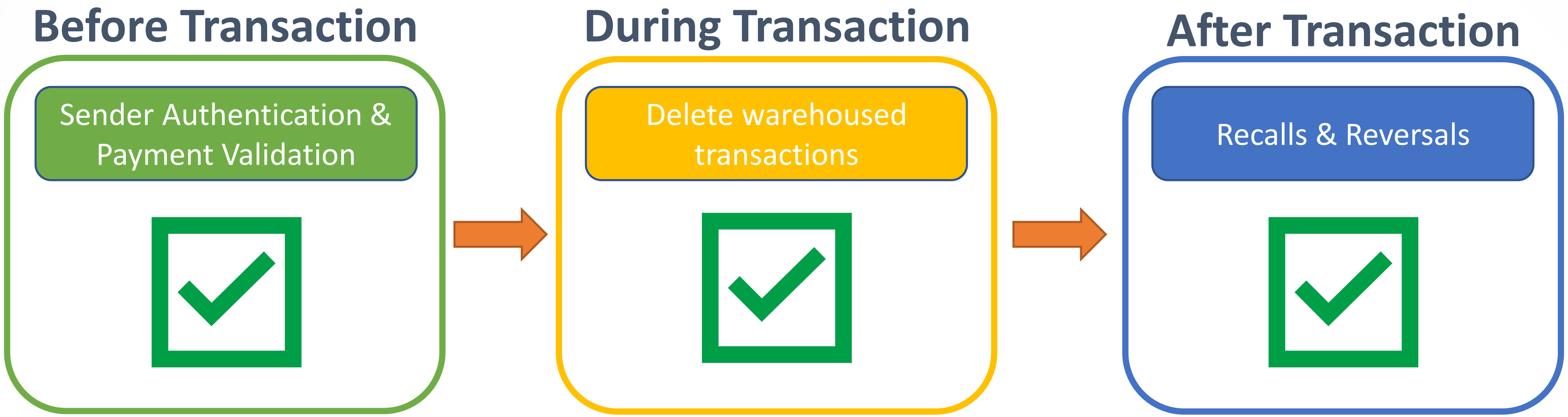
8% OF BANKING CUSTOMERS REPORTED BEING THE VICTIM OF P2P PAYMENTS SCAM IN 2023

Fraud Tied to P2P & Faster Payments

- Phishing
- Business Email Compromise
- Unauthorized transfers
- Accidental transfers
- Impersonation or imposter scams

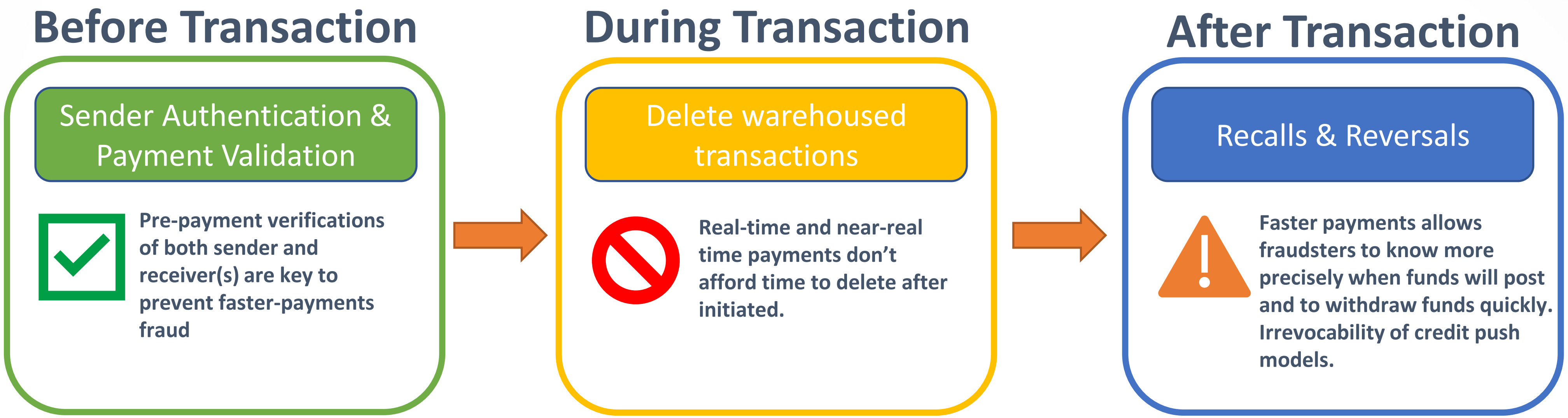
Fraud Mitigation Opportunities

- Traditional “Next-Day” payments allow opportunities for fraud prevention and mitigation across all three phases of a transaction:



Fraud Mitigation Opportunities

- Faster Payments limit fraud opportunities primarily to ”before” phase:



Before Transaction

Sender Authentication & Payment Validation

✓ **Pre-payment verifications of both sender and receiver(s) are key to prevent faster-payments fraud**

During Transaction

Delete warehoused transactions

🚫 **Real-time and near-real time payments don’t afford time to delete after initiated.**

After Transaction

Recalls & Reversals

⚠ **Faster payments allows fraudsters to know more precisely when funds will post and to withdraw funds quickly. Irrevocability of credit push models.**

P2P Scam vs. Fraud

- Zelle's Definition of "Scam:"
  - Customer knowingly involved in the transaction and ***authorized*** a payment to be sent, even if consumer was tricked or persuaded to OK a payment for a good or service not provided
    - Examples: Ticket purchases, buying pets, cash flip scams
  - Customer has no recourse if purchased item never received
  - Customer is at mercy of the stranger to send the money back

- Customers can believe that because external P2P services are offered through their FI that they are eligible for same level of protection/assistance if something goes wrong

P2P Scam vs. Fraud

- Zelle’s Definition of “Fraud:”
  - ***Unauthorized*** transaction sent from customer’s account
    - Fraudster gains access to customer’s bank account without permission
  - Consumers are protected by Reg E
    - Consumer senders will contact their FI to dispute the debit posted to their account that funded the outbound Zelle credit
  - Fraudsters use spoofing/social engineering to obtain consumer’s online banking credentials or create a Zelle account in their name

Customers should be instructed to only use service to pay people they know and trust!

Scam vs. Fraud

Scam

Authorized payment

Example: Customer purchases Super Bowl tickets with Zelle.

Customer has no recourse to dispute an authorized payment with its FI. Only option is to request funds back from seller.

Fraud

Unauthorized payment

Example: Online banking credentials are compromised, Fraudster enrolls customer in Zelle and transfers credits to an account controlled by fraudster.

Consumer customers are protected by Reg E.

Customers should think of using P2P services like they do cash – you wouldn't mail cash to a stranger!

P2P Sound Practices

New Account Limits

- Deterrent to fraudsters who want speed and high amounts

Monitor Account Owner Contact Information Changes

- Helps to identify fraudsters attempting to disassociate an account from its owner. Particularly suspicious for new account openings.

Account Alerts

- Promote out-of-band notifications to accountholders. Especially important for P2P transfer initiations and account maintenance/contact information changes.

Sound Practices

Cross-Channel Fraud Monitor

- Monitoring transactional activity across payment channels can help identify suspicious activity and provide context to seemingly harmless individual transactions.

Monitor Victimized Accounts

- Monitor activity of prior victims of fraudulent transactions or scams. Compels fraudsters to use new accounts and can help to proactively identify fraudulent transactions before the accountholder transfers the funds.

Sound Practices

Tokenization/MFA of Online Banking Credentials

- First line of defense in preventing payments fraud is to keep fraudsters from accessing banking credentials. With P2P services linked to OLB, there is more value for fraudsters in obtaining banking credentials.

Payee Validation

- Once fraudsters have access to account, the next line of defense is ensuring they cannot add new payees to send funds to. Requiring out-of-band authentication and potentially delay the confirmation of new payees to slow fraudsters down.

P2P Sound Practices

Terms & Conditions

- Verify the Terms & Conditions of your P2P service providers (when do they have financial responsibility for something that goes wrong)

Master Switch

- Provide ability for customers to turn off P2P from inside online banking

Consistent Policies & Procedures

- Document your FI’s scam vs. fraud policy and procedures so that you are handling issues consistently across your organization.

Sound Practices

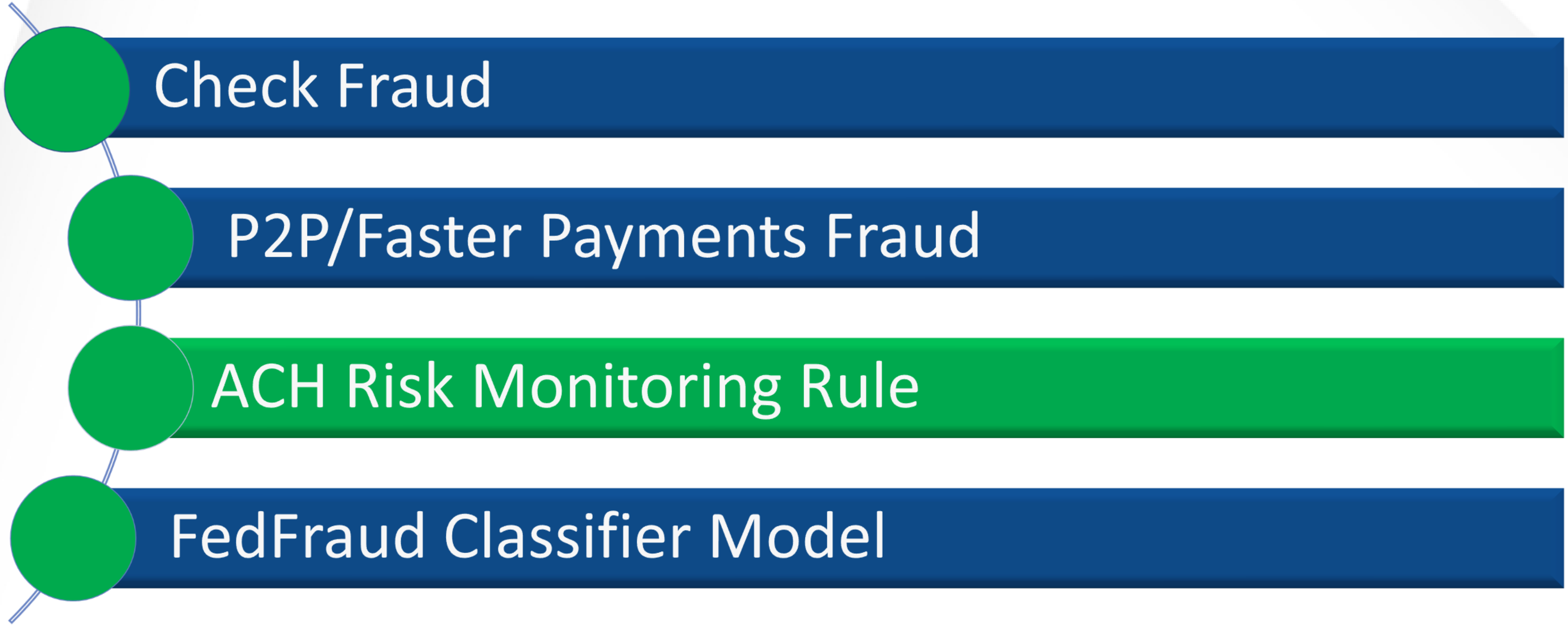
Customer & Staff Education

- Customers and staff should understand the responsibilities the FI and customers both have to prevent and recover fraud. Remind accountholders not to send money to strangers or use P2P services to purchase goods/services.

Threat Intelligence

- Every FI must keep up to date with the types of schemes used by fraudsters and analyze the components of each scheme to evaluate the effectiveness of their controls.

Agenda



- Check Fraud
- P2P/Faster Payments Fraud
- ACH Risk Monitoring Rule
- FedFraud Classifier Model

Background

Fraud monitoring rules are part of a larger Risk Management package of Rules intended to reduce incidence of fraud attempts and improve the recovery of funds after frauds have occurred.

These Risk Management Topics were born out of the lessons learned from the COVID-era credit disbursements (e.g., EIPs, State UI, SBA, etc.)

ACH Fraud Monitoring Rule Summary

- Requires ACH Receiving FIs (RDFIs) to establish and implement risk-based processes and procedures designed to identify *credit* entries initiated due to fraud or under False Pretenses

- Requires Originators, Third-Party Service Providers, Third-Party Senders and Sending FIs (ODFIs) to establish and implement risk-based processes and procedures reasonably intended to identify *all* ACH entries initiated due to fraud or under False Pretenses

ACH Fraud Monitoring Rule Implementation Dates

Network Participant	Phase 1 (March 20, 2026)	Phase 2 (June 19, 2026)
RDFIs	Applies to RDFIs with annual ACH receipt volume of 10 million or greater in 2023	Applies to all RDFIs
Originators, TPSs, TPSPs, ODFIs	Applies to all ODFIs and Originators, TPSs, TPSPs with annual ACH origination volume of 6 million or greater in 2023	Applies to all ODFIs, Originators, TPSs, TPSPs

FI Fraud Monitoring Requirements

- FIs will be required to establish and implement risk-based processes and procedures, relevant to the role it plays in connection with the receipt and origination of ACH entries.

- Each FI must review such processes and procedures at least annually and make appropriate updates to address evolving risks
  - Incorporate into annual ACH audit

Originating FI Considerations

- How to educate their Originators & Third-Parties on new requirements?

- When to inform them so they have time to comply?

- What level of monitoring/oversight is appropriate?

- ACH Origination Agreement changes to protect yourself?

General Preparation Guidance

1. Evaluate the controls you have in place today
   - It’s likely that your organization already has procedures/policies to monitor against fraud
   - Common ODFI controls:
     - Anomaly monitoring
     - Velocity/dollar limits
     - Return rate monitoring
   - Common RDFI controls:
     - Anomaly monitoring
     - Name matching

General Preparation Guidance

2. Evaluate the effectiveness of existing controls

- ODFI controls
  - Opportunity to tighten monitoring controls for higher-risk Originators
  - Are Originator return rates within Nacha-allowed limits or are there frequent exceptions
  - Receiving high number of requests for proof of authorizations

- RDFI controls
  - Opportunity to tighten monitoring controls for higher-risk accountholders (i.e., new, large dollar recipients, receivers of early-post credits (if applicable)
  - Analyze dispute demographics/volumes of unauthorized returns

General Preparation Guidance

3. Implement new controls

- Additional controls can be in-house or vendor-supplied
  - Discuss with your service & security providers about their plans for complying
- Solutions should be commensurate with your risk-appetite, size, and ACH operation complexity

General Preparation Guidance

- Industry focus on this rule change throughout 2025
  - Wespay working with Center for Payments to survey how industry players monitor for fraud today

- Nacha Resources: https://www.nacha.org/rules/risk-management-topics-fraud-monitoring-phase-1

Agenda

- Check Fraud
- P2P/Faster Payments Fraud
- ACH Risk Monitoring Rule
- FedFraud Classifier Model

Why Did the Fed Develop FraudClassifier Model?

- Inconsistent fraud data has long been an industry challenge
  - Lack of consistent fraud classifications and definitions across payment channels and organizations

- Leads to untimely sharing of fraud information
  - Takes time to standardize fraud data for industry studies

Who Developed FraudClassifier Model?

- Fraud Definitions Work Group
  - Established in March 2019 as part of the Fed’s initiative to advance its strategy for improving the U.S. payment system
  - Goal is to address industry challenges stemming from inconsistent fraud classification and lags in reporting
  - Comprised of 23 industry fraud experts
    - Member list is public and can be found on the Fed’s website: https://fedpaymentsimprovement.org/wp-content/uploads/fdwg-member-list.pdf

What is the FraudClassifier Model?

www.FedPaymentsImprovement.org

- A classification tool that can be used to classify fraud across payment type or channel in simple and consistent manner

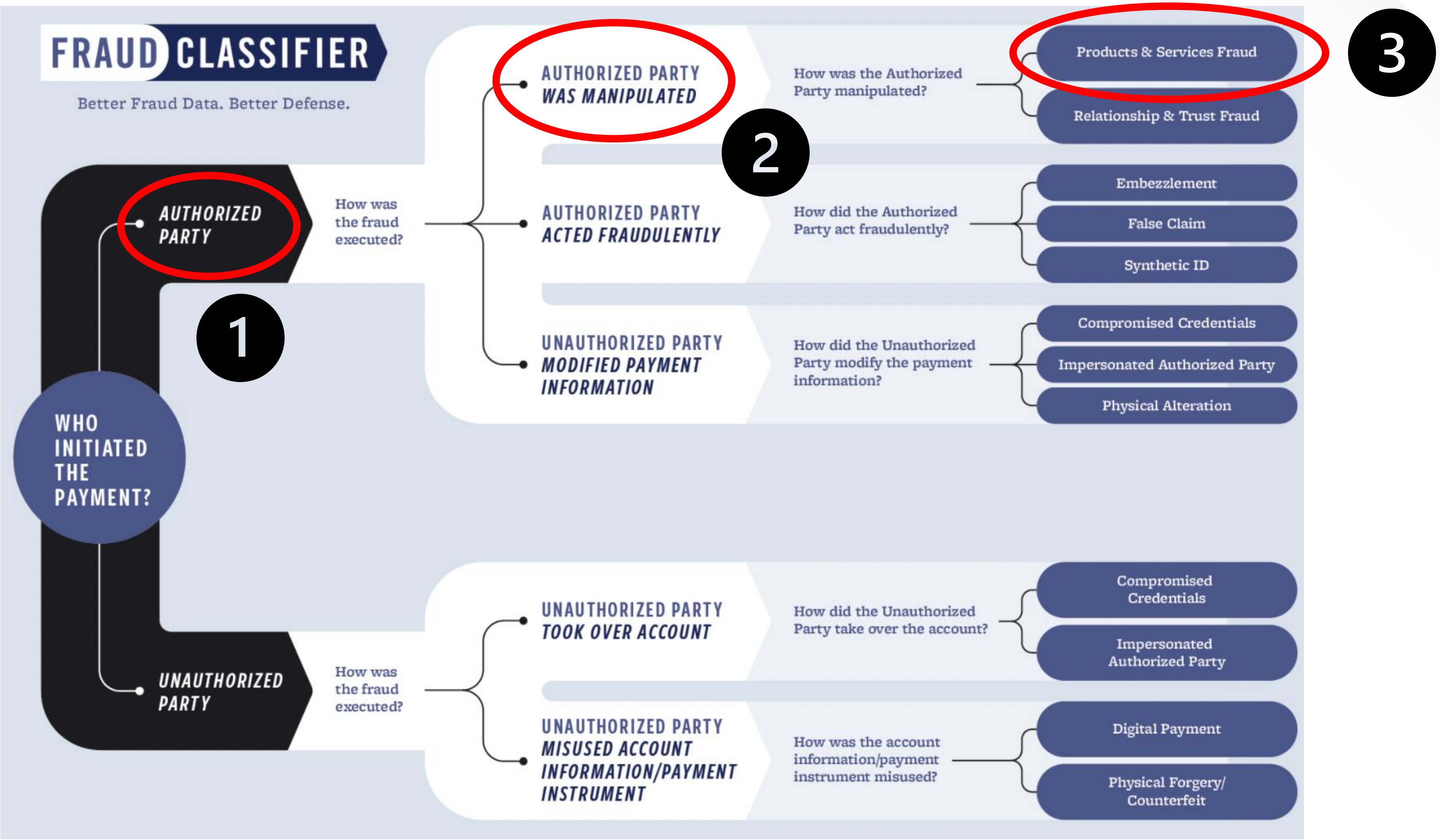
- Provides ability for an organization to:
  - Understand component parts of each type of fraud
  - Identify potential weak points of their own fraud controls
  - Easily see shared/different characteristics of each type of fraud
  - Speak the same language with other organizations when working together to prevent and mitigate fraud

What is the FraudClassifier Model?

- Enables faster reporting/tracking of fraud trends
  - Less time needed to consolidate/standardize classifications because common taxonomy/glossary is used
  - Faster time to market for industry fraud trend studies/publications

- Use of the model is *voluntary* and can be downloaded and used at no cost

Fed FraudClassifier Model



FRAUD CLASSIFIER

Better Fraud Data. Better Defense.

WHO INITIATED THE PAYMENT?

AUTHORIZED PARTY

How was the fraud executed?

- AUTHORIZED PARTY *WAS MANIPULATED*
  - How was the Authorized Party manipulated?
    - Products & Services Fraud
    - Relationship & Trust Fraud
- AUTHORIZED PARTY *ACTED FRAUDULENTLY*
  - How did the Authorized Party act fraudulently?
    - Embezzlement
    - False Claim
    - Synthetic ID
- UNAUTHORIZED PARTY *MODIFIED PAYMENT INFORMATION*
  - How did the Unauthorized Party modify the payment information?
    - Compromised Credentials
    - Impersonated Authorized Party
    - Physical Alteration

UNAUTHORIZED PARTY

How was the fraud executed?

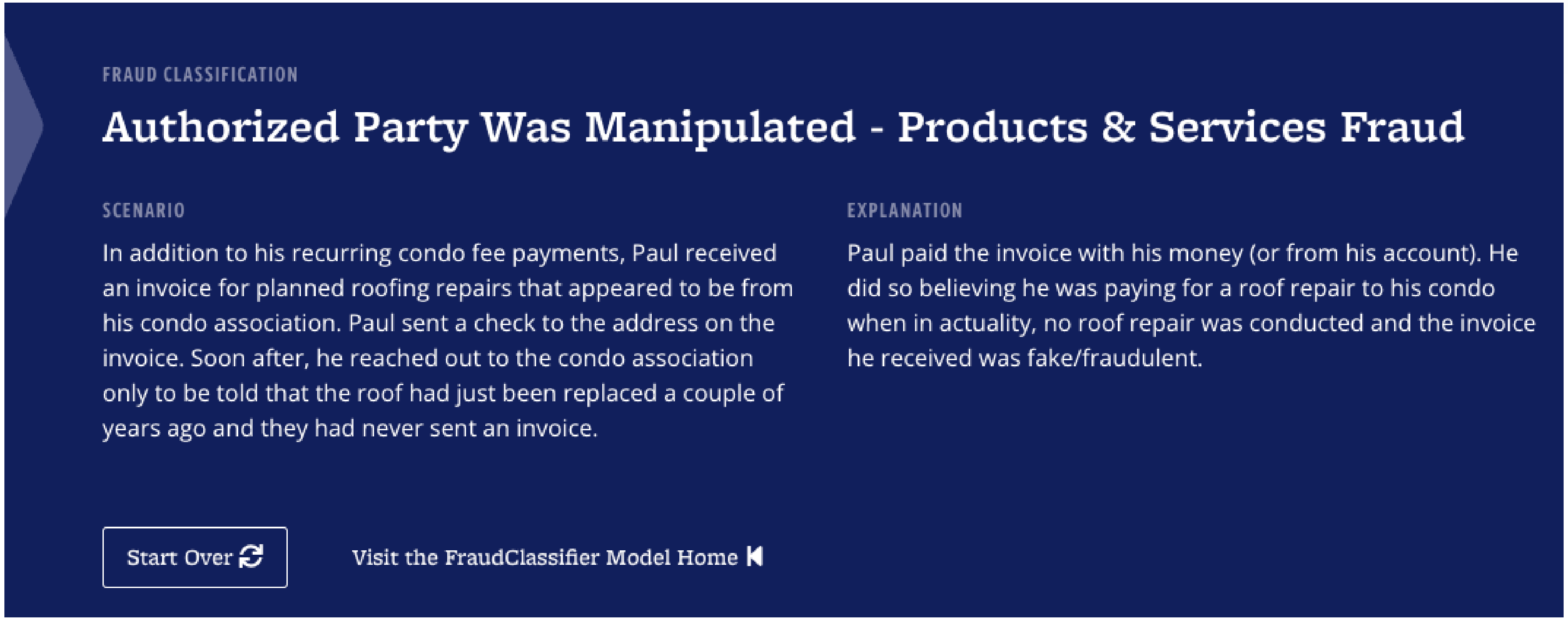
- UNAUTHORIZED PARTY *TOOK OVER ACCOUNT*
  - How did the Unauthorized Party take over the account?
    - Compromised Credentials
    - Impersonated Authorized Party
- UNAUTHORIZED PARTY *MISUSED ACCOUNT INFORMATION/PAYMENT INSTRUMENT*
  - How was the account information/payment instrument misused?
    - Digital Payment
    - Physical Forgery/ Counterfeit

1

2

3

Fed FraudClassifier Model



FRAUD CLASSIFICATION

Authorized Party Was Manipulated - Products & Services Fraud

SCENARIO

In addition to his recurring condo fee payments, Paul received an invoice for planned roofing repairs that appeared to be from his condo association. Paul sent a check to the address on the invoice. Soon after, he reached out to the condo association only to be told that the roof had just been replaced a couple of years ago and they had never sent an invoice.

EXPLANATION

Paul paid the invoice with his money (or from his account). He did so believing he was paying for a roof repair to his condo when in actuality, no roof repair was conducted and the invoice he received was fake/fraudulent.

FraudClassifier Model Fraud Types

1. Products & Services Fraud
2. Relationship & Trust Fraud
3. Embezzlement
4. False Claim
5. Synthetic ID
6. Compromised Credentials (Authorized Party)
7. Impersonated Authorized Party
8. Physical Alterations
9. Compromised Credentials (Unauthorized Party)
10. Impersonated Authorized Party
11. Digital Payment
12. Physical Forgery/Counterfeit

How to Use FraudClassifier Model

- Can be used to work ”forward” (i.e., left to right) to determine the type of fraud committed for a given scenario
- Can be used to work “backwards” (i.e., right to left) to understand how known fraud type occurred and where controls failed
- Still valuable even if all three questions are not able to be answered – even partial classifications can help promote consistency in reporting, communicating, education about fraud

Benefits of Adopting FraudClassifier Model

1. Standardized fraud vocabulary – facilitates communication and comprehension between organizations to identify and mitigate fraud

2. Consistent internal fraud information and tracking – ensures organization using the same definitions

Benefits of Adopting FraudClassifier Model

3. Improved fraud response strategies - allows organizations to apply controls across similar pain points/handoffs across payment types and methods

4. Customer education – helps educate customers on current fraud trends and methods and how to protect themselves

What to do with the data?

- It’s up to your organization how you want to use the model
    - Use of the model is NOT required nor are results required to be shared
    - Shorthand way to communicate fraud scenarios internally and externally
    - A simple spreadsheet can be a very effective tool in tracking the types of fraud experienced by your customers to highlight fraudster trends and/or potential control weak points

www.FedPaymentsImprovement.org

Thank You!

Questions?

Chris Selmi, *AAP, APRP*
President
Wespay Advisors
cselmi@wespay.org
(415) 373-1193