NACM'S 130TH CREDIT CONGRESS & EXPO JUNE 7–10 2026 St. Louis, MO

Date: June 10, 2026

Session: #38064

FRAUD UNMASKED:

Detecting the Signs, Preventing the Crime

Presented by: Wanda Borges and Matt Fluegge

1

Today's Presenters

WANDA BORGES
Borges & Associates, LLC
Co-Presenter
Phone: 516-677-8200 x 225
wborges@borgeslawllc.com

MATT FLUEGGE
United TranzActions
Co-Presenter
Phone: 608-213-8493
mfluegge@unitedtranzactions.com

2

Fraud Statistics

- **2025 Revenue Losses:** Business worldwide lost an average of 7.7% of annual revenue to fraud, totaling an estimated $534 billion revenue loss
- **Business Impact:** Nearly 60% of U.S. businesses reported higher fraud losses in 2025, driven by sophisticated attacks and legacy security gaps.
- **Prevalence of Fraud Experiences:** 65% of credit or debit card holders have encountered fraud, equating to an estimated 150 million U.S. adults
- **2024 Total Losses:** $12.5 billion
- **2024 Survey:** 17% of U.S. adults reported experiencing credit card fraud with the last year

3

Fraud Statistics

- **Global Losses:** Expected to exceed $41 billion in 2025, with projections reaching $43 billion in 2026.
- **U.S. Losses:** Estimated at $12.5 billion for 2025
- Card-Not-Present (CNP) Fraud losses predicted to surpass $200 million in 2025.
- **Identity Theft Reports:** Over 450,000 cases tied to credit cards expected in 2025.
- **Fraud Attempts:** rising 46% year-over-year, with e-commerce credit card fraud up 140% in the U.S. over the past three years.
- **Victim Impact:** About 151 billion Americans will be victims of credit card fraud this year

4

Fraud Statistics

- **Email Becomes the Most Common Contact Method for Scams:** Email surpassed text messages and phone calls as the most commonly reported method, including Business Email compromise
- The average loss per individual credit card fraud incident is about $400

5

Five Basic Elements Of Fraud

- Misrepresentation of a Material Fact
- Knowledge on the part of the Deceiver that the statement is untrue
- Intent on the part of the Deceiver to deceive the alleged victim
- Justifiable reliance by the victim on the statement, and
- Injury to the victim as a result.

6

FRAUD SCHEMES TARGETING TRADE CREDITORS

7

7

Shell Companies Buying Large Quantities of Goods and Disappearing

Fraudsters create a seemingly legitimate enterprise use polished websites, stolen EINs or fake references, OR

Have stolen a purchase order from an existing customer:

- Request goods
  - Order may be for a larger quantity than usual
  - Order may be for a product previously purchased from a competitor
- Delivery location is "new"
- Disappear before the first invoice is due

8

8

Corporate Identity Theft

- Uses spoofed emails (e.g. Agamemnon.co instead of Agamemnon.com)
- Forges Insertion Orders or Letters of Authorization
- Submits believable Purchase Orders
  - Real company refuses to pay the debt because they never authorized the buy in the first place

9

9

Bust-Out Fraud

- Behaves like a good customer for 60-90 days
  - Opens an Account
  - Pays initial invoices
  - Gradually increases spend
  - Makes One Large Buy
- Then vanishes

10

10

Fraudulent Credit References

- Fictitious Supplier Contacts or Landlord
- "Trade references" that are actually friends
- Banks that confirm information but only with trivial facts
- Trade Creditors relying on informal references may unwittingly approve high-risk accounts

11

11

Short-Term Fraud

- Chaotic Periods where credit verification is rushed
  - Holiday season approaching so claim is that goods are needed immediately to "get into the stores" timely
  - "Season" is beginning
  - Common in certain industries such as construction after a long cold winter
  - Fraudster claims new operating being opened and goods are needed for that event

12

12

Fraudulent Disputes or Refusal to Pay

- Claiming goods never ordered
- Claiming goods never received
- Claiming goods delivered late
  - Deliberate intention to not pay
- Refusals to Pay legitimate invoices
- Disappearing Act: Businesses closing or changing names to avoid payment

13

13

Prevention Strategies

14

14

Strengthened Identity Verification

- Verify beneficial ownership, not just operating name
- Match legal names against SOS filings and tax records
- Confirm physical location using video calls or Google Earth
- Validate domain age (fraudsters often use domain names created within 60 days)
  - Website created within last 3 – 6 months is a Red Flag

15

Test the Waters of a New Account

For new accounts, until creditworthiness has been established

- Allow limited purchases only
- Require partial prepayment
- Release additional inventory only after payment clears

16

Corporate Impersonation Defenses

When a brand is well known:

- Compare email domains to corporate registry
- Check for misspellings or alternate domain endings
- Confirm contacts through known corporate switchboards

ALSO

- Confirm billing addresses match corporate headquarters or known offices

17

PAYMENT FRAUD

18

Fraudulent Wire Transfers

- Fraudulent wire transfers – often the result of social engineering
  - Social Engineering - is the tactic of manipulating, influencing, or deceiving a victim in order to gain control over a computer system, or to steal personal and financial information. It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information
- Check twice before shipping your goods or providing your services
  - Large quantities of goods may be ordered by a purportedly known customer to be paid by wire transfer
  - A wire transfer is supposedly sent to you. A copy of a bank confirmation of transmission is provided but the money is never received – Goods have been already delivered

19

19

Tips For Preventing Fraudulent Wire Transfers

Verify with phone calls, no matter how well you know the sender.

Strong Passwords and MFA

Practice good email hygiene

Forward suspicious emails, even from within your organization

Have a special procedure for wires over a certain amount.

20

20

FRAUD CAN BE COSTLY

THE COST TO BOTH BUSINESSES AND CONSUMERS FROM CREDIT CARD FRAUD ARE BILLIONS OF DOLLARS EVERY YEAR.

Fraudsters are continually finding new ways to commit their illegal activities, so it is essential to develop fraud prevention and detection techniques to counter the threat of fraud and identity theft to keep losses to a minimum.

21

21

Types of Credit Card Fraud

- Card-Not-Present (CNP) Fraud
- Account Takeover
- Interception Fraud
- Chargeback Fraud

22

Card-Not-Present Fraud

- Fraudsters use stolen credit card information to make unauthorized purchases or payments
  - ✓Data breaches may expose cardholder details
  - ✓Card numbers may be bought on the dark web
- The trade credit grantor may be liable for the fraud, leading to chargebacks, revenue loss, and penalties from card processors.

23

Account Takeover Fraud

- Fraudsters gain access to a legitimate customer's business credit card account and make unauthorized changes or purchases.
- Typically achieved through phishing attacks, social engineering, or weak passwords.
- Credential stuffing, where fraudsters use stolen login information from one platform to access another.
- Email compromises where hackers hijack communication between businesses.

24

Interception Fraud

- Fraudsters place an order using the name of a legitimate customer
- Changes the delivery address
- Intercepts the delivery and reroutes goods to themselves
- Exploit gaps in order tracking or delivery systems

25

Chargeback Fraud

- A legitimate cardholder disputes a transaction that they actually authorized, claiming it was unauthorized.
- Fraudsters exploit this by intentionally making purchases and then disputing them.
- Filing false chargebacks.
- Exploiting weaknesses in the dispute process to get refunds for valid purchases.

26

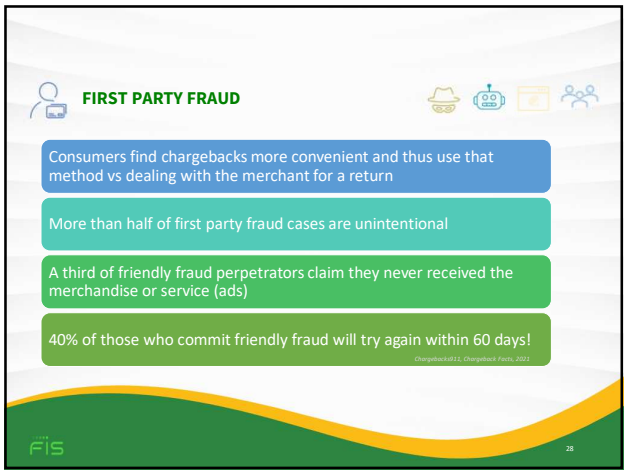
FIRST PARTY FRAUD

WHAT IT IS:

Also known as "Friendly Fraud" is when a cardholder files a chargeback against a transaction made on their account, sometimes with the explicit knowledge that they received the product or service

While it can happen following a genuine mistake, friendly fraud covers both accidental fraud and malicious fraud

27


FIRST PARTY FRAUD
Consumers find chargebacks more convenient and thus use that method vs dealing with the merchant for a return
More than half of first party fraud cases are unintentional
A third of friendly fraud perpetrators claim they never received the merchandise or service (ads)
40% of those who commit friendly fraud will try again within 60 days!
Chargebacks911, Chargeback Facts, 2021
FIS
28

28


12 Potential Signs of CNP Fraud (First 6)
1. First-time shopper: Criminals are always looking for new victims.
2. Larger-than-normal orders: Because stolen cards or account numbers have a limited life span, crooks need to maximize the size of their purchase.
3. Orders that include several of the same item: Having multiples of the same item increases a criminal's profits.
4. Orders made up of "big-ticket" items: These items have maximum resale value and therefore maximum profit potential.
5. "Rush" or "overnight" shipping: Crooks want these fraudulently obtained items as soon as possible for the quickest possible resale, and aren't concerned about extra delivery charges.
6. Shipping to an international address: A significant number of fraudulent transactions are shipped to fraudulent cardholders outside of the U.S. Visa AVS can't validate non-U.S., except in Canada and the United Kingdom.
29

29


12 Potential Signs of CNP Fraud (Next 6)
1. Transactions with similar account numbers: Particularly useful if the account numbers used have been generated using software available on the Internet.
2. Shipping to a single address, but transactions placed on multiple cards: Could involve an account number generated using special software, or even a batch of stolen cards.
3. Multiple transactions on one card over a very short period of time: Could be an attempt to "run a card" until the account is closed.
4. Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses: Could represent organized activity, rather than one individual at work.
5. For online transactions, multiple cards used from a single IP (Internet Protocol) address: More than one or two cards could definitely indicate a fraud scheme.
6. Orders from Internet addresses that make use of free e-mail services: These e-mail services involve no billing relationships, and often neither an audit trail nor verification that a legitimate cardholder has opened the account.
30

30

There Are Several Ways To Reduce Your Exposure To Payment Fraud

1. Procedural Measures
2. Technological Solutions
3. Best Practices

31

Procedural Measures

1. Employee Training
2. Clear Dispute Policies
3. Monitor Transactions

32

Technological Solutions

1. Use EMV Chip Technology
2. Implement Strong Authentication
3. Regular Security Audits
4. Secure Online Transactions
5. Tokenization

33

Technological Solutions

5. Point-to-Point Encryption
6. AVS and CVV Verification
7. Advanced Fraud Detection Tools:
   FraudSight & Guaranteed Payments
8. Alternative Payments:
   Electronic Check with Guarantee

34

AVS: How You Can Use It To Help Minimize Fraud.

AVS stands for Address Verification Service. Merchants use it on Mail/Telephone and Internet transactions to help verify that the cardholder is the person placing the order.

Here are the codes and what they mean:

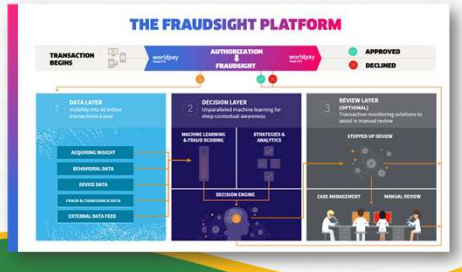
X - Exact match of both street address and 9-digit ZIP code (Street address means house number (i.e. 4215), not the name of the street (i.e. Broad Street).
Y - Exact match of both street address and five digit zip code.
A - Street address matches, but the ZIP code does not.
Z - The ZIP code matches, but the street address does not.
N - Neither the street address or ZIP code match.
U - Address information is unavailable from the issuer.
R - Address information is temporarily unavailable from the issuer please try again.
G - International card. AVS not available.
S - Usually indicates a foreign card.

Hot Spots for Fraud
Indonesia, Nigeria, Ghana, Singapore and Malaysia are the hot spots for fraud. Merchants should exercise **EXTREME** caution in placing ads for customers from these areas of the world.

35

Fraudsight

FraudSight is a leading merchant fraud detection and prevention solution provided by Worldpay. FraudSight will protect merchants from fraudulent transactions thus reducing their losses and fraudulent chargebacks. FraudSight uses machine learning and customized business strategies to stop bad transactions while letting the good transactions through.



36

Guaranteed Payments

Worldpay's Guaranteed Payments solution with Signifyd evaluates orders at checkout and delivers instant decisions backed by a financial guarantee against fraud on all approved orders. This effectively shifts the liability for fraud away from your business, allowing you to trust customers and grow fearlessly while reducing risk.

1 A shopper places an order on the merchant's site & clicks "Purchase."

2 Upon hitting "Purchase", the order is sent via Guaranteed Payments for evaluation & decisioning.

3 For Guaranteed Payments approved orders, Worldpay attempts authorization. For declined orders, the transaction is blocked.

4 If authorization is successful, the order is promptly approved; failed authorization orders are declined.

37

ELECTRONIC CHECK / ACH PROCESSING WITH A GUARANTEED SETTLEMENT

★ Exclusive UTA offering

- Immediate approval or decline
- Next Day Funding
- No Bounced Payments due to NSF, Fraud, or other reasons
- No chargebacks as there can be with Credit Card payments
- Processing fees are typically 70% to 85% lower than credit cards
- Instead of entering the customer's credit card number and expiration date, simply enter the customer's bank routing # and account # to obtain the approval

38

CREDIT CARD COSTS vs. GUARANTEED ACH

CREDIT CARD PAYMENT

$5,000 Transaction
Rate = 3.00%
Cost = $150.00

ACH PAYMENT
Guaranteed

$5,000 Transaction
Rate = 0.79%
Cost = $39.50

SAVINGS
$110.50 ⇄ 74%

39

How Prevalent Are Check Payments Today?

Year	# of Checks (millions)	Dollar Amount (billions)
2024	2.978	$8.173
2023	3.146	$8.449
2022	3.374	$8.948
2021	3.657	$8.758
2020	3.767	$7.875

Federalreserve.gov and federalreserve; fraser.stlouisfed.org; stlouisfed; scribd; gov.info

40

40

Businesses and consumers still rely on checks for several reasons

1. Established Infrastructure
2. Nearly Universal Acceptance
3. Cost Effective / Low Fees
4. Reluctance to Change

41

41

The Prevalence of Check Fraud

- Check fraud more than doubled from 2020 to 2022 according to the Financial Crimes Enforcement Network (FinCEN).
- FinCEN reported there were over 680,000 cases reported in 2022, up from 350,000 from 2021.
- 2023 = slight decrease to 665,505
- 2024 = still over 500,000 check fraud cases
- Fraud checks continue to be extremely prevalent, even as consumers move on to other electronic payment methods.

Thomasreuters.com; orbograph.com; Federalreserve.gov

42

42

Why Is Check Fraud Prevalent?

1. Technological Advancements
2. Ease of Access to Information
3. Economic Pressures
4. Insufficient Security Measures

43

11 Tips To Prevent Fraudulent Checks

44

1. Physical Features

- Holographic elements & embedded watermarks are hard to replicate
- Important to put those security features to the test
  - Fraud checks may say they have security features but usually fail authentication
- Authentic checks are printed on high quality paper stock
  - Fraud checks feel lighter with a slippery texture

45

2. Magnetic Ink Character Recognition (Micr)

- Unique texture
- Counterfeit checks may feature shiny MICR numbers.
- Feel and visually inspect the MICR line to distinguish the authenticity of the check

46

3. Font And Alignment

- Look for inconsistencies
  - Variations in font size
  - Misalignments

47

4. Edges

- At least one perforated edge
  - Indicative of professional printing
  - Legitimate checks are typically torn-off a checkbook
- Be cautious if all edges appear uniformly smooth
  - Indicative of personal computer printer

48

5. Misspellings And Mistakes

- Be wary of discrepancies
  - Spelling errors
  - Grammatical Mistakes
- Amateur fraudsters
  - Tend to rush through production
  - Lack attention to detail
  - Inexperienced

49

6. Visual Confirmation Of Identity

- Visually compare the person presenting the check with a valid identification
- Pre-written ID numbers should be verified
- Fraudsters tend to pre-write false ID numbers to bypass being identified
- False ID numbers allow fraudsters to circumvent negative databases

50

7. Validate Signatures

- Verify the consistency of the signature on the check against the presented identification
- Discrepancies may be indicative of a stolen identification
- Cross reference any other known signature sample for extra validity
  - Invoice
  - Paperwork

51

8. Non-regional Shopping Pattern

- Counterfeit check writers often shop outside of their local area
  - Less likely to be recognized
  - Usually travels within a 3 to 4 hour distance
- Be wary of large orders by phone or email
- Always be cautious when transactions are inconsistent with the customer's physical

52

9. In-store Pickup Preference

- Fraudsters often opt for in-store pickup rather than delivery
  - Allows them to quickly obtain the goods
  - Reduces the chances of detection during the delivery process
- Visible security cameras
  - Provides a deterrence
  - Helps collect crucial evidence

53

10. Unusual Behavior

- Pay attention to suspicious behavioral cues such as:
  - Signs of nervousness
  - Urgency and pressure
  - Readily available back up checks

54

11. Utilize UTA's Guarantee Services

- Technology plays a pivotal role… consider utilizing paper check and electronic check guarantee services offered by United TranzActions
- UTA's services can quickly authenticate a payment's legitimacy by cross-referencing the provided information with databases of known fraudulent activity

55

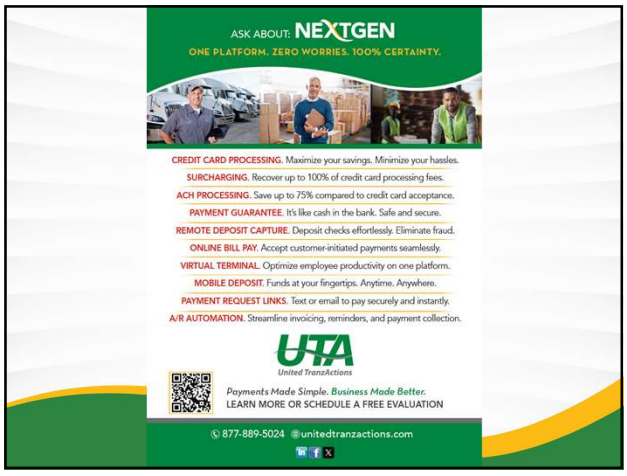
Secure Payment Processing Services

Efficiently accept payments while minimizing Fraud and Processing Fees

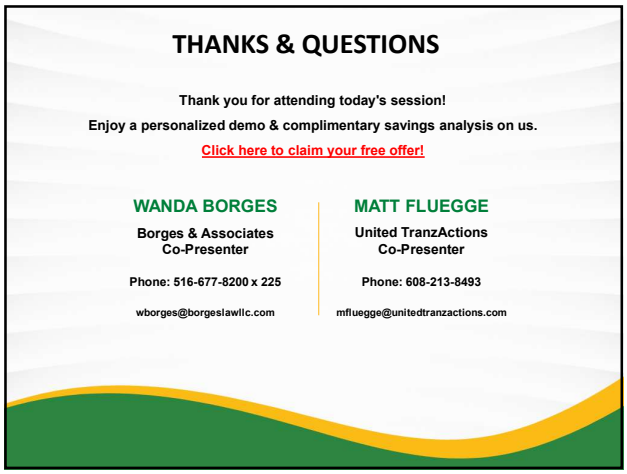
UTA Benefits Include:

- Robust fraud prevention tools
- PCI Validated - Point-to-Point Encryption Solution
- Tokenization Services
- Level 3 Processing For Reduced Fees
- Guaranteed Electronic Check Payments
- Free consultative analysis to save money and increase revenue

56



57


THANKS & QUESTIONS
Thank you for attending today's session!
Enjoy a personalized demo & complimentary savings analysis on us.
Click here to claim your free offer!
WANDA BORGES
Borges & Associates
Co-Presenter
Phone: 516-677-8200 x 225
wborges@borgeslawllc.com
MATT FLUEGGE
United TranzActions
Co-Presenter
Phone: 608-213-8493
mfluegge@unitedtranzactions.com

58