ICBA Payments

Payment Fraud Trends

Rebecca Kruse

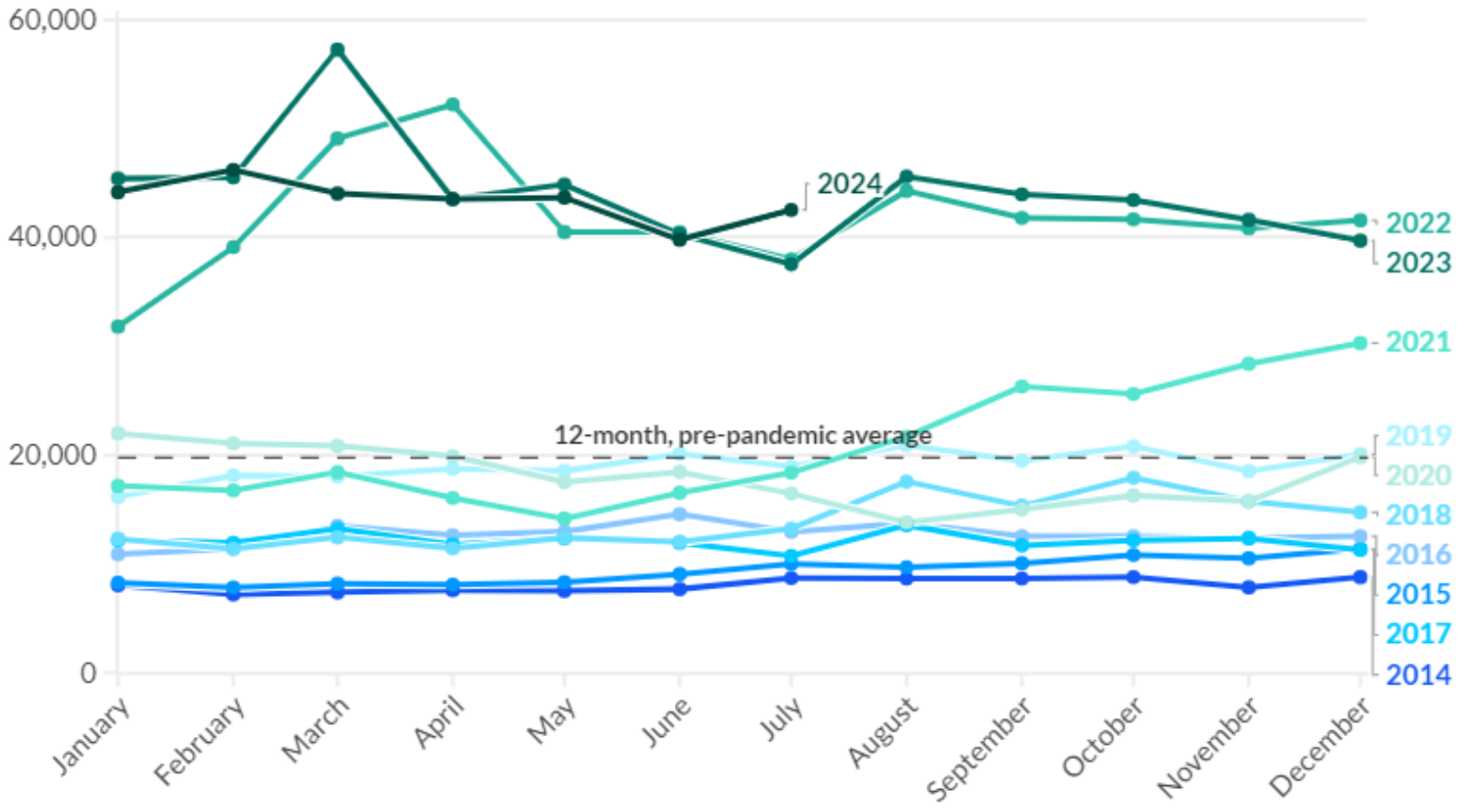
EVP, COO ICBA Payments

Types of payments fraud discussed

- Check Fraud
- Credit washing
- Friendly fraud & Visa changes
- Credit and debit card BIN attacks
- Instant payments – Authorized push payments (APP)
  - Faster, instant, real-time…not same day ACH
  - Networks:
    - The Clearing House's RTP
    - FedNow
  - Important: Credit push model only
- Zelle litigation and rule changes

Check Fraud

Check Fraud



Source: Fincen • Includes all SARs in the check fraud category reported by depository institutions. The 12-month, pre-pandemic period starts March 2019 and ends February 2020.

AMERICAN BANKER

- Number of fraud reports declining
- Value of fraud increasing
- Slowing compared to 2024, but much hire than pre-pandemic numbers

Credit and Debit Card Fraud

Synthetic ID Fraud

- A synthetic identity is a fake identity that combines real personal information, like a Social Security number, with fraudulent or fabricated information.
- If SSN used 5x in last 3 months, network alerts

Protect with

- Electronic Consent-Based Social Security Number Verification (eCBSV)
- Visa Issuer's Clearinghouse Service (ICS)

Credit washing

- FOX 25 Consumer Watch: Why you might be accidentally involved in a scam
by Mireya Garcia

- https://okcfox.com/news/consumer-watch/fox-25-consumer-watch-why-you-might-be-accidentally-involved-in-a-scam

- WSJ Podcast: 'Credit Washing': How Some Credit-Repair Firms Inflate Credit Scores

- https://www.wsj.com/podcasts/your-money-matters/credit-washing-how-some-credit-repair-firms-inflate-credit-scores/90eb2b8d-31f7-46c4-af45-dac14fc2dbb2

Credit washing

- Different from identity theft or synthetic identity
- Gaining popularity
- Actual person (not bad actor) washes credit to artificially inflate credit score to qualify for credit card
  - Individual disputes negative information on credit report and asserts identity theft
  - FCRA requires disputed information to be temporarily blocked from report, which can temporarily inflate credit score
  - Individual applies for credit card and is approved
  - Credit card limit is maxed out and customer defaults
- Protect with
- Participating with fraud consortium and information sharing

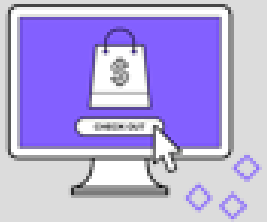
Fair Credit Reporting Act
§ 605B.Block of information resulting from identity theft [15 U.S.C. § 1681c-2]

- Block. Except as otherwise provided in this section, a consumer reporting agency shall block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft, not later than 4 business days after the date of receipt by such agency of
  - appropriate proof of the identity of the consumer;
  - a copy of an identity theft report;
  - the identification of such information by the consumer; and
  - a statement by the consumer that the information is not information relating to any transaction by the consumer.

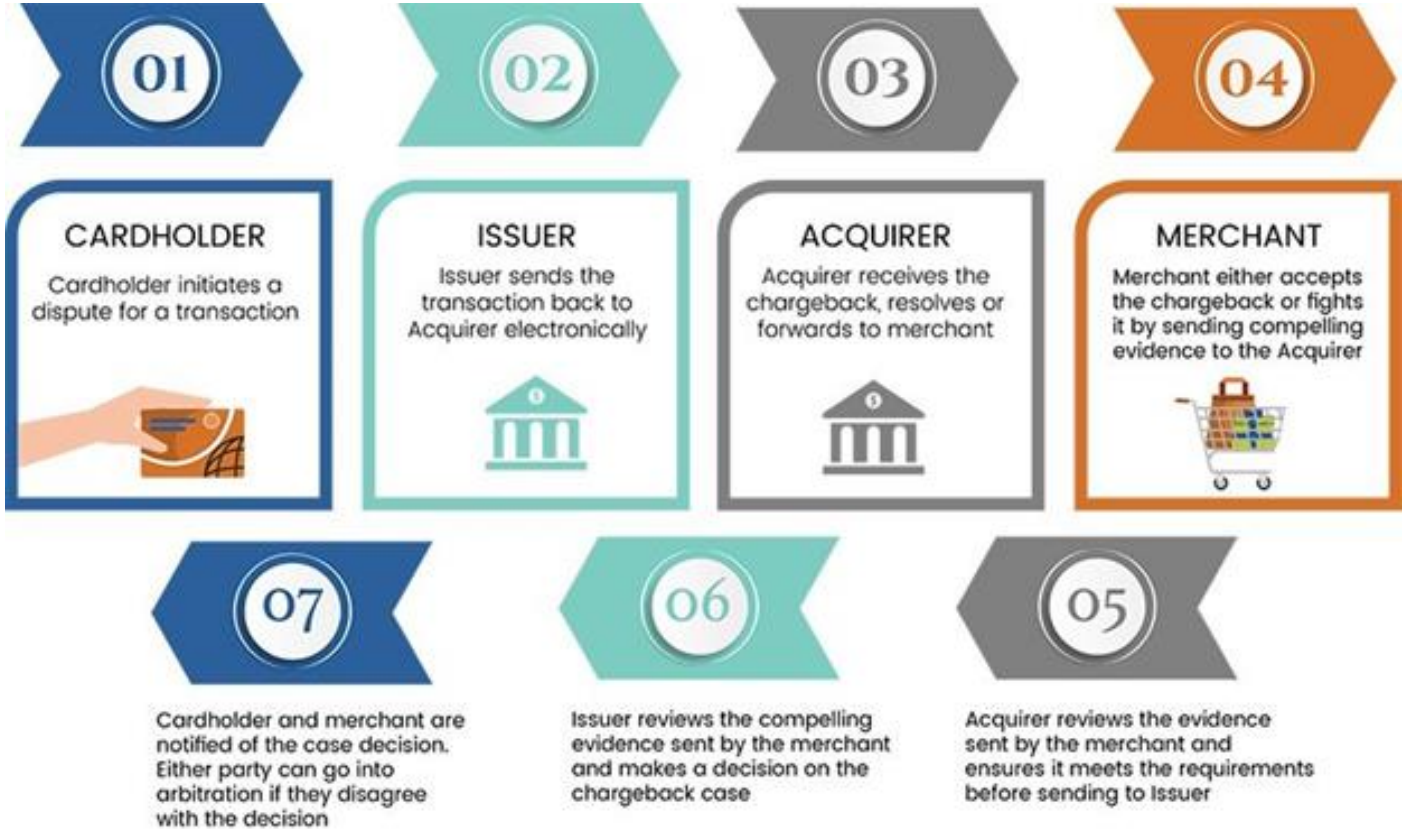
Repeat disputes from same consumer
CFPB § 1022.43 Direct disputes.

- **(f) Frivolous or irrelevant disputes.**
  - (1) A furnisher is not required to investigate a direct dispute if the furnisher has reasonably determined that the dispute is frivolous or irrelevant. A dispute qualifies as frivolous or irrelevant if:
  - (i) The consumer did not provide sufficient information to investigate the disputed information as required by paragraph (d) of this section;
  - (ii) The direct dispute is substantially the same as a dispute previously submitted by or on behalf of the consumer, either directly to the furnisher or through a consumer reporting agency, with respect to which the furnisher has already satisfied the applicable requirements of the Act or this section; provided, however, that a direct dispute is not substantially the same as a dispute previously submitted if the dispute includes information listed in paragraph (d) of this section that had not previously been provided to the furnisher; or
  - (iii) The furnisher is not required to investigate the direct dispute because one or more of the exceptions listed in paragraph (b) of this section applies.

Card Chargeback Process



https://www.chargebackgurus.com/blog/merchant-chargebacks-101-what-they-are-why-they-matter



Dispute vs Fraud Claim

Dispute

- Concern with quality of goods or services
- Timeline of up to 120 days to file
- Merchant liability (typically)

Fraud

- Cardholder is unaware of activity
- Timeline of 60 days to file
- Issuer liability

Friendly Fraud

Friendly fraud [aka First Party Misuse) occurs when a customer submits a fraud claim despite having received the goods or services they knowingly ordered.

Currently reported as the #1 fraud attack from both small and large merchants

Thoughts and triggers behind Friendly Fraud:

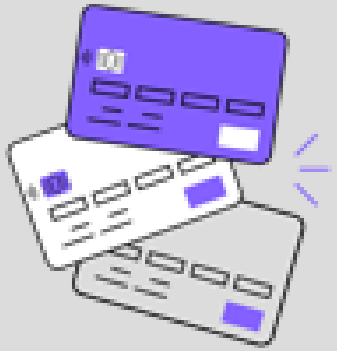
- Buyers Remorse
- Unclear merchant information on billing statement
- Better understanding of consumer liability rules
- Sharing of personal information amongst family members

Protections:

- Robust verification measures or tools that enables purchase behavior to be analyzed
- Proper and distinctive merchant identifiers on billing statements

- Visa Rules Change updated 4/15/23: Allows merchants to present additional data or evidence indicating the disputed charge is valid

BIN attacks / Account testing



BIN attacks and card testing fraud are two separate activities, but are often used together

- The primary purpose of a BIN attack is to “crack” credit card algorithms using software
- Account testing is verifying whether a card is active and has protection against fraud

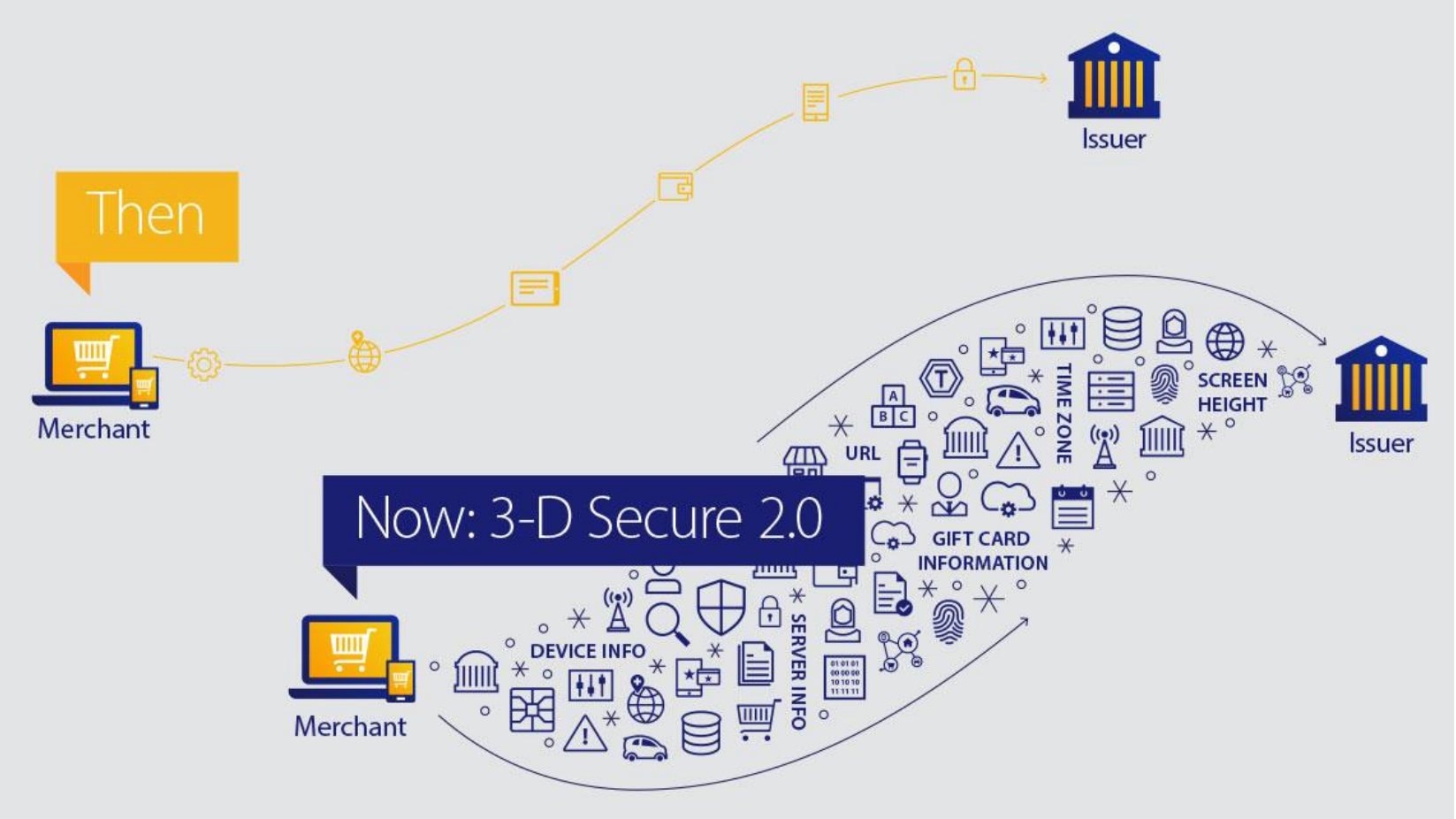
Banks are experiencing varied test authorization amounts occurring in short time blocks

Seeing increase against smaller FIs due to perceived deficiency in staff resources and sophisticated technology and program oversight

BIN attack fraud protection

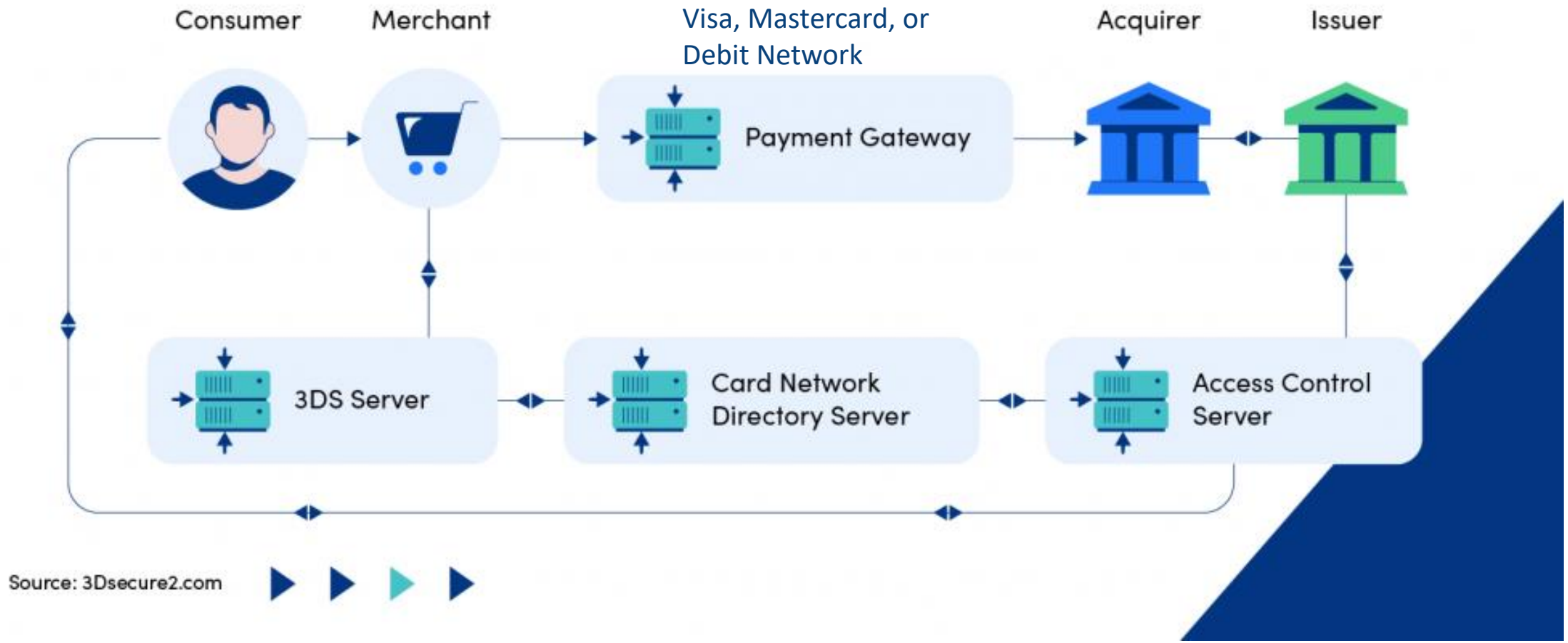
- Non-sequential card issuance – card number randomization
- Implementing expiration date matching on every transaction
- Blocked access after a set number of declined transactions (Velocity controls)
- Network/Processor reporting – e.g. Mastercard Safety Net
- Quick reporting to processors for research and action(s)

Evolution of 3-D Secure



https://usa.visa.com/visa-everywhere/security/future-of-digital-payment-security.html

Card transaction flow – 3D Secure

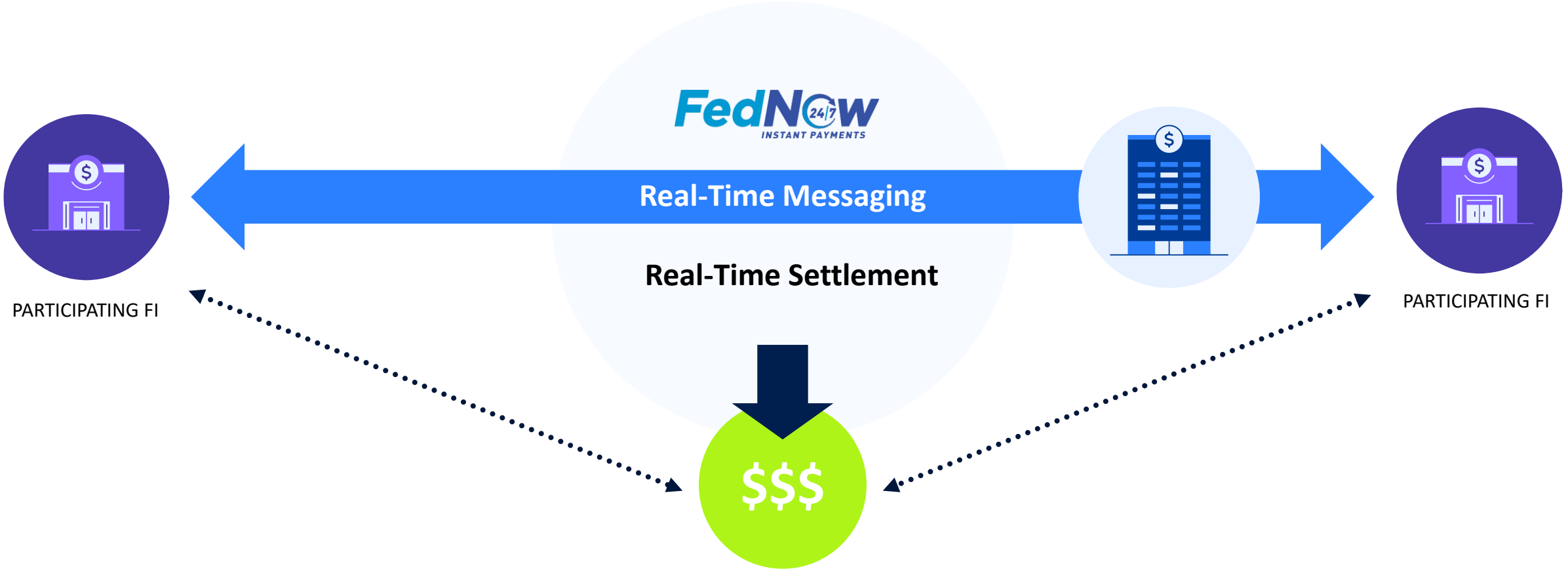


Card fraud general protection

- Neural network – evaluate transactions in real time
- Custom rules
- User defined card controls
- Participate in 3D Secure
- Card network proactive notifications/ranking
- Include in incident response plan
- Quickly identify common points of compromise

Instant Payments

Enabling 24/7 Two-Way Messaging with Real-Time Settlement

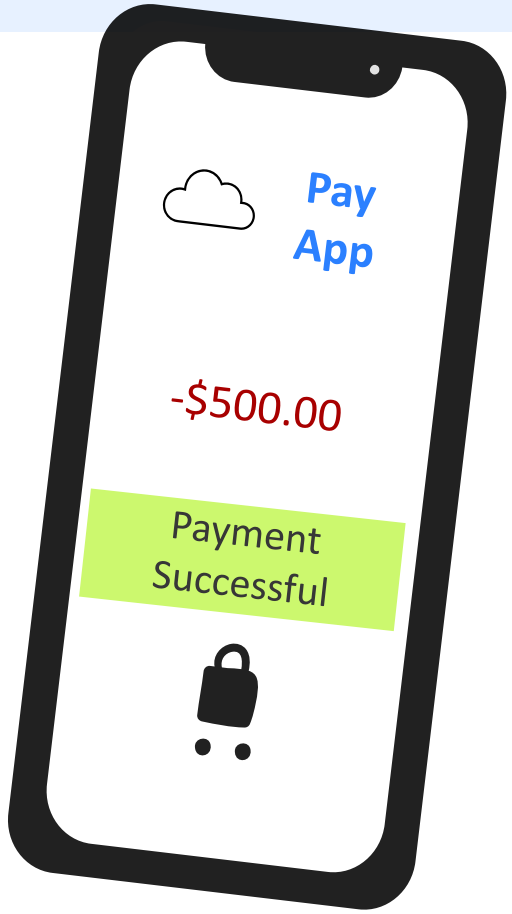


Fraud Lessons from 10+ Years of Faster Payments Internationally

Two main types of fraud have been identified: authorized (e.g. scams) & non-authorized

- Non-authorized fraud:
  - Identity theft
  - Friendly fraud
  - Cybercrime/ data breaches
  - SIM swap

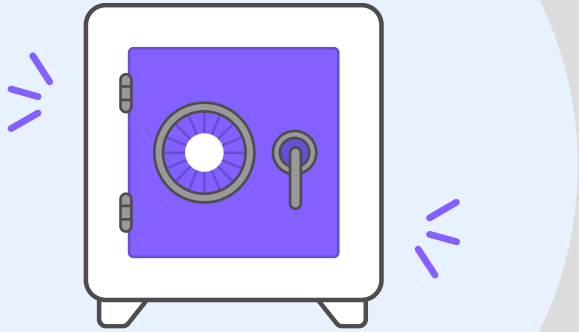
- Authorized Push Payment fraud (APP Fraud):
  - Only the UK and Japan have regulations in place to protect victims from APP fraud.
  - The most common type of APP fraud includes impersonation scams, advanced fee scams, and malicious redirection of payments.



Zelle Challenges

- Zelle is a payment app owned by the nation's largest banks
  - Closed loop instant payments
  - Card based non-bank participants
- Reg E covers unauthorized fraud
- APP is not unauthorized fraud because accountholder is initiating payment – Scam
- 38% consumer reimbursed in 2023 compared to 62% in 2019 (JMPC, BoA, Wells)
- Class-action lawsuit against JPMorgan Chase and Zelle for covering scammed customers lost
- JPMorgan Chase considering suing CFPB
- https://www.reuters.com/legal/jpmorgan-considers-suing-consumer-watchdog-over-zelle-2024-08-02/

Cross-channel fraud detection



- Most fraud detection is siloed by payment channel
  - ACH -> ACH
  - Card -> Card
  - Check -> Check

- Customers transact in many different channels
- Evaluate fraud across channels at the customer
- Include non-payment information like failed logins or new payees

Fraud Toolbox

- Crimedex Alerts
  - https://www.crimedex.com/
- FS-ISAC
  - https://fsisac.com
- Verizon Data Breach Investigations Report
  - https://enterprise.verizon.com/resources/reports/dbir/
- International Association of Financial Crimes Investigators – IAFCI
  - https://www.iafci.org/
- Association of Certified Fraud Examiners – ACFE
  - http://www.acfe.com/
- ICBA Community
  - https://community.icba.org/main/groups/72279/lounge
- United States Secret Service eInformation Network
  - https://www1.einformation.usss.gov/eInformation/home.seam
- United States Secret Service Electronics Crimes Task Force – ECTF
  - http://www.secretservice.gov/ectf.shtml
- FICO Card Alert Network Fraud Forum
  - https://community.fico.com/community/fraud-alert-network
- National Cyber Forensics Training & Alliance – NCFTA
  - http://www.ncfta.net/
- Electronic Consent Based SSN Verification (eCBSV)
  - https://www.ssa.gov/dataexchange/eCBSV/

ICBA Payments

Thank you

- Rebecca Kruse
- Rebecca.Kruse@icba.org
- 301.325.4561
- icba.org/payments

Disclaimer

This presentation contains suggestions for protection against payments fraud trends. Before acting on any information, you should consider the appropriateness of it with regard to your particular objectives and seek legal advice.