First Citizens Bank

Fraud Counterattack: How To Protect Your Business From Financial Threats

Featured Speakers

Kristen Saranteas

Treasury Management Services Executive,
First Citizens Bank

Sharon Crabbe

Financial Crimes Senior Manager,
First Citizens Bank

Ishanaa Rambachan

Partner,
McKinsey & Company

First Citizens Bank

Agenda

1. The fraud landscape & today's biggest threats
2. How & where fraud takes place
3. Building your defense
4. The future of fraud: What's next?

Let's Hear From You.

What do you see as your top fraud challenges?

- Rising cost and complexity of fraud response
- Lack of fraud awareness and training
- Adopting fraud prevention technology
- Balancing fraud prevention with user experience
- The fraud "you know" (BEC, checks, etc.)
- The fraud of the future (AI-powered, deepfakes, etc.)

2025: A Challenging Year For Fraud

Payments Fraud Activity on the Rise

80% of organizations were targets of either an actual or attempted payments fraud attack in 2023, up 15% from 2022.

Checks Continue to be Vulnerable to Fraud

Checks continue to be most susceptible to fraud, as reported by 65% of respondents. 70% of organizations have no plans to discontinue their use.

Business Email Compromise (BEC) Controls Have Room for Improvement

Less than 60% of organizations have written procedures required to safeguard against BEC.

Discovering Fraud

30% of respondents report that after a successful fraud attempt, their organizations were unable to recover the funds lost due to fraud.

Email Targets ACH Credits

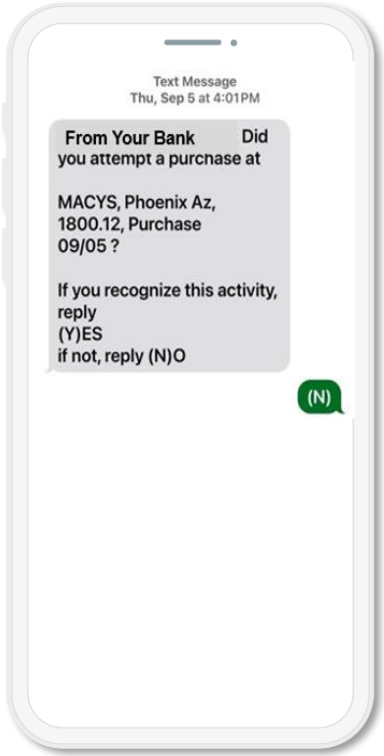
ACH credits have surpassed wires as the most vulnerable payment type for BEC fraud at 47%.

Organizations Overlook the Vulnerability of Payments Sent by USPS

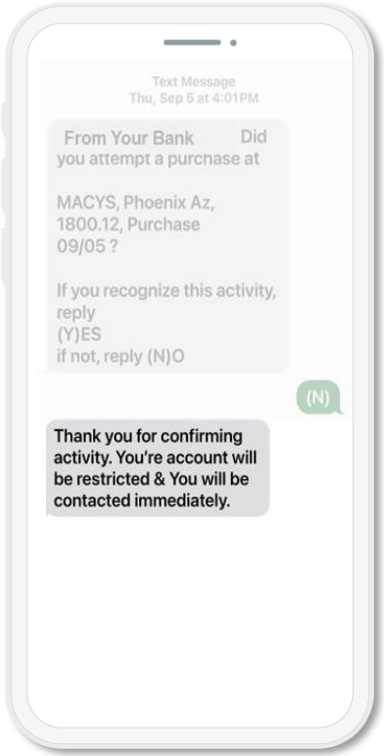
Over 20% of respondents report fraud due to interference with the USPS—10% higher than in 2022. Over 80% of organizations still deliver checks via USPS without tracking.

Source: 2024 AFP® Payments Fraud and Control Survey Report

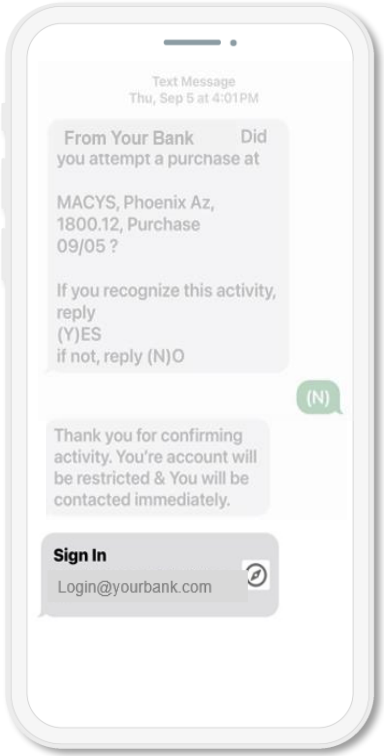
Bank Impersonator Scam Case Study



Business owner, John, receives text from "bank" and responds no.

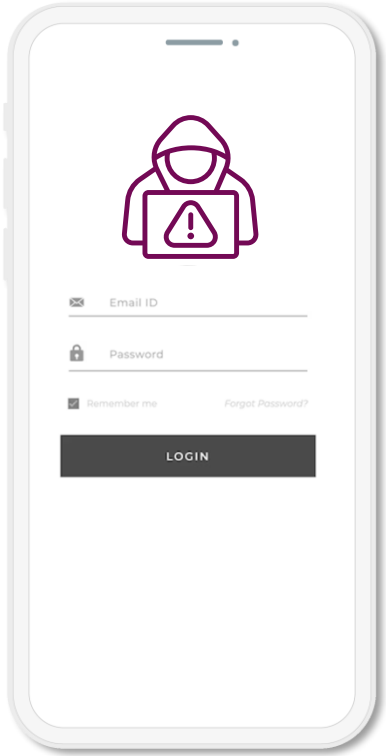


John receives call from the bank's phone number from "the bank's fraud department" offering to dispute charge.



John receives text during the call with a link to his "online banking login page" and enters his credentials.

John shares code he receives by text during call and believes a dispute has been filed for the unauthorized charge.



Fraudster uses John's info to log in to his online banking and initiate wires.

Check Fraud Case Study

Office Manager, Samara, reviews account daily to identify unauthorized activity.

Samara goes on medical leave and account reconciliation is neglected.

Several counterfeit checks pay on the account and go undetected.

When Samara returns, she files a check fraud dispute.

Claim is denied because the counterfeit checks weren't reported 30 days after date of statement showing first unauthorized check.

Types Of Check Fraud

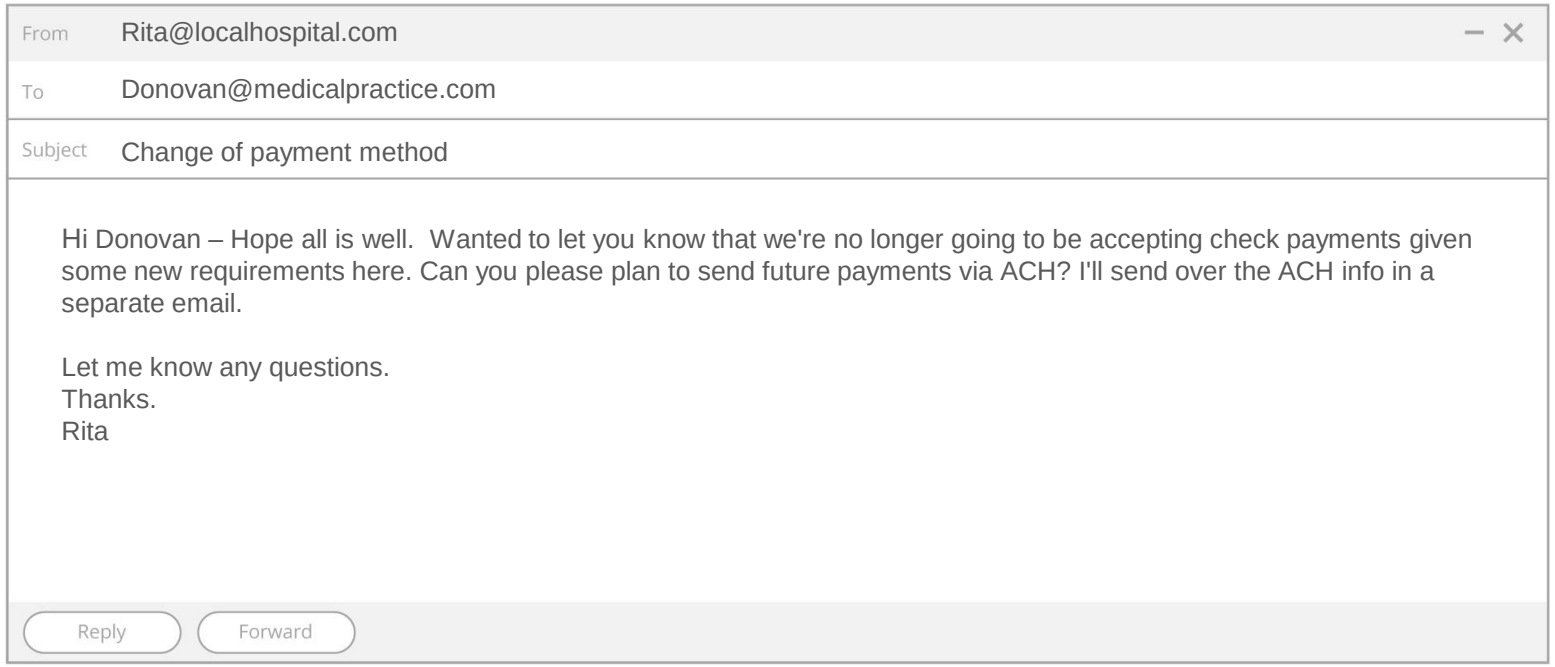
Counterfeit Checks
A check that resembles a legal check but is actually a fraudulent reproduction.

Altered/Washed Checks
A legal check that has been altered or washed, usually from the payee name and/or amount.

Forged Maker Signature
A legal check bearing a forged maker signature (front of check).

Forged Endorsement
A legal check bearing a forged endorsement signature (back of check).

Business Email Compromise Case Study



Donovan receives an email from "Rita" who he regularly corresponds with at a local hospital.

Donovan forwards the email to his accounts payable department and asks that the hospital's payment instructions are updated.

As invoices are received, payments are disbursed via ACH for several months.

The hospital contacts Donovan to report non-payment.

Because months passed before Donovan identified the compromise, no funds were recovered from the fraudster's bank.

Inside The Fraud Management Playbook

Beyond ‘Know Your Customer’: understand account access and transactional patterns to accurately and quickly detect anomalies

- Passive authentication routines (behavioral analytics and biometrics, device/IP server recognition, geo-location)
- Transactional monitoring that identifies out-of-pattern usage at the customer level (use of consortium models, sometimes customized with institutional data, augmented with rules-based detection, fast-cycle analytics).

Customer Journey Risk Tagging:

- As customers onboard, link accounts, make deposits, authenticate themselves and conduct money movement, capture and orchestrate all the risk signals along the journey and utilize a more robust risk assessment before transactional approval.

Support all the above with comprehensive analytics that’s used to identify risk for:

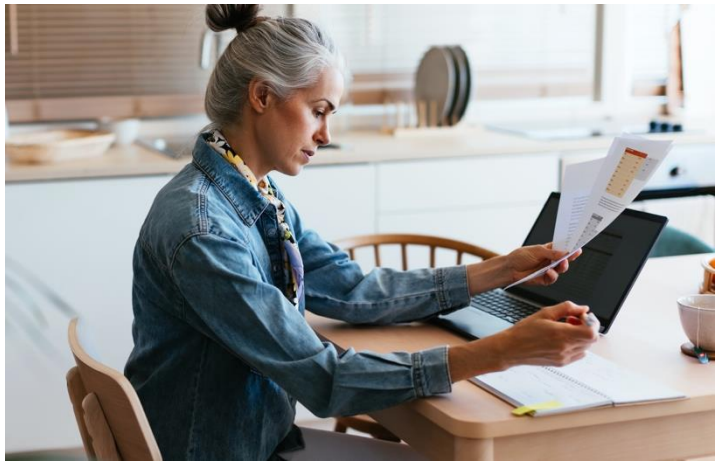
- ID Proofing at onboarding, remote access authentication, deposit activity, transactional activity
- Process breakage exploited by frauds (e.g., BEC, password guessing, check acceptance, etc.)
- Control effectiveness (e.g., recalibration of models/rules, approval/decline & risk appetite thresholds, other controls)

FirstCitizensBank

Why You Need To Protect Yourself

Why You Need To Protect Yourself

- **Consumers have protection under Reg. E but businesses do not**
- **Timeframes are tight on electronic transactions and provide less recourse for businesses**



Fraud Type	Personal Reg E, NACHA, Account contract, UCC	Business NACHA, Account contract & UCC
Checks	30 days after date of statement showing first unauthorized check	30 days after date of statement showing first unauthorized check
Debit Cards	60 days after discovery – bank gives provisional credit	No coverage
ACH Debit (RDFI)	60 days after posting	24 hours after posting
ACH Debit (ODFI)	Covered by Reg E	*No coverage* ACH reversal can be initiated up to 5 days after ACH is processed, no guarantee of funds return
Wires	No coverage	No coverage
Other Digital Banking Transactions (Zelle, Bill Pay)	Covered by Reg E	No coverage

Bank Tools To Protect Your Company

Bank Tools Serve As Insurance Policies

Bank tools & services	Definition	Implemented	'Very effective' or 'effective'
ACH Debit Blocks and Filters	Controls which ACH debits/credits can post to account.	90%	96%
Positive Pay	Compares checks/ACH debits to a list provided by customers.	93%	94%
Post no debits accounts	Blocks debits from posting to account.	63%	95%
Two-factor authentication or other security layers for payments	Security method that requires two forms of authentication to submit payments and other banking activity.	89%	63%
Counsel on structuring accounts to minimize risk	Receive best practice advice to ensure accounts are structured to optimize efficiency and reduce risk.	87%	78%

Source: 2024 AFP® Payments Fraud and Control Survey Report

Best Practices To Protect Your Company From External And Internal Fraudsters

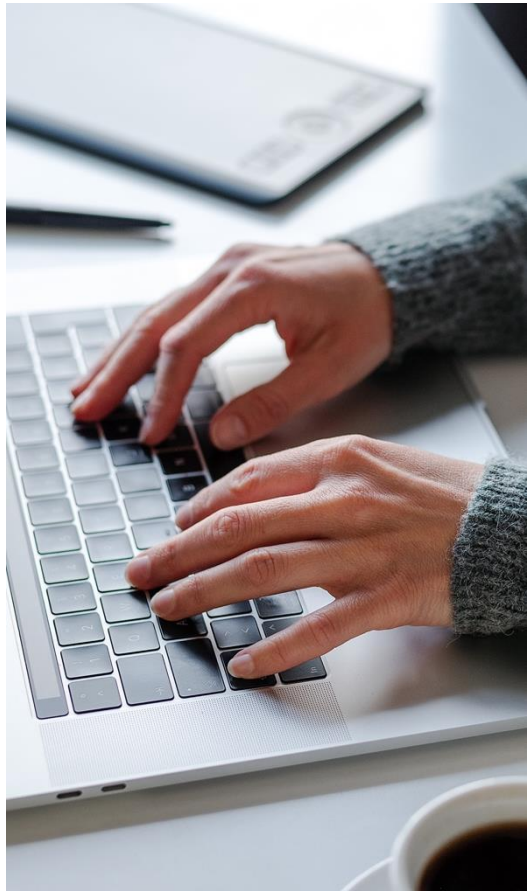
Establish A Disaster Recovery Plan

Prepare procedures for risk and fraud mitigation with the help of all trusted advisors to the company.

- **Attorney**
- **Accountant**
  With forensic accounting input
- **Bank relationship manager**
  With treasury management input
- **Insurance professional**
- **Key leadership of the company**
  Executive management, with IT professionals

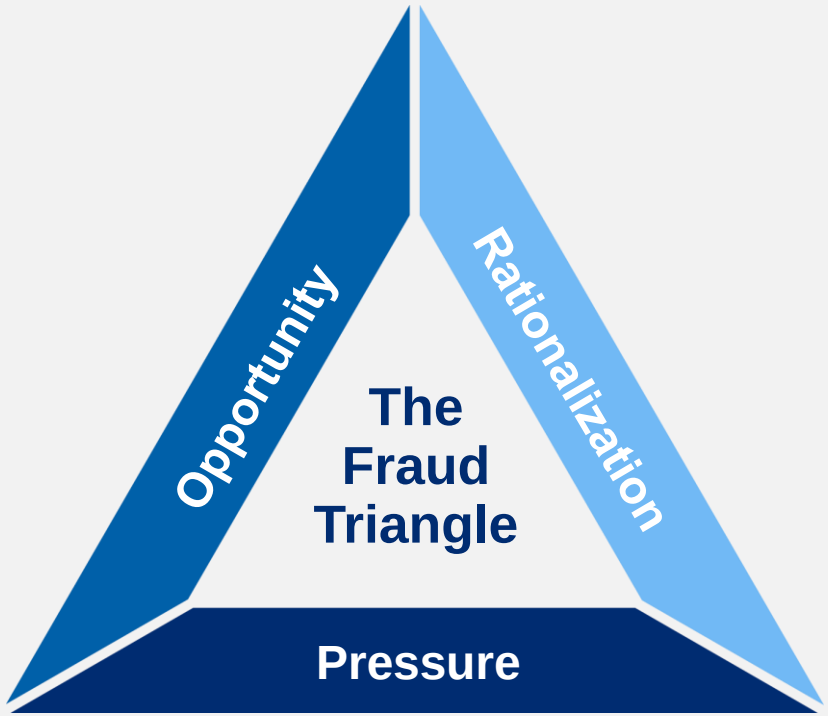
Implement Controls To Mitigate External Fraud

External Controls



- Engage outside professional to test internal controls
- Accounting firm for audit, review or compilation
- Protection of hardware & software
- Security of documents / checks
- Back-up information & review procedures

Establish Controls To Mitigate Internal Fraud



Stay up-to-date on System Security

- Observe and pursue unusual behavior or transactions
- Focus procedures on Accounts Receivable and Accounts Payable
- Daily reconciliation
- Move away from paper-based transactions
- Utilize Image Archive or other cloud-based storage

Employee Controls

- Segregation of duties and approval levels
- Hiring procedures
- Testing of processes
- Establish fraud hotline

Accounting/Treasury Department Controls

- Audit, review or compilation with testing

Tag: You’re A Victim Of Fraud: Now What?

Look Out For Warning Signs That Fraud Occurred

People

Employee habits/lifestyle

Data

- Information not being shared
- Vendor(s)/Bank(s) call with service or payment inquiries

Accounting

- Variances in results vs. budget
- Slower-than-normal collection of A/R
- Slower-than-normal reconciliation
- Co-mingling of funds among various entities
- Reports aren't prepared on time

Implement Your Action Plan

Quickly: Implement your Disaster Recovery Plan

- Contact accountant
- Engage forensic accountant
- Contact bank relationship manager and/or treasury management professional
- Contact attorney
- Contact insurance company

Call law enforcement after checking with legal counsel

DO NOT have IT personnel attempt to find the problem

Implement new controls

What's Next For Fraud Prevention?

Threats

1. **Customers and businesses are increasingly being targeted as frauds** have identified these as vulnerabilities (susceptible to scams, deepfakes, phishing, etc.).
2. **The level of first party fraud is greatly increasing:**
   - Account opening by mules/frauds
   - Authorized Push Payments (APP) – customers duped into sending money
   - Legitimate customers denying transactions they executed
3. **Fraudulent/nefarious merchants misrepresenting products**

Controls

1. Scam and ATO model availability
2. Increased control and risk signal orchestration
3. Improved passive authentication routines – use of text messaging to validate risky event/transaction occurrence

Thank You

You'll be receiving the recording and slides over the next couple of days.
Please share with anyone you feel would benefit.

To discuss your unique situation or to explore bank-provided fraud prevention tools, contact your banker.

Thanks to our panelists!

Kristen Saranteas
Kristen.Saranteas@firstcitizens.com

Sharon Crabbe
Sharon.Crabbe@firstcitizens.com

Ishanaa Rambachan
ishanaa_rambachan@mckinsey.com

CTP/CCM credits available: This webinar has been approved for up to 1.2 CTP/CCM recertification credits by the Association for Financial Professionals. You must score 80% or above on the quiz. Access the link to the quiz in the chat and in the follow up email.