Fraudsters Toolbox Series: RDC and Mobile Capture Fraud

Randall C. Traynham, AAP, AFPP, APRP, CTP, NCP

Director, Education

June 11, 2026

Disclaimer

- PaymentsFirst, through its Direct Membership in Nacha, is a specially recognized and licensed provider of ACH education, publications and support.
- Payments Associations are directly engaged in the Nacha rulemaking process and Accredited ACH Professional (AAP) program.
- Nacha owns the copyright for the Nacha Operating Rules & Guidelines.
- The Accredited ACH Professional (AAP) and Accredited Payments Risk Professional (APRP) is a service mark of Nacha.
- This material is derived from collaborative work product developed by Nacha and its member Payments Associations and is not intended to provide any warranties or legal advice and is intended for educational purposes only.
- This material is not intended to provide any warranties or legal advice and is intended for educational purposes only.
- This document could include technical inaccuracies or typographical errors and individual users are responsible for verifying any information contained herein.
- No part of this material may be used without the prior written permission of PaymentsFirst.
-

Learning Objectives

- Understand unique fraudulent tactics in RDC and Mobile Capture
- Learn risk detection strategies tailored for digital channels
- Develop measures to strengthen mobile deposit security
- Review industry best practices and emerging trends

Talking Points

- The RDC / Mobile Deposit Landscape
- Fraud Schemes & Attack Vectors
- Risk Detection Strategies
- Regulatory Framework & Best Practices
- Case Studies
- Q&A

The RDC / Mobile Deposit Landscape

Remote Deposit Capture has transformed the convenience but introduced significant fraud exposure

- Global RDC market: $12.74B in 2025, projected $29.83B by 2035
- 80% of organizations faced attempted mobile deposit fraud in 2024
- 65% of financial institutions reported RDC check fraud in 2024
- $21B – estimated U.S. Check Fraud losses in 2023 (FINCEN)
- 385% increase in check fraud since pandemic (U.S. Treasury)
- 31x more likely: check payments to involve fraud vs. real-time transactions

Why RDC Attracts Fraudsters

No face-to-face interaction with financial institution staff

Digital image manipulation opportunities

Deposit float exploitation window

Multi-institution duplicate presentment potential

Fraud Scheme #1

Duplicate Presentment

Depositing the same check multiple times across different channels or institutions

Mobile deposit at Institution A

Physical deposit at Institution B

RDC deposit followed by ATM deposit before clearing

Exceeded $400M in losses in 2023

Why?

- Lack of real-time cross-institution data sharing

Fraud Scheme #2

Check Kiting

Exploiting the deposit float between when checks are deposited and when they clear

Write bad check from Account A

- Deposit in Account B

Withdraw funds from Account B before check clears

Cover with another bad check from Account B to Account A

Digital alterations: Changing payee, amount, or date using image editing software

Chemical washing: Stripping ink from stolen checks and rewriting

Counterfeit checks: Fully fabricated using stolen account information

28% year-over-year increase in synthetic ID-related check fraud

Fraud Scheme #3

Altered & Washed Checks / Counterfeit

Fraud Scheme #4

Fake Check Scams

Fraudsters trick victims into depositing counterfeit checks via mobile banking

- Fake job postings with “advance payment” checks
- Overpayment scams requesting refund via wire or gift cards
- Mystery shopper and work-from-home schemes

Fraud Scheme #5

Account Takeover

Criminals gain access to victim's online / mobile credentials

Deposit fraudulent checks via victim's RDC / mobile app

Withdraw funds or transfer to external accounts before detection

Often combined with social engineering and phishing attacks

Create fake business or consumer entities with synthetic identities

Deposit high volume of fraudulent checks through RDC / Mobile

Withdraw funds before items are returned

Fraud Scheme #6

Synthetic Identity Fraud

Sophisticated scheme creating fictitious identities to open accounts, both commercial or consumer

Emerging Threat

- AI – generated deepfakes bypass biometric verification in mobile banking
- Deepfake Identity Bypass with synthetic audio / video used for account takeover attacks
- Dark Web Marketplaces — 1.9 million stolen U.S. checks appeared on dark web platform in 2024 along
- FinCEN alert issued November 2024 on deepfake fraud schemes
- Detection requires multi-layered AI defense systems

The Industrialization of Check Fraud

Real Case — SDNY (Southern District of New York) - June 2025): Six defendants charged in multi-million dollar check theft ring. They stole checks from USPS collection boxes in NY, chemically altered amounts and payees, then deposited via mobile and ATM across multiple institutions.

- 680K+ Check Fraud SARS filed in 2022 (all-time high, FinCen)
- 139% increase in mail thefts from mailboxes / drop boxes FY 2019 – FY 2023
- ~90% of mail theft incidents go unreported (U.S. Treasury estimation)

Risk Detection: Customer Due Diligence

- Enhanced screening for RDC / mobile deposit enrollment
- Verify identity with multi-factor authentication
- Risk-base approval process for higher-risk customer segments
- Ongoing account behavior monitoring post-enrollment

Risk Detection: Transaction Controls

- Set dollar limits per check, per day, and per month
- Implement velocity limits (number of items deposited)
- Tiered limits based on account age and history
- Dynamic adjustments based on real-time risk scoring

Risk Detection: Duplicate Detection Systems

- Image-based duplicated detection across all channels
- Cross-institution duplicate databases
- Real-time matching at point of deposit

Risk Detection: Image Quality Analysis

- Automated detection of blurry or poor-quality images
- Identify signs of digital alteration or manipulation
- Flag mismatched numerical and written amounts
- Verify indorsement presence and authenticity

Risk Detection: Behavioral Analytics

- Monitor deposit patterns: timing, frequency, amounts
- Detect anomalous behavior vs customer's baseline
- Flag rapid deposit-withdrawal cycles (kiting indicator)
- Device fingerprinting and geolocation analysis

Risk Detection: Positive Pay Integration

- Verify check number, amount, date, and payee name
- Flag duplicate check number automatically
- Exception reporting for unauthorized items

Risk Detection: Real-Time Risk Scoring

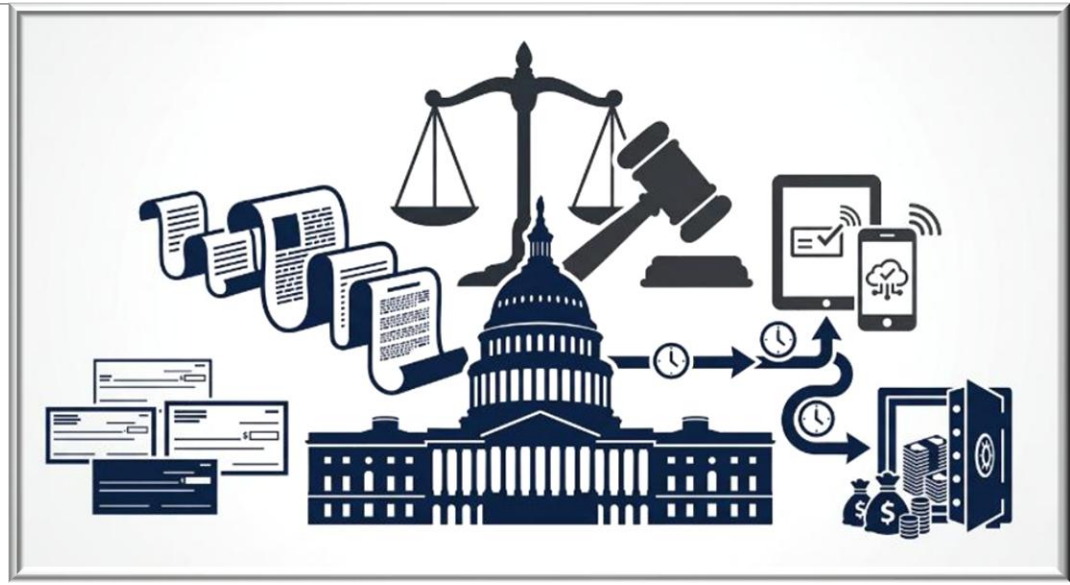
- AI-driven scoring at moment of deposit across all channels
- Instantly clear low-risk items, hold or escalate high-risk
- 75% + kiting case detection at deposit time (industry data)
- Combine transaction, account, and channel metadata

Risk Detection: Dynamic Funds Availability

- Move beyond fixed hold times to fraud-responsive availability rules
- Risk-based holds: instant, partial, or complete based on score
- Extended holds for high-risk deposits
- Post-deposit risk updates trigger fund freezes

Regulatory Framework: Regulation CC

Funds Availability Requirements and Disclosure Obligations for RDC deposits



- Check 21 Act enables electronic check processing
- Regulation CC Funds Availability applies (with contractual interpretation)
- State laws may impose additional requirements

Regulatory Framework: UCC 4-406

Customer's duty to discover and report unauthorized signatures or alterations

- Customers must examine statements with reasonable promptness
- 1-year deadline to report unauthorized signatures / alterations
- 3-year deadline to report unauthorized indorsements (UCC 3-118)

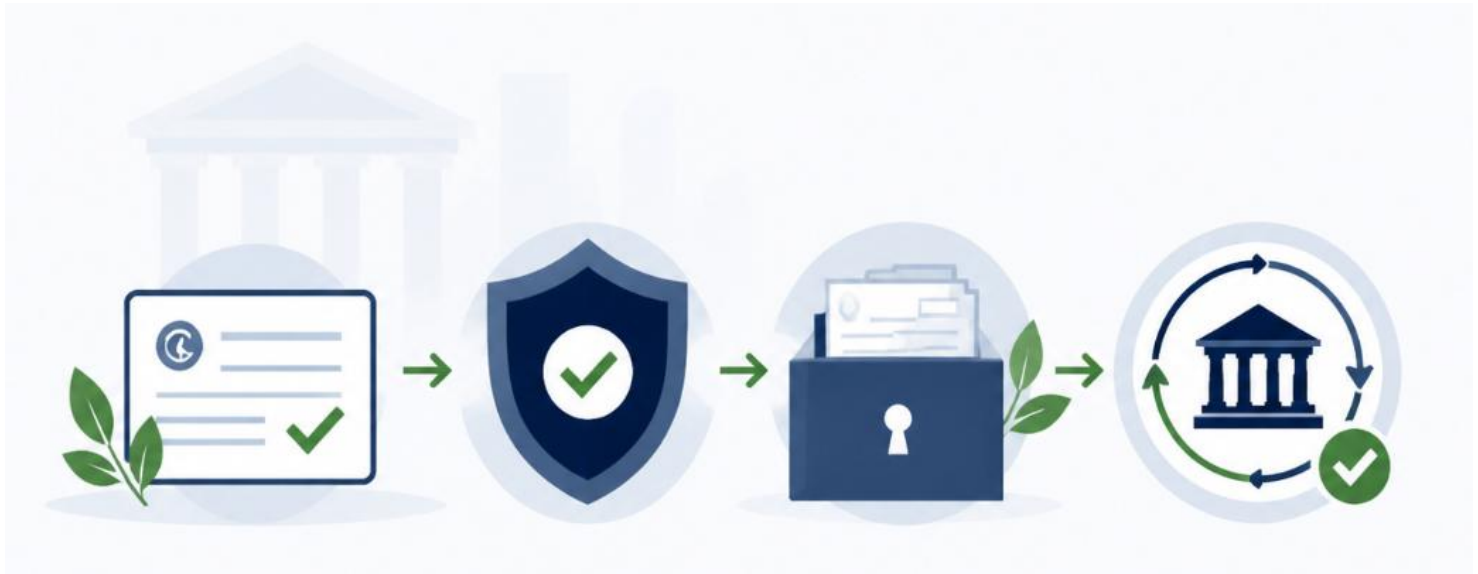
Regulatory Framework: FFIEC Guidance

January 2009 guidance on RDC risk management remains foundational

- Comprehensive risk assessment required before implementation
- Board / management oversight and governance
- Sound risk mitigation and monitoring systems

Best Practice: Comprehensive Agreements

- Clearly define roles, responsibilities, and liabilities
- Include indorsement requirements and check handling procedures
- Specify deposit limits, holds, and exception processes
- Address check storage, retention, and destruction requirements



Best Practice: Layered Authentication

- Multi-factor authentication (MFA) for all mobile deposit sessions
- Step-up authentication for risk spikes during deposits
- Biometric verification with anti-deepfake detection
- Device intelligence and behavioral biometrics

Best Practice: Staff Training Programs

- Regular training on fraud scheme recognition
- Real-time risk feedback interpretation at point of deposit
- Structured intervention procedures for flagged items
- Annual refreshers on emerging fraud trends and tactics

Best Practice: Member Education

- Educate members on fake check scams and red flags
- Clear communication about deposit holds and verification
- Warning messages about employment and overpayment scams
- Promote secure check handling and indorsement practices

Best Practice: Continuous Monitoring

- Real-time transaction monitoring across all deposit channels
- Automated alerts for suspicious patterns and anomalies
- Cross-channel analysis to detect kiting schemes
- Regular review of exception reports and fraud incidents

Best Practice: Technology Investments

- Advanced fraud detection platforms with Artificial Intelligence / Machine Learning capabilities
- Industry-shared check fraud databases
- Deepfake detection for biometric authentication
- Automated image quality and alteration detection tools

Integrated monitoring across branch, RDC, mobile, ATM, ACH, wire, P2P

- Stablecoin – distributed ledger platforms as a payment mechanism

Unified fraud detection platforms replacing siloed systems

Coordinated response to multi-channel attack patterns

Emerging Trend

Cross-Channel Fraud Detection

Fraudsters exploit multiple channels simultaneously

Your RDC Risk Assessment Framework

Identify

- Identify critical information assets and risk categories

Determine

- Determine inherent and residual risk profiles

Document

- Document existing controls and mitigation measures

Develop

- Develop ongoing remediation and monitoring plans

Action Items for Your Financial Institution

Review	Review RDC agreements for completeness and compliance
Audit	Audit current fraud detection capabilities and identify gaps
Enhance	Enhance member education on mobile deposit fraud

RDC Fraud is escalating: 65% of FIs experienced fraud in 2024

Layered defenses essential: technology, policies, training, monitoring

Real-time detection critical to prevent float exploitation

Regulatory landscape evolving with greater emphasis on fraud prevention

Takeaways

Transaction & Account Red Flags

ACCOUNT-LEVEL RED FLAGS

- 🆕 New account (under 30-90 days) with immediate large deposits
- 📈 Sudden spike in deposit volume or frequency
- 🔄 History of returned / bounced check deposits
- 📱 Minimal day-to-day spending activity — only deposits and withdrawals

TRANSACTION-LEVEL RED FLAGS

- ⚡ Large deposit immediately followed by wire/ACH/P2P transfer
- 🕐 Deposits at unusual hours or from unfamiliar device/location
- 📷 Check image quality issues: altered MICR line, inconsistent fonts
- 🔁 Same check serial number or routing/account combination seen before

💡 **CU Advantage:** Your local member knowledge is your competitive edge. Behavioral anomalies that another FI might miss are more visible to credit unions who know their members' financial patterns.

Consideration	Low risk indicators	Moderate risk indicators	High risk indicators
Tenure/relationship	>2–3 years, stable balances, no losses	6–24 months, limited history	New or re-opened, prior charge-offs
Industry	Low-fraud industries (professional services, established non-cash-intensive)	Mixed-risk industries	High-fraud/high-cash (check cashers, used auto dealers, money services)
Volume & limits	Low volumes, low limits, small average item size	Moderate volumes/limits	High volumes, high limits, large items
Return/fraud history	No or minimal returns, no fraud	Some returns, no fraud	High returns, prior fraud or SARs
Geography	Local, known markets	Broader domestic	High-risk or foreign geographies
Internal risk rating	Strong, low risk	Satisfactory	Marginal or special mention

Customer-Level RDC / Mobile Suitability Table

Questions?

AAP™
Accredited
ACH Professional

APRP™
Accredited Payments
Risk Professional

AFPP
Accredited Faster
Payments Professional™

PaymentsFirst

Continuing Education Credits

Fraudster's Toolbox: RDC and Mobile Capture Fraud

June 11, 2026

This session is worth 1.0 credits. Please keep this slide for your records.

Contact Us

(678)-384-9791

www.paymentsfirst.org

education@paymentsfirst.org

@PaymentsFirst