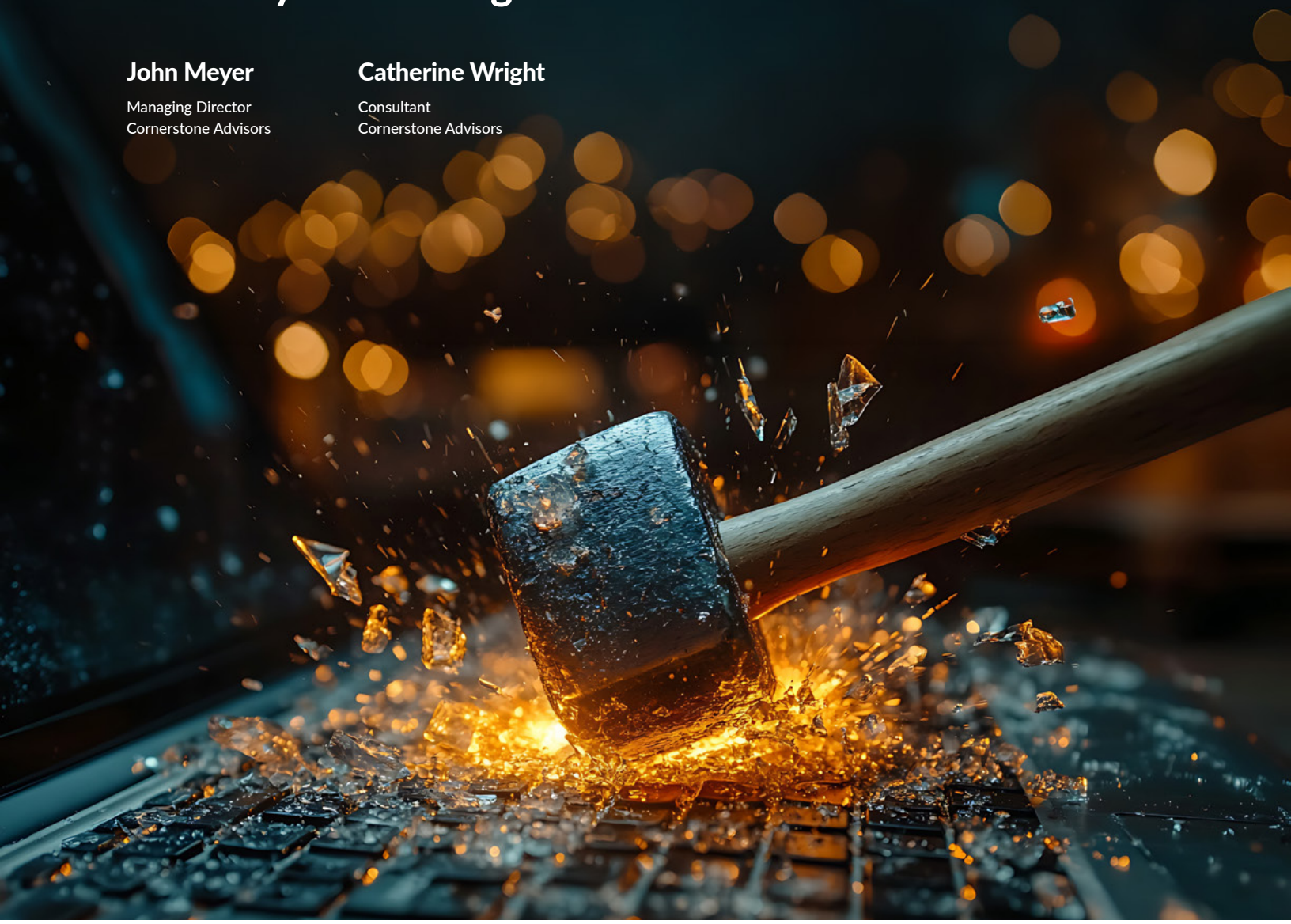
Cornerstone ADVISORS

Hammer the Scammer: The Fraud Defense Playbook

Industry Benchmarks. Winning Strategies. Five Plays for Stronger Defense.

John Meyer
Managing Director
Cornerstone Advisors

Catherine Wright
Consultant
Cornerstone Advisors



COMMISSIONED BY

THE LEAGUE OF CREDIT UNIONS & AFFILIATES

LEVERAGE Your Advantage

Hammer the Scammer: The Fraud Defense Playbook

©2026 Cornerstone Advisors

Hammer the Scammer: The Fraud Defense Playbook and its contents are protected by copyright laws, contain the trademark Cornerstone Advisors, and are Cornerstone's confidential and proprietary information. No part of this report shall be reproduced, stored in a retrieval system or transmitted by any means—electronic, mechanical, photocopying, recording or otherwise—without written permission from Cornerstone Advisors.

Cornerstone assumes no liability with respect to the use of the information contained herein, which is provided "as is," and there are no warranties of any kind provided by Cornerstone with respect to this report.

Cornerstone assumes no responsibility for errors or omissions and will not be liable for any damages resulting from the use of the information contained herein.

For information, contact:

Cornerstone Advisors
7272 E. Indian School Road, Suite 400
Scottsdale, AZ 85251
Tel: 480.423.2030
Email: info@crnrstone.com

TABLE OF CONTENTS

1 Introduction

1 What Credit Unions Are Telling Us

3 Account Takeover Is the Primary Threat

3 Existing Authentication Remains Heavily Dependent on Traditional Methods

3 False Declines Cause Friction

5 The Emerging Role of AI and Behavioral Technology

6 Five Plays Credit Unions Can Put Into Action

6 Implement Biometric and Behavioral Validation

6 Reevaluate Funds-Availability Practices

7 Strengthen Card-Number Security

7 Conduct Recurring Member Education

8 Participate in Fraud Consortiums and Peer Networks

9 Conclusion

10 About the Authors

11 About Cornerstone Advisors

11 About The League of Credit Unions & Affiliates

11 About *LEVERAGE*

Introduction

Fraud has always required credit unions to balance security, operational efficiency and member experience. Fraudsters are exploiting stolen credentials, compromised devices, social engineering, payment speed and fragmented controls to attack members across channels. At the same time, credit unions must protect the personal service and ease of access that distinguish them from larger financial institutions.

The challenge is no longer limited to stopping clearly unauthorized transactions. Credit unions must also identify scams in which members appear to authorize a payment, recognize account takeover before funds leave the institution, manage growing alert and dispute volumes, and avoid frustrating legitimate members with unnecessary declines and authentication steps.

Research from surveys conducted with The League/*LEVERAGE*, interviews conducted with high-performing credit unions and performance benchmarks from Cornerstone Advisors' Performance Vault point to a common conclusion: Fraud requires an enterprise response. Technology remains important, but technology alone is not enough. Governance, staffing, member education, operational controls, measurement and collaboration must work together.

What Credit Unions Are Telling Us

Credit unions are confronting fraud across nearly every major payment rail. Checks, debit cards, credit cards, automated clearing house payments, wires, peer-to-peer payments, ATMs and loans all create distinct points of exposure. Because the risk does not reside within a single channel or department, traditional controls focused on individual products or transaction types are increasingly insufficient.

To provide additional industry context, this playbook incorporates benchmarks from Cornerstone Advisors' Performance Vault™, a proprietary performance-benchmarking platform with over 300 participating financial institutions. Performance Vault™ data shows that median annual fraud losses, excluding teller overages and shortages and including debit- and credit-card fraud, totaled **$10.64 per checking account** annually for credit unions in the U.S., up over 10% from the prior year. The lower end of the benchmark range was $9.16 per account, while the upper end reached $15.99.

Performance Vault™ data shows that median annual fraud losses, excluding teller overages and shortages and including debit- and credit-card fraud, totaled $10.64 per checking account annually for credit unions in the U.S., up over 10% from the prior year.

By payment type, median annual fraud losses included:

- $1.01 per checking account from check fraud
- $0.59 per checking account from ACH and wire fraud
- $0.23 per checking account from P2P fraud
- $0.21 per checking account from ATM fraud
- $0.48 per checking account from other fraud categories

Card losses add another significant dimension. Median debit-card net fraud losses equaled **0.0411% of purchase volume**, while median credit-card net fraud losses equaled **0.0550% of purchase volume.**

CORNERSTONE'S TAKE:

Fraud losses are up 10% year over year for U.S. credit unions across all payment rails. Credit unions are fighting increasingly connected, cross-channel fraud with fragmented organizational responsibilities, traditional authentication methods and incomplete measures of fraud-management performance. The benchmarks and strategies in this playbook can help credit unions wage a winning defense against fraud.

Account Takeover Is the Primary Threat

Account takeover, or ATO, emerged as the most significant fraud type identified through the interviews with credit unions of all sizes. A clear majority of the institutions interviewed identified account takeover as the fraud type responsible for their greatest dollar losses during the prior two years. Criminals are calling credit union members, claiming to be from the "fraud department" and persuading them to disclose sensitive information such as account log in credentials or one-time passcodes. Once inside an account, a fraudster may initiate card activity, create a new payee, transfer funds, change contact information or exploit multiple payment channels.

The broader risk also includes authorized push payment scams. In these cases, the member themselves initiates or approves a payment after being manipulated by a criminal. Traditional transaction controls may see a recognized user completing an authorized action, even though the underlying purpose is fraudulent.

Other sources of ATO include data breaches, phishing campaigns, law enforcement impersonation scams and other social engineering tactics. Therefore, it is no longer enough to determine whether the correct password or one-time passcode was entered. Credit unions must also consider whether the device, behavior, destination, timing and transaction pattern are consistent with a member's normal activity.

Existing Authentication Remains Heavily Dependent on Traditional Methods

Nearly all of the institutions interviewed used SMS one-time passcodes for step-up authentication, while a majority also used knowledge-based authentication. By comparison, only a minority reported using biometrics, and approximately one-third used behavioral analytics as an authentication method.

Traditional authentication is still an important component of a layered control environment. However, stolen credentials, compromised mobile devices, social engineering and real time manipulation can weaken the effectiveness of any single control. Credit unions have an opportunity to strengthen authentication by incorporating biometric, behavioral, device, identity and transactional signals.

False Declines Cause Friction

Credit unions must prevent losses without unnecessarily declining legitimate transactions or creating excessive member friction. Strong controls can reduce exposure, but poorly targeted controls can also interrupt purchases, drive members to another card, generate calls and increase staff workload.

Approximately half of the institutions interviewed did not track their card false-decline rate. Among institutions that measured the rate, reported results varied considerably, and a minority expressed dissatisfaction with existing false-decline performance.

A false decline can have effects beyond the individual transaction. It can increase contact-center volume, generate member frustration, shift card activity to another issuer and cause a member to abandon a purchase. These consequences may not appear within traditional fraud-loss reporting.

Fraud programs should therefore measure both risk and friction. Relevant measures may include fraud losses, false declines, authorization rates, member contacts, abandoned transactions, alert volumes, manual review rates and the time required to resolve disputes. Looking at these measures together gives leaders a more complete view of whether controls are creating the intended result.

CORNERSTONE'S TAKE:

Smarter credit unions are fighting criminals that are getting members to reveal their credentials via phishing or banking impersonation scams. Many credit union compliance teams and legal teams argue that "information does not equal authorization," so if a member is being scammed the institution reimburses the loss and bears the expense.

The Emerging Role of AI and Behavioral Technology

Artificial intelligence and behavioral analytics can help institutions evaluate more signals, identify anomalies and prioritize alerts. Adoption, however, remains limited.

Among the institutions interviewed, a large majority either were not using AI and machine learning in payment decisioning or continued to rely primarily on rules-based approaches. Only a small minority reported using AI-assisted decisioning or AI-primary decisioning with human review.

Use of individual data signals was also uneven. Most institutions used third-party identity trust or risk scores. Approximately half used IP reputation or behavioral. Only a minority used machine-learning models, biometric signals or device fingerprinting.

The survey responses included favorable observations about behavioral technology. Respondents described tools such as BioCatch and Callsign as effective for blocking ATO and P2P fraud by looking at thousands of signals within digital banking sessions and pushing stepped-up authentication when suspicious behavior is detected. Some of those behaviors include device patterns, navigation, typing cadence, transactional activity and other risk signals in real-time that passwords and one-time passcodes cannot provide alone.

> "The opportunity is to use technology to distinguish normal activity from unusual behavior and direct limited human capacity toward the cases where it adds the most value."

Interviewees were adamant, however, that AI should enhance rather than eliminate human judgment. High-risk cases still require investigator review, member contact, documentation and escalation. The opportunity is to use technology to help distinguish normal activity from unusual behavior, reduce low-value manual review and direct limited human capacity toward the cases in which it adds the most value.

Credit unions evaluating AI-enabled fraud tools should also establish appropriate governance. This includes defining the business purpose, identifying the data used, testing outcomes, assigning ownership, monitoring false positives and determining when human review is required. Fraud models should be evaluated not only on losses prevented, but also on member friction, operational workloadency of decision-making.

Just as credit unions are leveraging AI for fraud detection and interdiction, the criminals are leveraging AI to write more convincing phishing emails and to set up phishing sites more easily to harvest login credentials. One study showed that the bad guys get 59% higher click rates when using AI to draft their phishing emails. Therefore, credit unions need to measure signals that indicate something else is amiss when a criminal attempts to login from an unfamiliar device or behaves differently from the member whose credentials they harvested.

CORNERSTONE'S TAKE:

As ATO has found ways around the traditional security of usernames/passwords and one-time passcodes, smarter credit unions are deploying AI that detects unusual behavior and other signals in real-time and employs stepped-up authentication for continuous identity verification.

Five Plays Credit Unions Can Put Into Action

Cornerstone interviewed the top performing credit unions to learn their secret sauce for preventing ATO fraud. We came away with five offensive plays credit unions should deploy to strengthen their defenses:

1 Implement Biometric and Behavioral Validation

2 Reevaluate Funds-Availability Practices

3 Strengthen Card-Number Security

4 Conduct Recurring Member Education

5 Participate in Fraud Consortiums and Peer Networks

1. Implement Biometric and Behavioral Validation

Credit unions should expand authentication beyond passwords, security questions and SMS passcodes. Biometric and behavioral technologies can provide additional signals related to the device, user interaction and transaction pattern.

Implementation should follow a risk-based approach. Rather than introducing friction for every interaction, institutions can apply additional validation to higher-risk events such as:

- Enrollment of a new device
- Changes to contact information
- Password or credential resets
- Creation of a new payee
- Unusual payment behavior
- Higher-risk transfers
- Activity inconsistent with the member's prior behavior

Credit unions should also define how risk signals will affect the member experience. A higher-risk event may trigger additional authentication, delay a transaction, generate an investigator alert or require member contact. These response paths should be consistent, documented and measurable.

2. Reevaluate Funds-Availability Practices

Funds-availability practices should be reviewed against current check, new account, deposit and account-takeover risks. Credit unions should identify where faster access creates disproportionate exposure and where risk-based holds may be appropriate.

The objective should not be to delay funds broadly. It should be to apply differentiated controls based on factors such as account history, deposit characteristics, channel, transaction behavior and identified fraud patterns.

Credit unions should coordinate any changes across fraud, deposit operations, compliance, branches, contact centers and digital banking teams. Member communications should clearly explain when funds will become available and what actions may be required.

3. Strengthen Card-Number Security

Credit unions should evaluate capabilities that reduce the useful life of compromised card credentials, including dynamically generated or randomized card information where supported by their card and digital ecosystems.

This strategy can be paired with:

- Card controls
- Real-time member notifications
- Tokenization via systems like 3DS
- Digital wallet provisioning controls
- Rapid card reissuance
- Monitoring for unusual card-not-present activity

Institutions should measure whether these capabilities reduce losses and member contacts rather than assuming adoption alone produces value. Relevant measures may include compromised-card replacement rates, card-not-present losses, time to re-issue cards, fraud-related contacts and changes in legitimate authorization activity.

4. Conduct Recurring Member Education

Member education must address how modern scams actually occur. Programs should explain that criminals may impersonate the credit union, government agencies, businesses, family members or other trusted parties. Education should reinforce that legitimate employees will not pressure members to disclose credentials or move funds urgently.

Credit unions can use:

- Branch education events
- Webinars
- Digital banking messages
- Email and social media content
- Transaction-specific warnings
- Contact-center scripts
- Targeted outreach tied to current fraud patterns

Education should be ongoing and responsive to emerging scams rather than treated as an annual communication. Messages should provide clear examples, warning signs and specific actions members can take when they are uncertain about a request.

5. Participate in Fraud Consortiums and Peer Networks

Fraud patterns often affect multiple institutions before any one credit union has enough activity to identify the broader trend. Consortium data and peer collaboration can help institutions recognize compromised identities, devices, accounts, checks and payment destinations earlier.

Credit unions should establish processes for receiving intelligence, determining its relevance and translating it into changes to rules, alerts, member communications, or operating procedures.

Participation should extend beyond simply receiving information. Institutions should determine which internal function reviews fraud intelligence, how urgent issues are escalated and how lessons are shared across fraud, operations, payments, digital banking, information security, compliance and member-facing teams.

Conclusion

Account takeover fraud is becoming more connected across identity, digital banking, payments and social engineering. ATO stands at the center of that convergence, while many institutions are managing high alert volumes, incomplete performance measurement, manual processes and limited investigative capacity.

Smarter credit unions do not need to solve every dimension of fraud at once. They do need a coordinated strategy that connects authentication, payment controls, technology, staffing, member education, collaboration and performance measurement.

The strongest ATO fraud programs will not simply decline more transactions or generate more alerts. They will identify risk earlier, apply friction more precisely, help members recognize manipulation, reduce unnecessary manual review and give investigators clearer information.

ATO fraud prevention will always involve tradeoffs. The practical objective is to make those tradeoffs visible and measurable, then direct limited resources toward the controls that reduce the most risk while preserving the trusted member relationships credit unions have worked to build.

The strongest ATO fraud programs will not simply decline more transactions or generate more alerts. They will identify risk earlier, apply friction more precisely, help members recognize manipulation, reduce unnecessary manual review and give investigators clearer information.

About the Authors

John Meyer | Managing Director

As a managing director with Cornerstone Advisors, John Meyer leads the firm's Business Intelligence and Data Analytics practice. Before joining Cornerstone, John was chief strategy officer and chief product officer at Abrigo (formerly Banker's Toolbox). His experience includes developing product strategies for anti-money laundering and fraud detection for over 1,000 U.S. financial institutions and ALLL solutions for over 1,200 institutions. Before Abrigo, John was with Harland Financial Solutions, where he held several senior positions including general manager over the branch automation and internet banking team.

p (407) 790-9015

e jmeyer@crnrstone.com

in /john-meyer-56375

Catherine Wright | Consultant

Catherine Wright brings a unique background in law, business and client service to Cornerstone Advisors. Before joining Cornerstone, Catherine worked as an Intellectual Property attorney, where she specialized in trademark protection, including the application and prosecution of trademarks with the USPTO. She also supported clients by drafting and reviewing a wide range of business contracts. Catherine's foundation in business and legal strategy enables her to approach client challenges with precision, structure, and a strong understanding of operational risk. Earlier in her career, she held leadership roles at Lululemon.

p (480) 660-5285

e cwright@crnrstone.com

in /wright-catherine

ABOUT
Cornerstone Advisors

For over 20 years, Cornerstone Advisors has delivered gritty insights, bold strategies and data-driven solutions to build smarter banks, credit unions and fintechs. From technology system selection and implementation to contract negotiations, vendor management, performance improvement programs, strategic planning, merger integration and enterprise program management, Cornerstone combines its expertise with proprietary data and research to help financial institutions thrive in today's challenging environment.

p 480.423.2030

e info@crnrstone.com

crnrstone.com

in /cornerstoneadvisors

@CstoneAdvisors

ABOUT
The League of Credit Unions & Affiliates

The League of Credit Unions & Affiliates provides a platform for advocacy, collaboration and innovation, representing 368 credit unions across Alabama, Florida, Georgia and Virginia and their 33.8 million members, as well as $477.6 billion in assets. The League serves as an advocate through credit union engagement, advocacy impact, Foundation resources, and *LEVERAGE* products and services.

www.the-league.coop

in /the-league-of-credit-unions-and-affiliates

/TheLeagueofCreditUnionsandAffiliates

@theleagueofcus

@theleagueofcus

ABOUT
LEVERAGE

LEVERAGE, the service corporation for The League of Credit Unions & Affiliates, is the business services provider that leverages credit union system resources, relationships and industry knowledge for optimal performance and sustained growth of its clients and business partners. It works to offer credit unions best-in-class products and services that result in reducing costs, maximizing results and making the most difference.

myleverage.com

in /myleverage

/MyLeveragePoweredbyTheLeague

Have questions regarding this report?

Ron Shevlin
Chief Research Officer | Cornerstone Advisors

rshevlin@crnrstone.com