CYBER-ENABLED FRAUD

From resilience to results in credit unions

OECS Credit Union Summit 2026

Navigating Change: From Resilience to Results

Akeem Shaw (Mr.)

Manager, Financial Compliance Unit

Office of National Drug and Money Laundering Control Policy

Technology makes everyday banking easier

- Members can check balances and transactions without visiting a branch.
- Digital payments let members send money and pay bills more quickly.
- Online shopping gives members access to goods and services wherever they are.
- Mobile and online services extend access beyond branch hours.

Convenience also creates new openings for fraud

Every new digital interaction gives criminals another way to reach a member.

- A convincing message can lead a member to reveal a password or one-time code.
- A false shopping page or payment request can redirect money to a criminal.
- A compromised account can move funds before the member notices.

What is cyber-enabled fraud?

Fraud carried out or scaled through digital technology.

- Criminals use calls, messages, email, websites or online accounts to deceive a member or gain access.
- The member may be tricked into sending money or disclosing credentials and verification codes.
- Funds can then move rapidly through digital payments, recipient accounts or cash withdrawals.

Adapted from FATF, Cyber-Enabled Fraud (2026); ONDCP Advisory No. CEF 1/2026.

What’s the _____ishing problem?

Click the video to play. Duration: approximately 4 minutes 44 seconds.

Local typology: the telecom impersonation call

01 THE CALL

A caller claims to be from a local telecom provider updating its system.

02 THE EMAIL

They ask only for the member's email address, preferably Gmail.

03 THE CODE

The fraudster initiates account recovery. A Google code reaches the member's phone.

04 THE DISCLOSURE

The caller says they sent the code. The member reads it aloud.

05 ACCOUNT ACCESS

The fraudster may access Gmail and any saved credit union credentials in Google Password Manager.

06 FUNDS MOVE

The credit union account is accessed and funds can be transferred or withdrawn rapidly.

Local scenario. Google Password Manager stores saved passwords; Google Wallet stores payment methods and passes.

Criminals often target the person

A convincing call can bypass strong technology.

- An impostor claims to represent a trusted organisation.
- Urgency persuades a member to share a code or approve access.
- The credit union must recognise the warning signs and act quickly.

Four patterns identified by the ONDCP

- Smishing and vishing: texts and calls seek credentials, security answers and one-time codes.
- Email takeover: a false “Yes, it’s me” prompt lets criminals intercept authentication messages.
- Marketplace fraud: a purported buyer or seller extracts account details or online credentials.
- Proxy withdrawal: a member receives illicit funds and withdraws or forwards them for a stranger.

ONDCP Advisory No. CEF 1/2026, pp. 1–2.

Signals that should trigger review

- Unverified device or browser, unusual IP or location, repeated failed logins or sudden password resets.
- New beneficiary created just before rapid transfers, mobile top-ups or layered payments.
- Funds moved immediately after an anomalous login, including several transfers near alert thresholds.
- Multiple ATM withdrawals soon after suspicious incoming funds.

ONDCP Advisory No. CEF 1/2026, pp. 2–3; additional controls proposed for LFIs.

Verification when compromise is suspected

- Contact the member through a previously established channel before releasing an unusual payment.
- Apply step-up authentication and a temporary hold where policy and legal authority permit.
- Review new beneficiary details and payment instructions against the member's usual activity.
- Escalate to Fraud, IT and the Compliance Officer through a defined decision path.

Monitoring across payment services

- Review EFTs, bill payments, peer-to-peer transfers and mobile top-ups against each member's normal behaviour.
- Tune alert thresholds to intercept rapid or structured payments, unfamiliar recipients and unusual business patterns.
- Escalate incomplete, illegible or alias-only beneficiary details; obtain and verify the required information before processing.
- For institutions that offer international wires, add jurisdiction, counterparty and cross-border pattern checks.

Apply controls to services actually offered. Credit unions without international wires should focus on their domestic channels.

A response clock for suspected fraud

Immediately	Suspend compromised access and take authorised steps to secure funds.
Without delay	File a SAR with the FIU; do not await the internal investigation. Supplement later.
Live incident	Contact your FIU/LEAs without delay.
Coordinate	Preserve digital evidence and work with LEAs

ONDCP Advisory No. CEF 1/2026, p. 3; use the current official CEF template when provided.

Actions that can cost critical time

The first minutes may determine whether fraudulent funds can be preserved.

Do not make a written request a routine precondition for urgent, lawful information sharing with the FIU when funds may dissipate. Record the request and response; formal written confirmation should follow.

Do not leave a compromised channel active while seeking administrative sign-off. Escalate and apply authorised protective measures.

Do not route urgent indicators through slow internal handoffs when designated response contacts can act.

Supervisory Authority expectations

- Maintain tested monitoring and verification across the digital services the credit union offers.
- Educate staff and members about current scam approaches, including OTP requests and push approvals.
- Consider pausing an unsafe product or service until effective controls are restored.
- Act promptly on recipient accounts holding suspected fraud proceeds, including holds or freezing where lawful authority permits.

ONDCP Advisory No. CEF 1/2026, pp. 2–3; protective measures subject to applicable legal authority.

Information sharing limits the next loss

The same scam can reach several institutions before one victim reports it.

- Share indicators of compromise and emerging methods promptly among Compliance, IT, Fraud and Internal Audit.
- Use designated persons to exchange actionable patterns across institutions through approved channels.
- Communicate the steps taken to contain exposure so other institutions can adapt their controls quickly.

Evidence that helps trace the money

- Transaction IDs, amounts, timestamps, beneficiary details and onward movement.
- Login history, device and IP data, MFA events, password resets and session records.
- The original message, call details, screenshots and the member's account of events.
- An auditable record of decisions, contacts, preservation steps and reporting.

Management should ask for results

- How long does it take from the first alert to a human decision?
- What share of reported cases reached the right teams within the target time?
- How much was prevented, recovered or lost, and through which channels?
- Which cases led to a control change and a tested improvement?

From resilience to results

A member's first report can be the best chance to limit the loss.

Give staff a clear decision path. Keep the data needed to trace funds. Measure whether the response worked.

Questions and discussion

Mr. Akeem Shaw

Manager, Financial Compliance Unit

Office of National Drug and Money Laundering Control Policy