DCUC
DEFENSE CREDIT UNION COUNCIL

1627 Eye St, NW
Suite 935
Washington, DC 20006

202.734.5007
www.dcuc.org

Jason Stverak
Chief Advocacy Officer

July 14, 2026

The Honorable Rand Paul
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

Re: Statement for the Record for the July 15, 2026 Hearing - "Exposing Fraud in America"

Dear Chairman Paul and Ranking Member Peters:

On behalf of the Defense Credit Union Council (DCUC), thank you for convening the Committee's July 15, 2026 hearing, "Exposing Fraud in America." DCUC welcomes the Committee's focus on identifying fraud, strengthening accountability, protecting public resources, and safeguarding American families. Fraud against government programs and fraud against individual consumers are closely connected: the same criminal networks use stolen identities, synthetic identities, compromised accounts, mule networks, spoofed communications, and social engineering to divert public benefits and steal household savings.

DCUC is the national trade association representing more than 200 defense-focused credit unions serving more than 40 million members, including active-duty servicemembers, members of the National Guard and Reserve, veterans, military retirees, Department of Defense civilian employees, and military families. Because these members frequently relocate, deploy overseas, access accounts remotely, use APO/FPO addresses, and receive military pay or veterans benefits, they can face distinctive exposure to identity theft, account takeover, check and payment fraud, imposter scams, benefit redirection, elder financial exploitation, and AI-enabled deception. For a military household, a fraud loss can compromise more than a bank balance; it can destabilize a family budget, damage credit, and create financial stress with readiness and security-clearance implications.

The scale of the threat continues to grow. The FBI's 2025 Internet Crime Report recorded more than one million complaints and reported losses exceeding $20 billion, including approximately $17.7 billion attributed to cyber-enabled fraud. The Federal Trade Commission reported that military consumers lost $584 million to fraud in 2024. Those figures capture reported losses, but they do not reflect the many attempted thefts stopped by credit unions and other financial institutions before funds leave a member's account.

Credit unions are not passive recipients of fraud reports. They are frontline investigators, educators, and responders. Their member-owned, relationship-based model enables them to combine sophisticated technology with human judgment, often recognizing that a transaction may be technically authorized but induced through coercion, impersonation, or deception. Defense credit unions perform this work while also accounting for legitimate patterns that can look unusual to automated systems, such as overseas logins, frequent address changes, shared household devices, powers of attorney, and rapid movement between duty stations.

Credit unions deploy layered, real-time controls to prevent fraud before it occurs. These measures include multifactor and step-up authentication, device and behavioral analytics, transaction monitoring, card controls, velocity and geographic rules, check and remote-deposit screening, document verification, loan-application analytics, and alerts that allow members to confirm or deny suspicious activity. Fraud teams continually adjust detection thresholds as criminals change tactics. Many credit unions also give members the ability to lock a card, establish transaction alerts, restrict account access, and communicate through secure channels when an attempted transaction appears inconsistent with the member's normal activity.

Human intervention remains equally important. Frontline employees, call-center staff, lenders, and fraud specialists are trained to identify social engineering, account takeover, unusual cash withdrawals, new payees, high-risk wires, suspicious checks, forged documents, elder exploitation, and signs that a member is being coached by a criminal. Credit unions use call-back procedures, enhanced authentication, in-person conversations, trusted-contact protocols, and transaction holds or additional verification where permitted. A well-trained employee who pauses a coerced transfer or asks one additional question can preserve a veteran's retirement savings or a servicemember's monthly pay.

Credit unions also invest heavily in education and trusted outreach. Defense credit unions provide financial education workshops, one-on-one counseling, scam alerts, email and text warnings, branch signage, digital-security guidance, and frontline training through programs such as AARP BankSafe. They partner with installation leaders, the Department of Veterans Affairs, veterans service organizations, Adult Protective Services, law enforcement, and community groups to reach members before a scam succeeds. These efforts are tailored to the threats military-connected consumers actually encounter, including fake VA-benefit calls, romance and investment scams, technology-support fraud, housing and permanent-change-of-station scams, grandparent scams, recruitment fraud, phishing, spoofing, and AI-generated voice impersonation.

When fraud is detected, credit unions move quickly to contain the harm. They file suspicious activity reports, preserve records, contact payment networks and receiving institutions, seek recalls or freezes when possible, report criminal activity to law enforcement and the FBI's Internet Crime Complaint Center, and coordinate with Adult Protective Services in elder-exploitation cases. They also help members reset credentials, replace cards, secure compromised accounts, navigate disputes, address identity theft, correct credit-reporting problems, and restore safe access to financial services. This combination of prevention, intervention, reporting, and recovery is central to the credit union mission.

The credit union system continues to innovate. Launch Credit Union has used RembrandtAi to strengthen real-time check and card fraud detection, reporting that it prevented more than $3.5 million in losses in 2024. Affinity Federal Credit Union partnered with Point Predictive to enhance auto-loan fraud detection using advanced analytics, while Digital Federal Credit Union has used SnapLogic and AgentCreator to build AI-enabled fraud-detection infrastructure. These examples demonstrate how credit unions are adopting advanced tools while retaining human review and a member-first approach.

As the Committee evaluates fraud across America, DCUC respectfully urges Congress to reinforce - not displace - the institutions already protecting consumers and public funds. A credit union can identify a suspicious transfer, but it does not control a fraudulent advertisement on social media, a spoofed call carried over a telecommunications network, a compromised government portal, or a criminal's use of stolen identity data. Effective policy should target the full fraud ecosystem, align responsibility with control and conduct, and preserve the resources credit unions need to invest in cybersecurity, secure payments, member education, and fraud response.

First, Congress should establish stronger, two-way public-private fraud information sharing. Federal agencies should provide timely, actionable indicators about compromised identities, fraudulent benefit enrollments, mule accounts, synthetic identities, and rapidly evolving scam typologies. Credit unions, the National Credit Union Administration, law enforcement, payment networks, telecommunications providers, and online platforms should have clear, privacy-protective mechanisms and appropriate safe harbors to share relevant fraud intelligence before funds move.

Second, federal agencies should modernize identity proofing and payment-change controls for government programs. High-risk changes to direct-deposit instructions, contact information, credentials, or benefit recipients should trigger risk-based verification, out-of-band notice to the legitimate beneficiary, and rapid procedures to reverse or recall misdirected payments. These controls must be accessible to deployed servicemembers, military spouses, veterans, seniors, rural consumers, and people with thin credit files or nontraditional documentation.

Third, credit unions need reasonable flexibility to slow, verify, or temporarily hold a transaction when objective red flags indicate likely fraud, while maintaining appropriate notice, human review, and appeal rights. Faster payments should not mean irreversible losses. Congress and regulators should modernize outdated rules so institutions can introduce narrowly tailored friction at the moment it is most likely to protect a member.

Fourth, Congress should help smaller and community-based credit unions adopt advanced fraud tools. Grants, technical assistance, shared fraud utilities, secure information-sharing platforms, model governance resources, and clear supervisory expectations would enable smaller institutions to deploy identity verification, behavioral analytics, document screening, and AI-assisted detection responsibly without sacrificing member access or privacy.

Fifth, the federal government should build a coordinated fraud-prevention campaign for military and veteran communities. The Department of Defense, Department of Veterans Affairs, FTC, NCUA, Treasury, law enforcement, and defense credit unions should use installations, transition-assistance programs, VA facilities, veterans service organizations, military spouse networks, and trusted financial institutions to distribute practical and timely warnings.

Finally, Congress should avoid blanket liability shifts that make credit unions responsible for scams originating on platforms, networks, or government systems beyond their control. Consumer protection is strongest when every participant in the fraud chain has incentives to prevent harm, share information, and respond quickly. Policies that divert limited credit union resources away from fraud detection and cybersecurity may ultimately make members less safe.

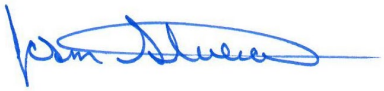
Suggested Policy Recommendations

1. **Include credit unions in government-wide anti-fraud coordination.** Any federal anti-fraud task force or strategy should include NCUA, credit unions, community financial institutions, and representatives serving military and veteran communities.
2. **Create a two-way, real-time fraud intelligence network.** Federal reporting and investigative systems should provide actionable alerts on compromised identities, mule accounts, synthetic identities, benefit redirection, and emerging scam typologies to trusted financial institutions.
3. **Expand safe-harbor protections for voluntary fraud information sharing.** Congress should enable privacy-protective sharing among financial institutions, agencies, law enforcement, payment networks, telecommunications providers, and digital platforms when the purpose is to prevent or recover fraud losses.
4. **Modernize federal identity proofing and account-change controls.** Agencies should use risk-based verification, out-of-band alerts, human review, and rapid recovery procedures for high-risk changes to benefits, direct deposit, contact information, and credentials.
5. **Permit narrowly tailored transaction delays and verification.** Credit unions should have reasonable authority to pause or verify suspicious checks, wires, electronic payments, and account changes when objective red flags indicate likely fraud, subject to notice and appeal safeguards.
6. **Improve rapid recall and fund-recovery mechanisms.** Payment systems and federal agencies should establish clear, 24/7 procedures for freezing, recalling, and tracing fraud proceeds before they are dispersed through mule accounts or converted to cryptocurrency.

7. **Fund technology adoption for smaller credit unions.** Grants, technical assistance, shared fraud utilities, and model governance resources can help community institutions deploy AI-assisted detection, document verification, device analytics, and secure reporting tools.
8. **Build a military and veteran fraud-prevention campaign.** DoD, VA, FTC, NCUA, Treasury, law enforcement, and defense credit unions should coordinate targeted outreach through installations, VA facilities, transition programs, veterans organizations, and military spouse networks.
9. **Align liability with control, conduct, and capacity to prevent harm.** Congress should avoid automatic liability shifts to credit unions for scams that originate on external platforms, telecommunications networks, online marketplaces, or compromised government systems.
10. **Measure prevention as well as losses.** Federal agencies should track attempted fraud stopped, recovery rates, time to action, false positives, false negatives, consumer burden, and the effectiveness of information-sharing programs.

DCUC appreciates the Committee's leadership and stands ready to assist Congress in developing a modern, coordinated fraud-prevention framework. Defense credit unions will continue to protect their members through technology, education, human intervention, and partnership, and they welcome the opportunity to help protect taxpayers, government programs, and the financial readiness of America's military and veteran communities.

Sincerely,



Jason Stverak
Chief Advocacy Officer
DCUC