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 13, 2026

The Honorable Pete Sessions
Chairman
Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

The Honorable Kweisi Mfume
Ranking Member
Subcommittee on Government Operations
Committee on Oversight and Government Reform
U.S. House of Representatives
Washington, DC 20515

Re: July 15, 2026 Hearing — "Emerging Fraud Threats and the Evolving Fraud Landscape"

Dear Chairman Sessions and Ranking Member Mfume:

On behalf of the Defense Credit Union Council, thank you for holding the Subcommittee's July 15, 2026 hearing, **"Emerging Fraud Threats and the Evolving Fraud Landscape."** DCUC appreciates the Subcommittee's attention to the rapidly changing fraud environment, the role of digital identity verification, and the need to protect taxpayers, consumers, and public programs from increasingly sophisticated criminal networks.

DCUC is the premier defense trade association representing credit unions serving military and veteran communities. Defense credit unions serve servicemembers, veterans, federal employees, retirees, and their families across the United States and around the world. Because these members often move frequently, deploy overseas, rely on remote access to financial services, and interact with federal benefit systems, they face unique exposure to identity theft, imposter scams, account takeover, payment fraud, and benefit-related fraud. DCUC has emphasized that defense credit unions are often the **first line of defense** when military families and veterans encounter suspicious transactions, elder exploitation, or scams targeting federal benefits.

The fraud threat is accelerating. The FBI reported that cyber-enabled crimes generated nearly **$21 billion** in reported losses in 2025, including more than **$17.7 billion** from cyber-enabled fraud complaints, and noted the growing use of artificial intelligence, fake social media profiles, voice cloning, fraudulent identification, and manipulated videos by scammers. The FTC reported that military consumers lost **$584 million** to fraud in 2024, and the FTC has warned that frequent relocation, new financial independence, and the pressures of military life can create vulnerabilities that scammers exploit. These losses are not merely financial. For servicemembers and their families, fraud can affect security clearance, deployment readiness, household stability, and trust in public institutions.

Defense credit unions are actively combating these threats through a combination of technology, member education, human intervention, and partnerships.

DCUC's recent comments to Congress have highlighted defense credit union efforts that include financial education workshops, one-on-one counseling, scam alerts, account alerts, transaction monitoring, frontline employee training to identify elder fraud red flags, and use of programs such as AARP BankSafe. Defense credit unions also work with law enforcement, Adult Protective Services, veterans service organizations, base leaders, and federal partners to help prevent losses before they occur.

Credit unions are also deploying advanced technology. DCUC has highlighted examples such as Launch Credit Union using RembrandtAi to help stop check and card fraud, Affinity Federal Credit Union partnering with Point Predictive to strengthen auto-loan fraud detection, and Digital Federal Credit Union using SnapLogic and AgentCreator to build AI-powered fraud infrastructure. DCUC has also emphasized that defense credit unions are expanding in-branch scam awareness and partnering with base commanders and VA offices to reach military-connected communities.

As the Subcommittee evaluates the evolving fraud landscape, DCUC respectfully urges Congress to adopt a balanced approach that strengthens fraud prevention without unintentionally weakening the credit unions that are already protecting consumers. Policy should target criminal actors, improve coordination, modernize outdated rules, and support responsible innovation. Congress should avoid broad liability shifts that would make credit unions financially responsible for scams originating on telecom networks, social media platforms, online marketplaces, or criminal imposter operations beyond the credit union's control. DCUC has cautioned that policies diverting credit union resources away from fraud detection, cybersecurity, and secure payments infrastructure could ultimately make consumers less safe.

DCUC encourages the Subcommittee to consider the following priorities:

First, Congress should strengthen public-private fraud information sharing. Credit unions, federal agencies, law enforcement, payment networks, telecommunications providers, and digital platforms need timely, actionable, and legally protected ways to share fraud indicators, mule-account patterns, synthetic identity signals, and scam typologies. The current information-sharing framework is often too narrow for modern scams, and expanded safe harbors should allow voluntary sharing of fraud information while preserving consumer privacy and data security.

Second, Congress should support interagency coordination to stop fraud before funds are lost. DCUC has supported the Taskforce for Recognizing and Averting Payment Scams Act, or TRAPS Act, because coordinated action among federal agencies, law enforcement, and financial institutions is critical when criminals move stolen funds quickly.

Third, Congress should modernize outdated payment and deposit rules to reflect real-time fraud risk. Credit unions need reasonable flexibility to slow or hold suspicious transactions when objective red flags indicate fraud, while maintaining appropriate consumer protections, notice, and appeal rights. Credit union testimony has specifically highlighted the need to modernize funds-availability rules and support "speed bumps" for high-risk transactions.

Fourth, Congress should help smaller and community-based financial institutions adopt advanced fraud tools. Not every credit union has the resources of a large financial institution. Technical assistance, grants, shared fraud utilities, and clear supervisory expectations can help smaller credit unions deploy artificial intelligence, identity verification, behavioral analytics, and secure reporting systems responsibly.

Fifth, federal digital identity policy must be risk-based, privacy-preserving, and accessible. Identity verification systems should reduce synthetic identity fraud and account takeover while protecting legitimate access for servicemembers, military spouses, veterans, seniors, rural residents, and consumers with thin credit files or nontraditional documentation. Federal agencies should measure false positives and false negatives, provide human review and appeal channels, and coordinate with trusted community institutions such as defense credit unions.

Finally, Congress should invest in targeted education for military and veteran communities. Fraud prevention works best when technology is paired with trusted messengers. Defense credit unions are ready to partner with Congress, the Department of Defense, the Department of Veterans Affairs, the FTC, NCUA, law enforcement, and veterans service organizations to deliver practical, timely fraud warnings to servicemembers, veterans, retirees, caregivers, and military families.

DCUC appreciates the Subcommittee's leadership on this issue. Defense credit unions stand ready to assist Congress in building a modern fraud-prevention framework that protects taxpayers, preserves access to financial services, and strengthens the financial readiness of America's military and veteran communities.

Sincerely,

Jason Stverak
Chief Advocacy Officer
DCUC

Suggested Policy Recommendations

1. **Include defense credit unions in federal anti-fraud coordination.** Any interagency fraud task force should include NCUA, credit unions, community financial institutions, and representatives serving military and veteran communities.
2. **Expand safe-harbor protections for voluntary fraud information sharing.** Congress should consider expanding information-sharing protections beyond money laundering and terrorist financing to include scams, synthetic identity fraud, account takeover, elder exploitation, mule accounts, and payment fraud. Credit union testimony has noted that current frameworks can be too limited for modern fraud typologies.
3. **Support TRAPS Act-style coordination.** DCUC has supported legislation focused on recognizing and averting payment scams, including stronger coordination among financial institutions, regulators, and law enforcement.
4. **Modernize funds-availability and payment rules.** Credit unions need reasonable authority to slow, hold, or verify suspicious transactions when fraud indicators are present, especially for check fraud, account takeover, elder exploitation, and high-risk electronic payments.
5. **Fund technology upgrades for small and community-based credit unions.** Congress could use grants, technical assistance, shared fraud utilities, or pilot programs to help smaller institutions deploy AI-based fraud detection, document verification, device-risk analytics, and secure information-sharing tools.
6. **Protect consumers without imposing blanket liability shifts.** Policies should focus liability on criminals and on the platforms or channels that enable fraud when appropriate, rather than automatically shifting losses to credit unions that did not originate or control the scam. DCUC has warned against approaches that could divert resources from fraud detection and cybersecurity.
7. **Build a military and veteran fraud-prevention campaign.** Congress should encourage VA, DoD, FTC, NCUA, and defense credit unions to coordinate targeted education on VA benefit scams, imposter scams, romance scams, deployment-related scams, elder exploitation, phishing, spoofing, and AI-enabled fraud.
8. **Require federal agencies to measure digital identity performance.** Agencies using digital identity tools should report fraud reduction, false rejection rates, demographic impacts, appeal outcomes, and safeguards for servicemembers, veterans, seniors, rural users, and consumers with thin credit files.
9. **Improve feedback loops from federal reporting systems.** Reports submitted to IC3, FTC Sentinel, FinCEN, and other systems should generate timely, actionable fraud typology alerts that can be shared with financial institutions and community partners.
10. **Preserve secure payments infrastructure.** Congress should avoid policies that weaken credit unions' ability to invest in fraud prevention, cybersecurity, secure card networks, and consumer support. DCUC has argued that interchange revenue helps support fraud prevention, cybersecurity, secure digital banking, and member services.

Suggested Questions for the Hearing

Questions for all witnesses

1. What are the fastest-growing fraud threats facing federal agencies and consumers today: synthetic identities, account takeover, check fraud, deepfakes, benefit redirection, elder exploitation, or payment scams?
2. How should Congress improve real-time fraud information sharing among federal agencies, law enforcement, credit unions, banks, telecom providers, payment networks, and online platforms?
3. What statutory safe harbors are needed so financial institutions can share fraud indicators quickly without creating unnecessary privacy, liability, or compliance risk?
4. How can federal agencies adopt stronger digital identity verification without excluding servicemembers, veterans, seniors, rural consumers, military spouses, deployed personnel, or consumers with thin credit histories?
5. What should Congress require agencies to measure when evaluating digital identity tools: fraud reduction, false positives, false negatives, demographic impact, appeal rates, or consumer burden?
6. How should agencies respond when AI-generated voice clones, fake IDs, manipulated videos, or deepfake documents are used to defeat identity verification?
7. Where are the biggest gaps between fraud detection and law-enforcement response, especially when funds move rapidly through multiple accounts or payment channels?
8. What role should community financial institutions, including defense credit unions, play in federal fraud-prevention strategies?

Questions for Jordan Burris, Socure

1. What digital identity verification methods are most effective against synthetic identity fraud and account takeover?
2. How can agencies combine document verification, device intelligence, behavioral analytics, and database checks while maintaining privacy and minimizing false denials?
3. How should federal identity systems account for military-specific circumstances, such as frequent relocation, APO/FPO addresses, overseas deployment, military spouse employment gaps, and nontraditional documentation?
4. What safeguards should Congress require to ensure digital identity tools are transparent, auditable, and appealable?
5. How can federal agencies distinguish between a legitimate high-risk user and a fraudulent identity without creating unnecessary friction for vulnerable populations?

Questions for David Maimon, SentiLink

1. What are the most common indicators of synthetic identity fraud, and how have those indicators changed with generative AI?
2. How quickly do fraud rings adapt when financial institutions or agencies deploy new controls?
3. What fraud signals could be safely shared with credit unions and other financial institutions to identify mule accounts, synthetic identities, and coordinated attacks earlier?
4. What are the best examples of public-private data sharing that materially reduce fraud losses?
5. How can Congress help ensure smaller financial institutions have access to the same high-quality fraud intelligence as larger institutions?

Questions for Marisol Cruz Cain, GAO

1. What recurring weaknesses has GAO identified in federal fraud-risk management, identity verification, and improper-payment prevention?
2. Should agencies be required to conduct fraud-risk assessments before launching or expanding major benefit, grant, loan, or payment programs?
3. What federal anti-fraud recommendations remain unimplemented, and which would produce the greatest near-term reduction in fraud losses?
4. How should Congress evaluate whether agencies are using digital identity tools effectively and fairly?
5. What governance model would best coordinate OMB, Treasury, GAO, FBI, FTC, FCC, NCUA, VA, DoD, SSA, and other agencies involved in fraud prevention?

Military- and veteran-focused questions

1. Military consumers reported hundreds of millions of dollars in fraud losses in 2024. What specific fraud typologies are most harmful to servicemembers, veterans, and their families?
2. How can VA, DoD, Treasury, FTC, NCUA, and defense credit unions better coordinate when veterans report benefit-redirection scams, pension fraud, account takeover, or identity theft?
3. Should federal fraud-prevention campaigns use defense credit unions, installation support offices, transition assistance programs, veterans service organizations, and military spouse networks as trusted distribution channels?
4. What additional protections are needed for deployed servicemembers whose accounts may be accessed remotely by family members, caregivers, or powers of attorney?
5. How can digital identity systems protect military families without penalizing frequent moves, overseas addresses, shared devices, or intermittent connectivity during deployment?