



**DCUC**  
DEFENSE CREDIT UNION COUNCIL

1627 Eye St, NW  
Suite 935  
Washington, DC 20006

202.734.5007  
www.d cuc.org

**Jason Stverak**  
Chief Advocacy Officer

**July 15, 2025**

The Honorable Andy Biggs  
Chairman, Subcommittee on Crime and Federal Government Surveillance  
House Judiciary Committee  
Washington, DC 20515

The Honorable Lucy McBath  
Ranking Member, Subcommittee on Crime and Federal Government Surveillance  
House Judiciary Committee  
Washington, DC 20515

**Re: “Artificial Intelligence and Criminal Exploitation: A New Era of Risk”**

Dear Chairman Biggs and Ranking Member McBath:

On behalf of the Defense Credit Union Council and our member institutions, I appreciate the Subcommittee’s focus on how emerging technologies like artificial intelligence (AI) enable new criminal schemes. DCUC represents over 200 credit unions serving more than 40 million members – notably including the men and women of America’s uniformed services, veterans, civilian defense employees, and their families. Many of our members operate on military bases and VA campuses, and they are acutely aware of how fraudsters exploit cutting-edge tools. We commend this hearing’s goal of curbing AI-facilitated fraud, and we welcome the opportunity to describe how defense credit unions are already responding with proactive measures and partnerships to protect their members.

**Advanced AI Fraud Detection:** Our credit unions have aggressively deployed AI-driven fraud prevention systems. For example, Launch Credit Union – serving a military community in Florida – integrated RembrandtAi’s real-time monitoring. Within the first year it “stopped check and card fraud in its tracks,” saving over \$3.5 million in 2024 alone. Likewise, Affinity Federal Credit Union recently partnered with an AI-powered risk platform (Point Predictive) to scan auto-loan applications. This “cutting-edge AI technology will...enhance our fraud detection capabilities” and streamline the lending process, according to Affinity’s risk operations team. Similarly, Digital Federal Credit Union (DCU) – another defense-focused credit union – is “leading the charge” with SnapLogic’s AgentCreator tool, using AI agents to build a modern, connected fraud-detection infrastructure. These examples illustrate that defense credit unions are not waiting for bad actors to strike: we are equipping ourselves with machine learning and real-time alert systems to flag anomalous behavior (sudden large transfers, frequent international transactions, etc.) and stop scams as they happen.

*Serving Those Who Serve Our Country*

**Member Education on AI Scams:** In parallel, our credit unions actively educate members about AI-enabled fraud. We maintain robust security centers and outreach campaigns. For instance, DCU’s website provides detailed guides on identifying AI scams – reminding members that scammers now use voice deepfakes, phishing bots, and more. As DCU advises, “AI scams will continue to change and evolve... one of the most important ways you can protect yourself is by staying informed with updates on emerging scams from trusted institutions like DCU”. Across our network, credit unions send fraud alerts by text and email, hold in-branch seminars on scam awareness, and publish online tutorials. Many of our branches are literally on base or VA grounds, so we can reach service members and veterans directly. In recent comments to Congress we stressed that credit unions operate ongoing “financial education efforts and member outreach programs” to keep military and veteran families informed about the latest fraud trends.

**Regulatory Collaboration and Advocacy:** Defense credit unions work closely with federal regulators and law enforcement to stay ahead of AI crime. We have encouraged agencies like NCUA and the FBI to share threat data with credit unions and to include credit unions in interagency task forces. In the policy arena, DCUC has strongly supported bipartisan measures such as the Taskforce for Recognizing and Averting Payment Scams (TRAPS) Act. That legislation – championed by Senators Crapo and Warner – would establish protocols for freezing suspicious transfers and improving coordination between financial institutions and law enforcement. As we recently stated in congressional testimony, the TRAPS Act “would empower financial institutions to freeze suspicious transfers and work more seamlessly with regulators and agencies to protect seniors and vulnerable consumers”. National credit union organizations (and DCUC in particular) also continue to urge Congress to modernize liability protections and data-sharing rules so that institutions can act decisively when fraud is detected, without fear of undue legal exposure.

**Examples of Credit Union Action:** To give concrete examples:

- *Launch CU (Florida):* Using AI-powered monitoring, Launch CU “saved \$3.5M+ in 2024 with real-time AI fraud detection,” according to a recent report. Their system flagged suspicious check and card transactions instantly, allowing staff to reverse or block fraudulent payments in real time.
- *Affinity FCU (NJ/NY):* Affinity reports that integrating AI into auto lending fraud screening “will enhance our fraud detection capabilities but also improve the efficiency...of our lending processes”. This means more scams caught at the point of loan origination, protecting both members and the credit union.
- *Digital FCU (DCU, Mass.):* DCU has publicly shared that it is “using SnapLogic and AgentCreator to power AI-driven fraud detection” and build a modern, connected infrastructure. In practice, this involves AI agents that continuously analyze transaction patterns and member behavior for anomalies.

**Defense Community Outreach:** An often-overlooked strength is that many of our fraud-fighting teams are veterans and military spouses. They “recognize when something feels ‘off’” and know how to talk to service members and retirees who may be hesitant to report a scam. This “veterans helping veterans” model means members trust their credit union and are more likely to heed warnings and seek help. In partnership with local base commands and VA offices, credit unions host financial-counseling events that cover emerging scam threats. For example, our members routinely brief units and veterans’ groups about phishing and impersonation schemes – now including those augmented by AI (deepfakes, etc.). In a recent DCUC letter we recommended federal support for outreach and education campaigns “targeted at older veterans and military families,” leveraging the trust we’ve built on installations.


**Willingness to Partner on Solutions:** DCUC stands ready to collaborate directly with this Committee and federal agencies to strengthen fraud defenses. In prior testimony we *offered* to pilot new anti-fraud initiatives in defense communities – including AI-based scam-detection pilots, real-time alert networks, and joint public messaging campaigns with federal partners. We also have offered expert testimony and data to congressional investigators, drawing on our daily experience confronting complex, cross-border scams. Defense credit unions are uniquely positioned to detect and disrupt these scams, and we are eager to partner with Congress on scalable solutions. Whether by sharing proprietary fraud-modeling insights, coordinating on rapid payment reversals, or standing up sector-wide tip lines, our community is prepared to help pioneer the national strategy against AI-enabled crime.

In summary, credit unions serving the defense and military community are already aggressively using AI tools, education, and partnerships to shield their members from AI-driven fraud. We believe these efforts should be recognized as a key line of defense and scaled nationally. We appreciate the Subcommittee's commitment to this issue and welcome any opportunity to provide additional information or work together to implement solutions.

Thank you for your consideration. We look forward to continuing to support the Subcommittee's important efforts to protect service members, veterans, and all Americans from AI-enhanced crime.

If you have any questions or would like to meet to discuss this issue in greater detail please email me at [jstverak@dcuc.org](mailto:jstverak@dcuc.org).

Sincerely,



Jason Stverak  
Chief Advocacy Officer  
DCUC

CC: Subcommittee on Crime and Federal Government Surveillance