OREGON

CREDIT UNIONS

House Interim Committee on Commerce and Consumer Protection
Hearing on Financial Scam Prevention
November 18, 2025

Background on Oregon Credit Unions

2.3 million Oregonians – 55% of the population – trust credit unions as their financial partners. Credit unions' not-for-profit, member-owned, cooperative structure inherently holds them accountable to the people and communities they serve. Across the state, credit unions look out for consumers' financial well-being by providing financial education, helping them to save for a brighter future, and making the loans that help them get the keys to their dream homes, help them open businesses on Main Street, and buy the autos that help them get to work and school.

Protecting Members

Protecting members' private information is critically important for credit unions and can pose strict legal, ethical, and regulatory requirements. Federal laws like the Gramm-Leach-Bliley Act (GLBA) and related regulations mandate that credit unions safeguard the confidentiality and security of members' nonpublic personal information, restrict unauthorized sharing with third parties, and provide members with annual privacy notices explaining how their information will be used and protected. But most importantly, respecting member privacy is foundational to maintaining trust between credit unions and their members.

- GLBA governs how institutions meet privacy standards and maintain transparent privacy policies, and FFIEC standards require financial institutions to protect customer information through risk management, secure storage and transmission, and clear communication with consumers.

  Credit unions undergo regular examinations by state and federal regulators to ensure safety, soundness, and compliance with these requirements. This oversight is more extensive than what applies to non-regulated service providers and other industries.

Credit union staff are required to undergo critical training programs to help them effectively prevent financial fraud and protect members. These trainings focus on awareness, detection, and compliance with industry regulations, helping staff recognize, prevent, and respond effectively to various fraud risks.

Sample of Common Required Training Topics

- Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Training: Staff must be trained on BSA/AML regulations to detect suspicious activities, perform proper due diligence, and follow reporting procedures for potential money laundering or terrorism financing activities.
- Fraud Prevention and Detection: Training covers the newest fraud tactics, red flags for suspicious activities, fraud policy compliance, and internal reporting channels. Front-line staff learn how to spot scams targeting members, such as identity theft, check fraud, elder financial exploitation, and account takeover schemes.
- Financial Exploitation and Elder Abuse Training: Specialized programs like AARP's BankSafe teach staff to identify and act on signs of member exploitation or financial abuse by third parties or trusted individuals, with emphasis on protecting vulnerable member populations.
- Internal Controls and Segregation of Duties: Credit unions emphasize training around implementing and following internal controls, including dual controls, role separation, account verification, timely reconciliations, and limiting access to accounts belonging to staff or their families.
- Regulation and Compliance: Staff receive training to stay compliant with Consumer Credit Protection laws, including the Fair Credit Reporting Act (FCRA), and to protect member information throughout daily operations.
- Role-Specific Red Flag Training: Staff in various roles (e.g., tellers, loan officers, member service reps) are trained to recognize specific indicators of fraud related to their duties, such as discrepancies in new account openings, unusual transaction patterns, or attempts to bypass account security.

Credit unions must implement technical, administrative, and physical safeguards to ensure the security and confidentiality of member information and prevent unauthorized access or use.

- Members have the right to opt out of certain kinds of information sharing, and credit unions are required to make these rights clear in their privacy notices.
- Credit unions must contractually require third-party service providers with access to member data to adhere to security and confidentiality standards.
- Respecting member privacy is foundational to maintaining trust between credit unions and their members. Mishandling data can result in legal consequences, reputational harm, and loss of member confidence.
- Credit unions prioritize investment in cybersecurity and privacy controls not just due to regulations, but also to protect members from fraud, data breaches, and identity theft.
- Privacy protection is not a one-time activity; it requires ongoing staff training, regular policy reviews, and continuous system updates to address new threats and regulatory changes.
- Credit unions are required to provide annual privacy notices to keep members informed and ensure transparency.

In summary, protecting member private information at credit unions is both a regulatory requirement and a core responsibility, essential for compliance, risk mitigation, and maintaining member trust.

Respectfully,
Pam Leavitt
Sr. Vice President of Regional Grassroots and Political Programs/Legislative Affairs for Oregon