ProSight

5 Fraud Prevention Tips

to Help Safeguard Your Credit Union

1 Synthetic Identity Theft

Synthetic Identity Theft is when cybercriminals combine real and fake personal info to create a new ID, building up “good customer” credibility over the long term in order to max out loans and lines of credit—before vanishing without a trace.

Prevention Tip: Employ cross-network analytics to create a 360° member view across different institutions, platforms, and merchants to detect conflicting bits of personal data and identify areas of compromise.

2 Check Fraud

Check Fraud is an exploding epidemic backed by foreign entities who create bogus paper checks that look like the real thing. (Even money orders and cashier’s checks aren’t immune.) Of course, these “checks” bounce once deposited since there are no funds backing them up.

Prevention Tip: While counterfeit checks may look professional, there are some telltale signs your members should watch out for—like flimsy paper stock, company misspellings, and suspicious routing numbers that can be revealed with an online search.

3 Shared Branch Fraud

Shared Branch Fraud happens when cybercriminals use a member’s stolen identity to gain access to their account or HELOC, then perform unauthorized withdrawals at an acquirer credit union in a shared branch network.

Prevention Tip: Work with acquirer credit unions in your shared network to bolster security tools and establish cash withdrawal limits, including blocking HELOC disbursement requests. Explain potential risks to members and offer an opt-in/opt-out policy for shared branching.

4 Call Center Fraud

Call Center Fraud is on the uptick as cybercriminals use their arsenal of stolen personal details to bypass voice recognition systems and screening questions to reset PINs and test accounts—which is proving especially successful in today’s climate of quick call center resolution.

Prevention Tip: Institute authentication procedures that combine automated and knowledge-based verification, like requesting the phone number of record, following up with a mobile code, and asking an additional security question.

5 Account Takeover

Account Takeover (ATO) occurs when a cyberthief gains access to a member’s credit union account (usually through a data breach, phishing scam, or malware attack) and takes over that account online, using it as their own personal piggybank.

Prevention Tip: Put a proactive plan in place that detects unusual activity, like thousands of accounts being created from one IP address or multiple account access attempts in a short period of time. Also, employ multi-factor account authentication for members.