TruStage™

Member authentication & verification

Risk overview

Member authentication tools and tactics have evolved over time. But fraudsters continue to successfully impersonate members to carry out fraudulent transactions.

The online channel has become a valuable tool for credit unions in providing member convenience – like account opening, loan applications, and other banking transactions. However, this also provides fraudsters with another channel and one with more obscurity challenging organizations in properly authenticating and verifying members and potential members.

Member authentication used to be much easier, when your members and potential members walked through the office doors.

Data breaches have fueled the problem since they often lead to identity theft. The uptick in Social Security number compromises, in addition to other personally identifiable information – names, addresses, and birth dates - from these breaches compounds the problem.

The stolen personal information has significantly increased the number of identity theft-related fraud losses reported. Fraudsters are opening fraudulent accounts and applying for loans – more than ever.

The online channel provides a cloak of anonymity; however, fraudsters also continue to visit branch offices, making it critical for staff to be alert and cautious when opening accounts and processing loan applications.

Common ID theft-related fraud losses

- New account fraud
- Loan fraud
- Call center fraud
- Account takeovers

Key Mitigation Tip

The **Fair and Accurate Credit Transactions Act (FACT Act)** requires credit unions to adopt a written Identity Theft Prevention Program to detect, prevent and mitigate identity theft in connection with the opening of a covered account or existing covered accounts. Ensure your program is up-to-date to reflect today's identity theft fraud environment and staff in key positions are adequately trained.

Common identity theft-related fraud losses

New account fraud

New account fraud losses are increasing through the online channel. Fraudsters who open accounts at credit unions typically use stolen identities. In addition, these fraudsters make fraudulent deposits of checks or ACH debits and withdraw the funds before the items are returned unpaid to the credit union.

When opening new accounts, whether online or in person, credit unions should emphasize the importance of member identification. Avoid placing too much reliance on government-issued photo IDs since they are easily counterfeited. Consider the use of an identity verification solution to verify the membership applicants' identity - especially with potentially high-risk accounts. Many credit unions have experienced success in preventing fraudulent accounts from being opened by using a skip tracing solution to screen high-risk accounts.

Loan fraud

Losses stemming from identity theft-related loan fraud tend to be more severe in dollar amount than the losses associated with new account fraud. Once a fraudster opens an account, usually through the online channel, they immediately apply for loans, including unsecured loans, credit cards, and vehicle loans. These losses are increasing as more credit unions accept loan applications through the online channel.

Loan staff who process loan applications should be trained on how to spot fraudulent applications. They should scrutinize credit reports to identify red flags that could signal possible identity theft.

Call center fraud

Fraudsters frequently target the call center and often request changes to members' contact information (e.g., phone number, email address, etc.) which typically leads to other forms of fraud, such as requesting wire transfers through the call center.

To mitigate the risk, credit unions should deploy an identity verification solution that relies on strong out-of-wallet questions, or an out-of-band authentication method for authenticating members. Phone printing is gaining popularity as one call center fraud solution. Phone printing serves the same function for phone calls as device printing does for online banking interactions.

Account takeovers & online banking

Fraudsters use stolen identities to impersonate members by enrolling member accounts for online banking.

Once enrolled, they change the member's contact info through online banking. Then, once logged into the account, fraudsters take advances against member line-of-credit loans, such as HELOCs; request wire transfers; use bill pay or the external transfer service to transfer funds out of the member's account; use the external transfer service to initiate ACH debits to pull funds from external accounts for deposit to the member's account and then transfer the funds out of the member's account before the ACH debit entries are returned; or view canceled checks, including HELOC checks, to manufacture counterfeit checks.

Deploy a strong authentication method for online banking enrollment

- Deploy an identity verification solution that relies on strong out-of-wallet questions.
- Examples of strong out-of-wallet questions include:
    - What year did you open your account?
    - Who is the payable on death beneficiary on your account?
    - What is the last loan you paid off with us, approximate date and collateral used?
- Some online banking vendors offer an out-of-band authentication method using one-time-passcodes (OTPs) to authenticate members using the online banking self-enrollment feature. When a member attempts to enroll for online banking, the system generates an OTP and the member is given options for receiving the OTP - by phone, email or SMS text message. The member must enter the OTP to complete the enrollment.
- Transmitting OTPs via email is best to be avoided due to email's inherent risks (i.e., email accounts can be hacked). In addition, transmitting OTPs via SMS text message can be defeated if a member's mobile phone is fraudulently ported to a new carrier. Credit unions should assess these risks when considering this out-of-band authentication method.
- Use geolocation tracking of the IP address used to enroll the account for online banking to determine if it is consistent with the member's address.
- Confirm online banking enrollments by sending a letter to members, provided the address has not been changed in the last 60 days.
- Be alert for changes to a member's contact information that occur immediately following the account being enrolled for online banking.

Looking for additional insights?

If you'd like to discuss in more detail, simply schedule a no-cost 1:1 discussion with a TruStage™ Risk Consultant by contacting us at **800.637.2676** or at **riskconsultant@trustage.com**.