Online Account Opening & Funding
Risk Overview

Deposit Account Services

Offering online account opening and funding provides for a fast and convenient method for opening accounts. However, this convenience feature also exposes credit unions to a number of risks. Credit unions should conduct a risk assessment prior to introducing this service to identify the risks so that important loss controls can be implemented to help manage loss exposures

The Risks of Convenience

The online channel has quickly become the most important tool available to credit unions for opening new accounts. Online account opening and funding has become popular as credit unions seek to streamline the new account process by looking for more efficient and convenient ways to open and fund new accounts. This service not only allows individuals to open accounts online via the credit union's website, but it also allows the individuals to fund the accounts.

The online channel provides fraudsters with yet another avenue to commit fraud against credit unions while concealing their true identity. Fraudsters often use consumers' personally identifiable information (PII) that is compromised in data breaches to open fraudulent accounts at credit unions. Although fraudsters may open fraudulent accounts in-person, they prefer to use the online channel as it provides a cloak of anonymity.

At a Glance

- **Verifying the Identity of New Members**
  Understand how to verify member identity and enforce proper controls to minimize account opening fraud
- **Account Funding Methods**
  Learn about the different account funding methods - ACH, payment card, check and their associated loss controls
- **Automated Approval**
  Be cautious when using the online account opening and funding solution's automated approval feature as fraudulent accounts could be mistakenly approved

Read on to learn more about fraud risks and controls related to online account opening and funding.

There are two primary fraud risks in offering online account opening and funding:

A fraudster could open the account under someone else's identity with the intent to commit fraud, such as fraudulently obtain a loan, or

A fraudster could use a fraudulent method of funding the account, such as a fraudulent ACH deposit, and withdraw the funds before the item is returned unpaid.

Verifying the Identity of New Members

New Member Identification Tips

Verifying member identities through consistent controls can help minimize fraudulent account opening. While many vendors' online account opening and funding solutions include an identity verification product, they often rely on questions derived from credit reports which the fraudster likely has in hand. Credit unions should ensure that the identity verification product accompanying a vendor's online account opening and funding solution rely on strong out-of-wallet questions.

Some credit unions require membership applicants to upload a copy of their government-issued photo ID, such as a driver's license or state ID card, as an additional step in verifying their identity when opening accounts online. Credit unions should avoid relying on driver's licenses and state ID cards as a means of verifying the identities of individuals since they are easily counterfeited.

Be alert for mismatched addresses, since this has traditionally been **among the top red flags** presented in fraudulent online account opening.

Among other verifications performed, identity verification products verify the membership applicant's address. This is typically accomplished by comparing the membership applicant's address against multiple databases. Mismatched addresses signal the possible existence of identity theft.

Avoid asking for a driver's license or utility bill to resolve mismatched addresses. These documents are easily counterfeited. Instead, consider resolving mismatched addresses by using a robust identity verification service, such as a skip trace solution.

Identifying High-Risk Applications

When a high-risk application is identified, consider screening the membership applicant using a robust identity verification product. Some credit unions have successfully prevented fraudulent accounts from being opened online by screening high-risk applications using a skip tracing solution.

Interested in learning more about Deposit Account Services and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Online Account Opening & Funding Risks

The methods of funding accounts opened using the online account opening and funding feature generally includes checks, ACH and payments cards (e.g., credit and debit cards). There are risks associated with each funding method.

Account Funding Methods

Funding by ACH: Funding new accounts by ACH can be pretty risky. Funding an account by ACH debit involves pulling funds from an account at another financial institution for deposit to the newly opened account. The ACH debit can be returned as NSF, account closed, account not found, or as unauthorized. It's the unauthorized ACH debit that creates the most risk since Receiving Depository Financial Institutions (RDFIs) have up to 60 days to return debits their consumer accountholders claim as unauthorized.

Trial deposits are often used when originating ACH debits against accounts at RDFIs to verify the membership applicants are authorized to conduct transactions on the funding accounts. This involves initiating small dollar deposits (usually less than $1) against the funding account and the membership applicant is required to confirm the transaction with the credit union. However, trial deposits are not foolproof since the membership applicant could have unauthorized access to the funding account allowing him or her to confirm the trial deposits with the credit union.

LOSS CONTROLS

Implement a monetary limit for funding new accounts via ACH, such as $2,500 or an amount based on your risk tolerance. In addition, consider CUNA Mutual Group's optional coverage, the Fraudulent Deposit-Enhanced Endorsement, to protect against fraudulent deposits made via ACH.

Funding by Payment Card: Some credit unions allow membership applicants to fund the account with a payment card (credit or debit). Funding accounts with a payment card places the credit union in the role of an online merchant. CUNA Mutual Group's Plastic Card Policy protects you as issuers of cards – not as merchants accepting cards for payment. Any loss from funding an account with a payment card would be uninsurable.

LOSS CONTROLS

To mitigate the risk of large uninsurable losses, adopt a low funding limit for plastic cards, such as $2,500 or an amount based on your risk tolerance.

Funding by Check: Individuals opening accounts through the online channel can fund the accounts the old-fashioned way – by mailing a check to the credit union. This exposes credit unions to check fraud losses.

LOSS CONTROLS

Minimizing risk with funding by checks is pretty easy – use extended check holds. Regulation CC allows extended holds on checks deposited to new checking accounts during the first 30 days of account opening.

Interested in learning more about Deposit Account Services and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

Automated Approval Feature

Many online account opening and funding solutions offer an automated account approval feature allowing membership applications that meet certain criteria to be automatically approved. Be cautious when using the automated approval feature as fraudulent accounts could be mistakenly approved.

If you opt to use the automated approval feature, establish parameters or rules for approving accounts. Consider implementing rules such as:

- Disabling the automated approval feature over weekends. These applications should be manually reviewed.
- Require a manual review of applications submitted by individuals who live outside of the credit union's normal trade area.
- Require a manual review of applications from individuals who qualify for membership by joining a nonprofit organization that is within the credit union's field of membership.
- IP addresses should be checked to determine if the IP address used to open the account is consistent with the membership applicant's physical address and whether the IP address was previously used to open an account.
- Block IP addresses if fraud is suspected. Understand, however, that fraudsters can quickly switch to other IP addresses.

It should be noted that some automated approval features may no allow you to establish rules. Evaluate the risk in deciding to use the automated tool feature prior to implementing.

Compliance Regulations and Considerations

There are a number of compliance issues to consider when opening accounts online through the your website, including the Customer Identification Program rules under the USA Patriot Act, the Identity Theft Red Flag Rules under the Fair and Accurate Credit Transactions Act (FACT Act) and the Electronic Signatures in Global and National Commerce Act (E-Sign Act) for the delivery of electronic disclosures.

Customer Identification Program Rules

The Customer Identification Program (CIP) rules of the USA Patriot Act require credit unions to verify the identity of new members. CIP provides for verifying the identity of new members through documentary or nondocumentary methods. Documentary methods of verifying an identity generally include the use of unexpired government issued photo ID. However, credit unions are not in a position to physically inspect the government issued photo ID of new members who open accounts online. Therefore, the use of a nondocumentary method should be used when accounts are opened online. A nondocumentary method of verifying a new member's identity includes the use of a third party identity verification service. Another option is obtaining a credit report and comparing the personal information provided by the new member to the personal information contained in the credit report.

Fair and Accurate Credit Transactions Act

Verifying the identity of new members is also addressed in the Identity Theft Red Flag Rules under the Fair and Accurate Credit Transactions Act (FACT Act). Section 114 of the FACT Act requires credit unions to develop and implement a written Identity Theft Prevention Program (Program) to detect, prevent and mitigate identity theft when opening a covered account and on existing covered accounts. In summary, Section 114 requires credit unions to include in their Program policies and procedures that enable credit unions to:

- Identify relevant patterns, practices, and specific forms of activity that are “red flags” signaling possible identity theft and incorporate those red flags into the Program,
- Detecting red flags identified as relevant in connection with opening a covered account and existing covered accounts,
- Responding appropriately to any red flags that are detected to prevent and mitigate identity theft, and
- Updating the Program periodically to reflect changes in risks from identity theft.

When using an identity verification service or a credit report to verify the identity of new members who open accounts online, credit unions should be alert for the following red flags indicating possible identity theft:

- Notice of address discrepancy or mismatched address
- A Social Security Number or birth date provided by the new member that does not match the corresponding data
- Notice that the Social Security Number appears in the Social Security Administration’s Master Death File
- A Social Security Number was issued before the date of birth provided by the new member
- A fraud or active duty alert
- Notice that the new member had accounts closed at other institutions due to abuse
- An address provided by the new member that is reported as a known fraud address or is a commercial or institutional address

Credit unions should ensure the appropriate staff receives training on the types of red flags that signal the possibility of an identity thief attempting to open an account online. Additionally, credit unions should ensure that the procedures for resolving any red flags detected are adequate to reduce the risk of identity theft.

E-Sign Act and Electronic Disclosures

Opening accounts online necessitates the use of electronic signatures and the delivery of electronic disclosures. Certain disclosures, such as the funds availability disclosure for transaction accounts under Regulation CC and the Truth-in-Savings disclosure under Part 707 of the NCUA Rules must be provided at or before account opening. Therefore, credit unions must comply with the Electronic Signatures in Global and National Commerce Act (E-Sign Act).

Visit the Protection Resource @ cunamutual.com

Interested in learning more about Deposit Account Services and related risks?

Contact CUNA Mutual Group Risk Consultants at 800.637.2676 or riskconsultant@cunamutual.com

E-Sign Act and Electronic Disclosures Continued

The first step towards compliance is to obtain the membership applicant's electronic affirmative consent to the required E-Sign Act disclosure. The disclosure must include the following:

- The option to have the record provided on paper;
- The right to withdraw consent to receive electronic records and any conditions, consequences, or fees in the event consent is withdrawn;
- The scope of the consent (e.g., all disclosures, periodic statements and notices; or disclosures and notices only);
- The procedures members must follow to withdraw consent;
- The procedures members must follow to provide updated contact information (i.e., email address);
- How members may obtain a paper copy of the electronic record and any related fee; and
- Hardware and software requirements to access and retain the electronic records

The membership applicants' consent to the required disclosure must reasonably demonstrate they can access the electronic record in the format used (e.g., Adobe PDF). The reasonable demonstration requirement is the most difficult compliance step and is often overlooked. It is not sufficient to disclose to membership applicants that they need, for example, Adobe Reader to access the electronic disclosures.

One method to comply with the "reasonable demonstration" requirement is to insert the required E-Sign Act disclosure in a sample Adobe PDF document along with an "I agree" button. Members must open the document and click on the "I agree" button to the disclosure. Another option is to place a "code" in the E-Sign disclosure contained in the sample Adobe PDF document. Members would have to open the PDF to retrieve the code and enter it on the HTML web page. The credit union should track members who consent to the disclosure under either method.

Insightful knowledge, experience, and resources when you need it most.

Contact CUNA Mutual Group's **Risk & Protection Response Center**
at **800.637.2676** or by email at riskconsultant@cunamutual.com for additional insights.