

RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.



Alert Type

Awareness

Watch

Warning

Check Holds Not Used As Fraudsters Take Off With 6-Figure Amounts

Fraudulent deposit losses associated with new account scams are increasing at an alarming rate with individual losses reaching 6-figures. Unfortunately, in most cases, check holds were not imposed, and the fraudsters were able to withdraw the funds immediately at another branch location or through an ATM.

Details

Fraudulent deposit losses associated with new account scams are increasing at an alarming rate. Fraudsters either opened the new account with a fraudulent check or waited up to six months before depositing a fraudulent check. Savvy financial criminals frequently wait more than 30 days before making a fraudulent deposit, or they will make small deposits and withdrawals in the first month to establish a pattern. The fraudulent checks have ranged from \$1000 up to \$87,000.

Unfortunately, in most cases, check holds were not imposed, and the fraudsters were able to withdraw the funds immediately at another branch location, shared branch location, or through an ATM.

In some scenarios, the fraudsters that opened a new account with good money also opened an IRA account with a fraudulent check. The fraudulent IRA rollover checks, typically mailed to the credit union, ranged from \$50,000 to \$147,000. The fraudsters frequently withdrew the funds on the same day – again through various means.

Credit unions should be cautious when new members request to open an IRA account, particularly when the IRA rollover check is received by the credit union via overnight mail. Additionally, you should avoid allowing withdrawals from newly-opened IRAs.

Since Regulation CC (Reg CC) does not apply to IRA accounts, credit unions are authorized to place extended holds on checks deposited to newly-opened IRA accounts.

Risk Mitigation

Credit unions should consider these loss controls:

When opening new accounts in person or by mail:

- Screen new members using an identity verification solution
- Flag new accounts for at least six months to alert tellers and front-line staff to the new account status
- Impose extended check holds in accordance with Regulation CC (Reg CC) on deposits made to new accounts

Date: October 13, 2020

Risk Category: Scams, Fraud; Reg CC, Fraudulent Deposits, New Account Fraud; IRA

States: All

Share with:

- Branch Operations
- Executive Management
- Front-Line Staff / Tellers
- Member Services / New Accounts
- Risk Manager
- Transaction Services



Your feedback matters!
Was this RISK Alert helpful?



Check Holds Not Used As Fraudsters Take Off With 6-Figure Amounts

Risk Mitigation

As more accounts are established through digital channels, credit unions need a reliable and accurate method to verify that an applicant not only provides authentic information, but that he or she is who they say they are.

If you offer online account opening and funding, consider

- Use an identity verification solution that relies on strong out-of-wallet questions to screen new members.
- Be alert for multiple credit inquiries in a relatively short period of time when examining new membership applicants' credit reports.
- Disable automatic approvals over weekends. These applications should require a manual review.
- Require a manual review of applications from individuals qualifying for membership by joining an association within the field of membership or who live outside of the credit union's normal trade area.
- Scrutinize IP addresses, including:
 - Geolocation tracking of IP addresses to ensure they are consistent with the individual's address.
 - Be alert for multiple applications received from the same IP address.
 - Block IP addresses if fraud is suspected. Note that fraudsters may quickly switch to different IP addresses after the block is in place. If you or your member think they are part of a money mule scam, stop transferring money. Then, report it to the FTC at www.ftc.gov/complaint.
- Screen suspicious applications identified through a robust identity verification service. Some credit unions have experienced success in blocking fraudulent membership applications by screening suspicious applications through a skip trace service.
- Refrain from opening accounts if you are unable to verify the identity of new membership applicants. Send an adverse action notice explaining the reason(s) for denying the account.
- If members can fund the account online (e.g., by ACH or payment card), ensure the monetary limits are reasonable.
- Use extended holds in accordance with Reg CC on check deposits made to accounts opened online through your website.

Risk Prevention Resources

Access CUNA Mutual Group's [Protection Resource Center](https://www.cunamutual.com/protection-resource-center) at [cunamutual.com](https://www.cunamutual.com) for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- [Online Account Opening & Funding Risk Overview](#)
- [Reg CC Availability Guide](#)
- [Accepting Checks for Deposit](#)



Access the Protection Resource Center for exclusive resources:

- [Loss Prevention Library](#) for resources & checklists
- [Webinars and Education](#)
- [RISK Alerts Library](#)
- [Report a RISK Alert](#)

The Protection Resource Center requires a User ID and Password.

Facing risk challenges?

[Schedule](#) a free personalized discussion with a Risk Consultant to learn more about managing risk.

© CUNA Mutual Group, 2020.

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.