

Recruitment Scam Hits Credit Unions

April 21, 2010

Summary

Fraud rings around the country are recruiting individuals for a fee to open new accounts at credit unions with the intent to commit fraud. Existing members are also recruited to sell their financial information.

State(s): All

Type of Alert: Recruitment Scam

[Risk Mitigation Recommendations](#)

CUNA Mutual alerts credit unions of this risk. Please pass this information on to all appropriate employees. If your credit union has experienced a loss, contact our Credit Union Protection Response Center at 800.637.2676.

Details:

Credit unions across the country continue to report cases of fraud where individuals are recruited and paid by fraud rings to open accounts at credit unions. This particular recruitment scam is primarily focused on the recruits obtaining a card and PIN after the account is opened, which is turned over to the fraud ring. Existing credit union members are also recruited and paid by the fraud rings for allowing the rings to use the members' cards and PINs, or check information, for transactions that the members later claim as unauthorized. Credit unions are encouraged to take extra measures when a member reports unauthorized activity on their account. Credit unions should pay special attention to new account openings, changes on existing accounts, and members reporting unauthorized activity on cards, checks, or ACH transactions. To help determine if your member participated in the scam, you may consider creating a member challenge program which should include action steps such as requesting them to file a police report and be willing to press charges and obtaining a notarized document stating they did not participate in the fraud.

RISK Scenarios:

Recruitment fraud targets individuals willing to open accounts at credit unions. After the account is opened, the individual applies for a card and PIN or a share draft account. The card and PIN or share draft account information is subsequently used for fraudulent purposes. Fraud rings are also recruiting existing credit union members willing to sell their personal or financial

information. The members subsequently claim the transactions were unauthorized.

This recruitment scam differs from recruiting members through work at home or job scams referred to as the money mule scam. For information on this scam, reference the RISK Alert titled New Money Moving Scam Uses Members' Personal CU Accounts – issued May 28, 2009.

RISK Mitigation Recommendations:

- Alert members to the recruiting scam using your website, statement stuffers, or newsletters and advise them to report attempts to recruit them to the credit union and law enforcement.
- Credit unions should use an identity verification service to confirm the identity of new members.
- Consider implementing a waiting period before new members are eligible to receive a card and PIN.
- If you opt to create a member challenge program, request members to report the incident to the police and press charges along with completing a notarized letter stating they did not participate in the fraud.
- Request and review photographs or film from merchants and/or ATM operators where the fraudulent transactions occurred.
- Report all cases of fraud where you suspect your members are involved to law enforcement.
- Pay special attention to account updates/changes involving card requests, unauthorized checks or ACH clearing items.