RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type Awareness | **Watch** | Warning

Remain Vigilant of Tax Refund Fraud

The Internal Revenue Service (IRS) reported a decrease in ID theft-related tax refund fraud through the first nine months of 2016 stopping 787,000 confirmed ID theft tax returns totaling more than $4 billion. Credit unions should remain vigilant as you are in prime position to identify tax refund fraud impacting your organization and your members based on the methods for issuing refunds – via ACH credit or check.

Details

ID theft-related tax refund fraud involves fraudulently filing tax returns under another person's name and Social Security number. Each year, credit unions and credit union members report these schemes impacting them even though the IRS has made significant progress in combating this type of fraud.

Despite the encouraging trend, credit unions should not become complacent as taxpayer identities continue to be stolen in a number of ways including through data breaches and phishing scams. Since you are on the receiving end of the transaction – refunds via ACH credit or check – you can help combat this fraud by watching for these red flags:

- Multiple tax refunds deposited to a member's account
- Incoming tax refunds via ACH credit where the name does not match the account number
- Suspicious presentment of refund checks (e.g., double-endorsed checks), or a large number of refund checks deposited to a business member's (e.g., a check cashing business) account

With many tax refund fraud cases involving ACH (direct deposit), you should also be familiar with the rules and guidance on ACH transactions, particularly:

- Credit unions are allowed to post incoming ACH tax refunds only using the account number (there is no requirement to match the name on the account)
- If you become aware of an ACH tax refund being misdirected to the wrong account, you are required to notify the government, which can be accomplished by returning the ACH entry using the return reason code, R03 (No Account/Unable to Locate Account)

Date: January 24, 2017

Risk Category: Fraud, Funds Transfer / ACH, Scams, Compliance

States: All

Share with:

- ☐ Risk Manager
- ☐ Operations Team
- ☐ Compliance Team
- ☐ Accounting Staff
- ☐ Executive Management

To share risk insights or gain additional assistance:

- Report a RISK Alert
- Contact the **Risk & Protection Resource Center**
  - o 800.637.2676
  - o riskconsultant@cunamutual.com

Risk Mitigation

Credit unions should consider these mitigation tips:

- Understand your obligations related to tax refund ACH credits where the name does not match the account number. It is recommended you return these transactions using the R03 return reason code.
- Do not look for a different account to post the credit, even if the name might be associated with another account number, or it appears to be an error. Your credit union assumes liability for any problems by not posting to the account number in the ACH entry. It is recommended you return the credit using the R03 return reason code.
- Be careful responding to member inquiries about their refund going into another member's account due to an error in the account number:
  - Do not provide information on the other member's account.
  - If the funds are available in the other member's account and you are aware of a mismatch, return the credit using the R03 return reason code.
  - Do not move the funds between the accounts.
  - Refer your member to the IRS to ask about the status of their refund.
- Return ACH credit refunds to closed accounts using the R02 return reason code, Account Closed. Do not post it to another active account.
- Contact your Regional Payments Association with questions on how to handle ACH transactions or returns.
- Complete the required Suspicious Activity Report (SAR) if you know or suspect potential tax refund fraud.

Risk Prevention Resources

Access CUNA Mutual Group's Protection Resource Center at cunamutual.com for exclusive Risk Management resources to assist with your loss control needs. The Protection Resource Center requires a User ID and password.

Additional resources that you may find helpful include:

- Direct Deposit of IRS Tax Refunds Resource Page (Bureau of the Fiscal Service)
- A Guide to Federal Government ACH Payments (Green Book), Chapter 2
- FinCEN Advisory (FIN-2013-A001) for a more comprehensive list of red flags

Contact **CUNA Mutual Group Risk and Compliance Solutions** at **800.637.2676,** via riskconsultant@cunamutual.com, or use Ask a Risk Manager for additional risk insights and to learn how we can assist your credit union.

Access exclusive resources within the Protection Resource Center:

- Loss Prevention Library for white papers & checklists
- Webinars and Education
- RISK Alerts Library

Check out other Risk & Compliance Solutions areas of practice to help you manage your most pressing risks.