Northwest Credit Union Association
Idaho • Oregon • Washington

Fraud Alert

Fraudulent SBA Disaster Relief Payments

The following alert was shared by the Illinois Credit Union League, and based on a Secret Service alert.

Several credit unions have reported members receiving ACH deposits representing SBA disaster relief payments to inactive or non-business accounts. The payments are labeled “SBAD TREAS 310” – which commonly denotes SBA Economic Injury Disaster Loan (EIDL), and may have the company ID of 9101036151. Some payment amounts exceed $10,000.

While details of the scam are limited, credit unions have described an advance fee scheme.That is, fraudsters are recruiting your members to receive EIDL payments via ACH. The member is instructed to keep a certain amount of the payment and send the remaining to the person who is directing the activity.

If you’ve experienced SBA fraud, please report it to Special Agent Brett Lehnert with the Small Business Administration – Office of Inspector General at brett.lehnert@sba.gov

ACH Guidelines:

- If the credit union returns an ACH credit you believe is fraudulent, use Return Reason Code R23 (Credit Entry Refused by Receiver) or R03 for a name mismatch or R17 for an invalid account number initiated under questionable circumstances. The use of R17 requires “Questionable” to be inserted in the first twelve positions of the addenda record.
- Under NACHA Operating Rules, the credit union is not liable for funds resulting from fraudulent ACH credit entries if the funds are no longer available in the member’s account. NACHA Rules provide the ODFI warrants to the RDFI that the entry is correct and properly authorized. If the RDFI posts a fraudulent credit to the account number in the entry, and the funds are withdrawn, the RDFI is not liable for the funds.

- The credit union cannot return partial funds. The NACHA Operating Rules require return entries to contain the same dollar value as the original entry. A partial return of funds must be handled outside the ACH network (e.g., with a wire transfer or official check), or with a new credit entry agreed to by both institutions.
- If you receive a warrant from the Secret Service or other law enforcement agency requesting a return of fraudulent funds, you should only return whatever is left in the account.

Risk Prevention Tips:

- Manually review incoming ACH credit entries to identify suspicious records.
- Be aware of members that withdraw the entirety of funds received from the ACH deposit
- Many members may have rightfully applied for SBA relief loans, Verify the legitimacy of the member's business prior to returning or releasing potentially fraudulent funds.
- Close their account and/or file a suspicious activity report, as necessary.
- Contact Special Agent Brett Lehnert at the email address provided above.

The Takeaway? As we face a world trying to recover from a pandemic – scammers are out in force taking advantage of the most vulnerable. We need to remain on guard and urge our members to do the same.

If you have questions about this communication, contact the NWCUA's compliance team at 800.546.4465, or compliance@nwcua.org.