

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

ACH Debit Payments (Credit Card and HELOC) SUMMARY

We are seeing a spike in losses when credit card and home equity lines of credit (HELOC) payments are made using ACH. Since the Receiving Depository Financial Institution (RDFI) has up to 60 days on consumer ACH payments to return the funds, there is significant time for this fraud to be executed. Losses can far exceed the approved credit limit. In one instance the loss was over 20 times the approved line of credit on the loan. In addition, risk increases if members can make credit card payments online through their vendors payment system. The lack of controls could result in much higher losses when the RDFI returns these ACH consumer payments back to you as the ODFI as unauthorized, NSF or closed account.



HOW THE ATTACKS ARE PLOTTED

- A bad actor or a member utilizes the available credit on card or line of credit, typically approaching their approved limit.
- A payment is made, and credit availability is immediately restored.
- The cycle is repeated several times.
- Eventually ACH payments are returned by the RDFI typically as fraud, insufficient funds, or closed account.
- The balance due will now include the amount of all returned ACH payments.
- The loss in most cases exceeds the line of credit approved once all returned payments are applied against the member's line of credit account.

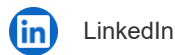
RISK MITIGATION STEPS

- Delay restoring a member's credit line after an ACH payment has been made to revolving credit. Regulation Z only requires you to credit the payment as of the date received, it does not require you to make credit available concurrently, as long as it doesn't cause over-the-limit fees or charges.
- Understand the risks associated with accepting ACH payments (ODFI warrants risk for ACH credits and debits initiated by you as the ODFI).
- Consider limiting ACH payments to one ACH payment per month.
- Limit ACH payments to the lower of the balance due or the credit limit.
- If you allow payments higher than balance due or credit limit, make sure members are unable to spend a credit balance.
- Work with your vendor/card processor, fraud monitoring system and/or core processor to implement velocity (number of payments) rules for payments to revolving credit.
- If you are using a third party to process ACH payments, review the agreement for potential shifts of liability. You need to fully understand the authentication layers when a member or bad actor signs into the credit card payment system.

While this risk alert focuses on payments made using ACH as the current trend, the same scheme has been committed in the past using paper checks. It is important to remember that fraud is cyclical and ever evolving and as the payments industry evolves, so will the fraud.

RISK MITIGATION RESOURCES

- The [Federal Register](#) provides details about delaying availability of credit after accepting ACH and Check payments towards lines of credit.
- Tap into knowledge from our experts by [visiting our risk alerts library](#).



The information presented in this email is intended for informational purposes only and should not be construed as legal advice or a legal opinion and it may not reflect the most current legal developments. You should seek the advice of legal counsel of your choice before acting on any information provided in this email.