

Reading on a mobile device? Please view our [mobile version](#).



Fraud Alert

ATMs and EMV Compliance

Recently, credit unions in the northwest have experienced fraud occurring via counterfeit ATM cards being used to make cash withdrawals at ATMs.

Fraudulent withdrawals are always a possibility if bad-actors are able to obtain compromised card data. The prevalence of card skimmers and data breaches contribute to the rise in fraud and, in particular, have contributed to the recent trend in fraudulent ATM withdrawals.

Once a point of compromise is discovered, credit unions move quickly to block the compromised cards and issue new ones. However, during the time between the creation of the counterfeit card and the credit union shutting off the card, fraudulent withdrawals can happen and many are left wondering where the liability lies given the new EMV liability provisions.

Mastercard and Visa rules shifted ATM liability to non-EMV compliant ATMs in 2016 and 2017, respectively. This means that if a fraudulent transaction occurs with a card that, at original issuance, was EMV compliant at a non-EMV compliant ATM, the ATM owner is liable for the transaction. If the card was not EMV compliant but the machine was, then the issuer retains liability.

There is also a rule provision that allows the processor to notify the issuing institution if the magnetic stripe is being read due to an issue at an EMV-capable machine. When this occurs, the denial or acceptance of that transaction will be the responsibility of the issuer.

Additionally, if the credit union's ATM is not EMV compliant, it is important that transactions are coded as fallback transactions. Within the liability shift provisions, there is an exception that provides some relief to non-EMV compliant ATM owners. If a non-EMV compliant ATM codes a transaction as a fallback, then the liability shifts back to the issuer of the EMV card. This coding

shifts the liability back to the issuer because it not only notifies the issuer that the transaction is not EMV-compliant, but also provides the issuer with the option to either accept or deny the transaction.

#CUobsessed

Katie Clark CUCE, BSACS

Director, Regulatory Compliance & Risk Management

Northwest Credit Union Association

503.350.2221 • 800.995.9064 x221

www.nwcua.org

If your credit union needs to report fraud, please fill out [this form](#).

Copyright © 2018 Northwest Credit Union Association

Idaho Office: 2710 W Sunrise Rim Rd, Suite 100 • Boise, ID 83705

Oregon Office: 13221 SW 68th Pkwy, Suite 400 • Tigard, OR 97223

Washington Office: 18000 International Blvd, Suite 350 • SeaTac, WA 98188

If you would like to stop receiving ALL emails from us, go [here](#).

To sign up for other mailing lists, go [here](#).

Please send any comments about this email to webmaster@nwcua.org.