INSIGHTS *by CSCU*

CSCU

WHAT CREDIT UNIONS SHOULD KNOW ABOUT FALLBACK TRANSACTIONS

As more POS terminals are being upgraded to EMV chip-ready, and more credit unions are getting chip cards in the hands of their members, questions regarding fallback transactions are being generated.

What is a fallback transaction?

Simply stated, a fallback transaction occurs when a chip card is presented to a chip enabled terminal ("chip-on-chip"), but the transaction is conducted as a swipe, usually due to the terminal unable to read the chip on the card. This could be due to a defective or scratched chip, a terminal or network incorrectly configured or with a chip reader that is defective (all legitimate reasons for fallback), or a chip intentionally damaged so it cannot be read, on a counterfeit card encoded with magnetic data stolen from a chip card.

When a terminal is properly configured, the process flow would be:

If a cardholder attempts to swipe a chip card at a chip-enabled terminal, the terminal should display instructions to insert the card into the reader.

1. The cardholder inserts the card (either because they initially knew to do so, or were directed by the terminal) but
2. In this case, the terminal is not able to communicate with the chip on the card.
3. After the terminal retries to read the chip (a pre-configured number of retries), the terminal will display a CHIP ERROR; USE MAG STRIPE message to the cardholder (sometimes reworded for cardholder display).
4. The cardholder swipes the card, and the transaction is sent to the issuer for authorization.

Why it's important to understand fallback transactions.

Fraud liability is the main reason to fully understand fallback transactions. If there is counterfeit fraud involving a chip-issued card at a non chip-enabled terminal, then the merchant who did not upgrade the terminal is responsible for any fraud, meaning the issuer can chargeback the fraud to the merchant. However, if the terminal is enabled to read chip cards, but the transaction is conducted using magnetic swipe, then the issuer is responsible for the liability for fraudulent transactions, if the issuer authorizes the fallback transaction.

Is it possible to counterfeit an EMV card?

For now, it will be extremely difficult to counterfeit or modify the chip. But if the fraudsters can get a hold of payment credentials (from a breach) then they can create a counterfeit card that looks like a real chip card, with the stolen credentials on the mag stripe. However, if the mag stripe data is counterfeit, more than likely the chip on that same card is altered, fake, or is from a stolen chip card and made to be unreadable. When the counterfeit card is inserted into the chip-enabled terminal, the terminal will not be able to proceed using EMV, and will most likely (depending on settings at the terminal) display instructions to swipe the card. If the issuer then authorizes the fallback transaction (it is coded as a fallback) and it is fraudulent, the issuer is liable for the fraud.

So should I decline fallback transactions?

It is strongly recommended that you do not decline fallback transactions, not for the first one or two years. At least initially, there will be many legitimate reasons for fallback: valid but defective or otherwise unreadable chips, merchant terminals not configured properly, technical interoperability, etc. Based on observations from the EMV roll-out in Canada, legitimate fallbacks will significantly decline by the end of the second year, and issuers can begin to decline fallback.

How can I tell if the transaction is a fallback?

If the terminal is configured correctly, the authorization request from the processor should be encoded with:

Terminal Entry Capability 5 (chip device)
Track 2 Equivalent Data Service Code (Digit 1) is 2 or 6 (chip card), and
POS Entry Mode 02 or 90 (magnetic-stripe read)

It is these three items, when viewed together, which defines that a chip card, at a chip terminal, used mag stripe entry.

What should I be doing differently?

Monitor reports from your processor for fallback transactions. Several fallback transactions on a single cardholder may indicate a defective card, or the need for member education (that member is probably getting frustrated), or it may indicate a counterfeit card in use. Several fallback transactions from a single merchant may mean a terminal or a processor or a PIN debit network is not properly configured.

For more information:

CSCU
888.930.2728
Email: info@cscu.net
3031 N. Rocky Point Dr. W.
Ste. 750
Tampa FL 33607
cscu.net