Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

Do you block fallback authorizations at Point of Sale (POS) and Automated Teller Machines? If not, you may be at risk.

CHIP CARD HISTORY & SUMMARY

Back in October 2014, the chargeback rules shifted the fraud liability to the weakest link at the POS to the entity that was not chip enabled. In 2016-2017 the fraud liability shift applied to ATMs that were not chip enabled. Then, debit and credit card issuers added the chip and/or contactless option to prevent card present counterfeit.

What changed with the shift in fraud liability involving fallback on chip enabled cards at the POS and Automated Teller Machine?

Fallback was introduced after the chip rollout. If the chip card would not read, you had the option to offer fallback authorizations on a chip magnetic stripe at the POS or ATM. If you offer fallback authorizations, as the card issuer you have given up your dispute/chargeback rights and will retain the fraud losses. The key issue is the merchants' POS devices/systems need to be programmed properly so there are no issues accepting a chip enabled card on their chip enabled POS device.

POINT OF SALE (POS) FALLBACK

Fallback can present itself in two ways at POS:

1. A bad actor inserts a fake chip on a chip enabled card and the chip will not read. The merchant will instruct the cardholder to swipe the card and if you offer fallback the authorization will go through as a magnetic stripe authorization. As the card issuer, you have no chargeback rights against the merchant.
2. A legitimate cardholder's chip will not read on the merchant's chip enabled POS device. The merchant will instruct the cardholder to swipe the card and if you offer fallback the authorization will go through as magnetic stripe authorization. As the card issuer, you have no chargeback rights against the merchant. You need to notify your cardholders to let you know if this is happening so you can report that merchant to the card association(s). You may also need to reissue your cardholder a new chip card like you did when a card's magnetic stripe demagnetized in the past (prior to the chip roll-out.)

AUTOMATED TELLER MACHINE (ATM) FALLBACK

If your Automated Teller Machines (ATM) are chip enabled and your cards are fully chip enabled, there is no reason to allow fallback to a magnetic stripe authorization. If you have the old-fashioned ATM network cards, this could be an issue since these cards are not chip enabled. For financial institutions that no longer offer the old-fashioned ATM network cards, blocking fallback at your ATMs is a non-issue. This will prevent

foreign non-chip cards and fake chip cards from being used at your chip enabled ATMs.

HOW THE ATTACKS ARE OCCURRING

Fallback attacks are happening when the bad actor puts a fake chip on the card and the chip will not read at either a POS or ATM. If your financial institution allows fallback when the chip authorization fails, the authorization will get approval as a chip magnetic stripe authorization, or a key entered authorization. If you allow mag stripe fallback, you've given up your chargeback rights to the card present merchant. We strongly recommend you understand the risk involved with a fallback authorization on chip cards. Chip technology - both cards and readers - are tested and certified and the fallback should be very rare.

The question to ask is: Does your financial institution want to assume the fraud liability risk for magnetic stripe and/or key entered fallback authorizations when the chip technology fails? If your financial institution authorizes the fallback transaction (coded as a fallback) and it is fraudulent, you are liable for the fraud losses.

HOW CAN I TELL IF THE AUTHORIZATION IS A FALLBACK?

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

- Terminal Entry Capability 5 for the chip device
- Track 2 Equivalent Data Service Code (Digit 1) is 2 or 6 for the chip card and POS Entry Mode 02 for partial magnetic stripe, 90 for full unaltered magnetic stripe read, or POS 01 for manually key entered authorization
- MasterCard chip card fallback entry mode is POS 80 when the chip card was unable to process, and the magnetic stripe read is the default

These items define if a chip card at a chip terminal used magnetic stripe entry (POS 02 or POS 90) or manually key entered (POS 01) authorization. If you opt not to block the fallback authorization option, we strongly recommend you block all partial magnetic stripe read (POS 02) and manually key entered for card present situations only (POS 01) from being a part of the fallback authorization options.

RISK MITIGATION STEPS

- We strongly recommend blocking fallback at the POS and ATMs.
- Check that you are not experiencing fallback fraud if you have not blocked the chip card fallback authorization option. Confirm the authorization strategy you have in place is helping to minimize or prevent fallback fraud. (For example: allow one fallback authorization up to X number of dollars within a 24-hour timeframe.)
- Understand you will not have any disputes/chargeback rights against the merchant for unauthorized fallback fraud on your chip cards. You will retain the fraud.
- Understand the risk of fallback fraud versus member/customer service when making your business decision. Chip technology is tested and certified and should be working properly. Blocking the fallback authorization option will help prevent your financial institution from incurring fallback fraud liability risk.
- Monitor reports from your processor for fallback authorizations to help identify the merchant and merchant's terminal that is not reading the chip properly. Report this merchant to the card association so they can investigate why the POS is not reading the chip when the chip is working at other merchants.
- Work with your card processor and authorization provider to block fallback authorizations on your chip card program(s) at the POS terminals.

- Work with your ATM authorization provider to block fallback authorizations on your chip card program(s).
- Educate your cardholders to use the contactless option (if available) on their dual-purpose chip card or use a mobile wallet if the chip will not read at the POS.

As we continue to partner and manage risk together, we will provide updates and information about how you can prevent the bad guys from committing fraud against your financial institution. Continue to keep us abreast of any upticks you may be experiencing so we can all dig deep to get to the root causation.

RISK MITIGATION RESOURCES

- Download the free risk checklist: Chip Fallback Authorizations Strategies to Reduce Fraud Impact
- Read the article: Canada Payment Security Roadmap (PDF Download)
- Register for our quarterly deep dive, Let's Talk Fraud, into what's happening in the world of fraud.
- Learn more from our risk experts by visiting our fraud library.
