FAQ Document

Financial Institution

Card Fraud Prevention FAQs

Card fraud has reached its highest point in years. As this fraud continues to rise, so do the questions relating to how to prevent these crimes.

The following are frequently asked questions relating to card fraud with responses provided by industry-acclaimed fraud expert, Ann Davidson, VP of Risk Consulting at Allied Solutions.

1. What are the quickest and most effective ways to respond to card fraud?

The best method to fight the fraud that you are experiencing is to find out how the bad guys are getting in. Take the card(s) you are experiencing fraud on and use the card with the least amount of card transactions and compare this card to the other cards to see if you can identify a common point of purchase (CPP). Quick action steps would be to lower the daily $ limit, create flash fraud rules and to block the card in certain locations (i.e. block countries or locations). These quick fixes may help until you are able to dig deep and find out the root causation of "how" the card fraud is happening.

2. What are the top 5 ways to prevent card present fraud?

(1) Lower daily dollar limits

(2) Require a PIN

(3) Adjust your fraud monitoring parameters

(4) Validate that 100% of all cards are chip enabled

(5) Dig deep to find out why you are having card present fraud and identify how the bad guys are able to get through your card security layers. Reach out for help if needed from your vendor(s).

3. What are the top 3 ways to prevent card-not-present (CNP) fraud?

(1) Find out why you are not able to charge back the fraud to the merchant. Was there a security tool the bad guys were able to use such as Verified by Visa (VBV) or MasterCard SecureCode (MCSC) and create a password for your cardholder?

(2) Validate if the CVV2/CVC2 was compromised and was validated during the authorization. This means the bad guy was able to obtain the 3 digit CVV2/CVC2 number on the back of the card, or this was a phishing attack.

(3) Was the full address verification (AVS) a match which prevented a chargeback to the CNP merchant?

The key with CNP fraud is in most of the cases, you as the card issuer, have chargeback rights back to the merchant unless VBV/MCSC passwords matched, CVV2/CVC2 was authenticated and AVS was a full match. It is key you find out why you are not able to charge the fraud back to the merchant.

4. What is the number one issue you are seeing as to why card fraud continues to grow and is not mitigated or stopped?

Today the number one card fraud issue appears to be fallback fraud which allows the bad guys to continue with magnetic stripe fraud on a chip card at a point of sale or at an ATM. Another prevalent issue of fraud is happening on all the cards that are not chip enabled cards. To help prevent this fraud is to accelerate and mass reissue all of your cards that are not chip enabled today. Once your program is 100% chip enabled, make sure you address your fallback authorization strategies for both point of sale and automated teller machine or the fraud will move to card-not-present (CNP) fallback fraud.

5. Is card fraud more prevalent in the card present (CP) or card-not-present (CNP) space?

Card present. As skimming and data breaches continue and fraudsters know where the weakest links are, they will use a counterfeit card to obtain cash or gift cards. Industry experts claim attacks will continue to migrate to CNP fraud, but today we are continuing to see CP fraud as most prevalent around the country.

6. Is there one particular card vendor (card processors, network, core data processor, and others) that is better at managing risks than other vendors?

Each vendor who handles your layers of card security is a key player to help prevent or mitigate card fraud. It is critical to find out what layers of card security are in place and what actions your vendors are doing for you, and to find out why you are experiencing card fraud if all of the card security layers are in place. Each vendor has pluses and minuses and we do not endorse any vendor over another. What we do endorse as you are selecting your vendor: find out what they have available to manage your card risk and what have been their successes to help prevent and mitigate card fraud. This is key as you obtain your RFPs on your card vendors in today's environment.

7. What trends are you seeing in terms of issuers setting their host systems to decline ALL fallback transactions?

The option should be available for you to block fallback at the point-of-sale and ATM. It is your decision as the card issuer to block fallback and educate your cardholders if there is a cardholder service issue. What we have heard from financial institutions who have blocked fallback is that they have very few to no cardholder service issues.

8. Are CVV requirements set by the card issuers or the merchants?

The settings for CVV/CVC (for non-chip cards) and dCVV/ICVV (chip cards) are set by the card issuer during the validation by the merchant. If it does not match or is missing, the authorization should be declined. Check with your card vendor and find out how they have your settings set up. Each vendor performs the validation differently.

9a. If a cardholder authorizes a friend to make a purchase and the friend uses the card other places, does the cardholder still have dispute rights?

If the credit or debit card was given to the friend to use they become an authorized user, and the card owner forgoes all dispute rights. You will want to read the disclosure information you provide to your cardholders when they receive a credit card (Regulation Z) or debit card (Regulation E), as well as your card association's liability rules.

9b. What if a cardholder gives their card to someone to use, the person gives the card back, and then the person steals the card? After the theft, then the cardholder can file a claim, right?

Yes, because in this case the person who stole the card is an unauthorized user. You will want to review your account holder disclosure as to the liability assessment based on date reported and the date of the first fraud.

10. Are any financial institutions limiting ACH payment frequency to card balances? If so, what kind of limits are most common?

What we are seeing for ACH payments on credit cards is that financial institutions are limiting the number of payments made using ACH within a 30 day timeframe. We have also seen some financial institutions not accept any ACH payments on credit cards. Others are also making sure there is never a credit balance that is created on the credit cards line of credit. Monitoring your incoming credit card payment report daily is a key management tool to manage this risk.

11. Do most financial institutions deny Fallback Transactions on their EMV cards?

Not today. But we are hearing from more financial institutions that are looking into blocking these fallback transactions to help prevent any fallback fraud. It is key to look at your fallback authorization strategies for both point-of-sale authorizations and authorizations at your ATM's to determine the best course of action to take.

12. When do you predict tokens will be coming out as an additional security measure for online purchases?

Token capability is available today by some of your card vendors. It is key for you to talk with your authorization vendor and ask if it's available and use it if it is. If not, push your authorization vendor to have tokenization available for you in the future. Tokenization is currently in use for many of the mobile payments being performed today. (For example, ApplePay uses tokenization as one of the security layers in the authentication and authorization).

14. We don't decline transactions due to address mismatch. Should we be declining those?

You have chargeback rights for your Address Verification Service (AVS) unless it is an exact address match. You will want to confirm this with your authorization vendor who is performing the AVS for you. This could be at your core DP level or at your card processor level. The party performing the AVS for you must hold your cardholder file information.

15. Too many national merchants still use fallback. So simply denying fallback transactions can create issues at these and other merchants, correct?

Correct. You may want to report these merchants to the card associations because you are giving up your charge-back rights in the event of card present fraud. In the meantime, you still have the option to allow fallback, but you may want to limit the dollar amount and the authorization to one transaction. It's your decision as to how you wish to manage fallback but the bad guys are out there finding out who allows it and who declines fallback on chip cards.

16. Is there a limit to how far back a cardholder can dispute a debit transaction under Visa zero liability?

You will want to review Visa's zero liability requirements. Also, review your disclosure given to your accountholder as to the liability and the reporting timeframe as to cardholder assessment.

17. If our financial institution's debit and credit cards are chip enabled, but our ATM-only cards are not chip enabled, can we still considered 100% chip/EMV?

What we are seeing in the industry is many financial institutions have eliminated the Network ATM card programs and have moved these cardholders to Visa/MasterCard/Discover Debit Card programs, since there are so many more layers of security with these card programs. Under the card association rules, you can offer a Visa/MasterCard debit card to a savings accountholder. If this accountholder does not have a checking account you will want to use a limit to not allow non-PIN authorizations. You will also need to follow Regulation D for these savings accountholders on the number of PIN authorizations. You may also want to reach out to other financial institutions who have eliminated their Network ATM programs and hear what they are experiencing.

18. Would our processor be able to provide us with statistics on how many fallback transactions we have?

Your processor should be able to provide you a report sharing with you the number of chip magnetic stripe fallback authorizations you are experiencing. Then, they should be able to share with you how many of these transactions were unauthorized versus authorized. If they do not have these types of reports, we strongly encourage you to request that they produce these reports for you.

19. We have all EMV chip cards with transactions completed online or over the phone. We see hundreds of fallback transactions (not fraudulent) each month from specific merchants' stores. Why do we see so many from these merchants?

EMV chip cards do not apply to card-not-present (CNP) transactions, i.e. mailed, over-the-phone, or online authorizations. EMV chip cards can only be applied to card present (CP) authorizations, i.e. those used with the physical card at the merchant's point-of-sale device. Fallback authorizations only apply to "chip magnetic stripe card present" transactions.

20. Many cardholders have shared they are not able to use their chip cards at certain merchants. Is there any way to circumvent this issue?

Unfortunately no. However, I strongly recommend you talk to your card association(s) and card vendor(s) so they can help resolve any potential issues with your cards or the merchant's card readers. If it is discovered that the merchant does not have chip enabled card readers, you should inform your members that is the case.

Contact us to receive more risk education and support: alliedsolutions.net/contact-us.

1164-11/18