FAQ Resource

October 2022

Let's Talk Fraud: Thwart Online & Payment Card Fraud

During our "Let's Talk Fraud" webinar series, we discuss strategic approaches to protect your accountholders and keep them educated and informed. Learn more prevention tactics and best practices with answers to these commonly asked questions.

Table of Contents

Payment Card Fraud

Q: What is the best way to prevent card fraud?

A: There are many different ways bad actors perform card fraud schemes, such as card present fallback, card not present, and ATM card fraud attacks. While there is not one "silver bullet" method for preventing the different kinds of card fraud attacks, these protocols can help mitigate card fraud attacks:

- Establish strong identification requirements for all account access and information requests across all channels
- Enable EMV on all cards and ATMs
- Block and reissue cards with any risk of exposure, big or small
- Review POS entry codes to unveil the type of card fraud taking place to identify and repair weaknesses

Register for "Let's Talk Fraud" to learn about the latest fraud prevention tools, tips, and strategies to safeguard your financial institution: ***alliedsolutions.net/lets-talk-fraud***

CARD NOT PRESENT FRAUD

Q: How is 3DSecure payment fraud occurring and how can we prevent losses?

A: 3DSecure (3DS) is a fail-safe program used by card processors to protect card not present transactions from fraud. If a fraud attack occurs when 3DS is in use, this means there was a failure in your financial institution's authorization and/or fraud monitoring processes. Since these losses cannot be charged back to the card processor or merchant, it is extremely important to take steps to prevent these exposures. Here are steps your financial institution should take to protect against these 3DS fraud attacks:

- Make sure your institution is signed up for 3D Secure 2.0 and are authorizing these kinds of secure transactions
- Dig into these authorizations (ECI 05) to ensure all fraud tools and practices are turned on and working
- Adopt strong remote authorization processes, including address verification, Geolocation, and dynamic CVV codes
- Contact your card processor(s) directly to find out how and why these fraudulent authorizations passed through their channels in the first place
- Offer accountholders text/email transactions and or fraud alerts so they can catch and report any unauthorized transactions

Q: What happens if a consumer makes a purchase on a website, but later realizes the site was a scam? Can a financial institution use chargeback rights since there was fraud?

A: If an individual was scammed, it's not fraud since the consumer did not perform that activity or that activity was unauthorized. If a consumer is being scammed, work with your chargeback team at the financial institution or third-party vendor. There are some chargeback rights if the individual did not receive the purchased merchandise.

Q: What is internet order fraud and how can it be prevented? How do Regs E and Z come into play?

A: Internet order fraud is an old term for card not present fraud: fraud that occurs through an online or mobile purchase made with a payment card. These crimes often happen from an external breach through a merchant. Adopt strong security layers to prevent chargeback from these card not present attacks.

These layers include:

- Address verification service (AVS)
- CVV2/CVC2
- 3D Secure 2.0
- Fraud monitoring systems
- Machine learning fraud analysis and prevention tools

Regulation E applies to an accountholder's level of liability for attacks on debit cards and ACH debit transactions. **Regulation Z** states that up to $50 in losses can be assessed for credit card transactions. Keeping fraud data and reports on hand is key to properly assess the liability. It is also important to review your EFT disclosures with your card providers, as the liability will be assessed differently under those agreements.

Q: What are financial institution chargeback rights with debit card fraud, ATM fraud, and provisional credit?

A: Your financial institution has chargeback rights if fraud occurs on one of your chip-enabled cards at a non-chip enabled ATM or POS device, as long as you have fallback authorizations blocked. Similarly, you have chargeback rights if fraud involving another financial institution's non-chip-enabled card occurs at one of your chip-enabled ATMs or devices.

On the flip side, if your financial institution still has non-chip enabled cards or ATMs, you forgo your chargeback rights if one of the following fraud crimes were to occur:

- Magnetic stripe card fraud using one of your non-chip enabled cards
- Fraud using chip-enabled cards on your non-chip enabled ATMs
- Fraud at a chip-enabled ATM using your non-chip enabled cards

Your provisional credit periods must align with the standards outlined by your card vendor(s): Visa offers a 5-day provisional credit period. The provisional credit period for all other card vendors, including Mastercard, is 10 days.

Q: Does Reg E apply to the P2P transactions when it comes to the debit cards and their ability for chargebacks?

A: Reg E does apply to P2P debit card transactions under the electronic funds transfer. To confirm, be sure to review your EFT disclosure agreements. For consumers, debit transactions would apply to Reg E under debit card. For payment apps, scammers are getting the number during consumer enrollment or from unauthorized means. Chargeback rule of card not present under the unique category code for Merchant Category Code 4829 for money transfers.

Q: How can institutions mitigate contactless payment fraud?

A: Since the COVID-19 pandemic, there has been a rise in the use of digital wallets and mobile payments. In turn, many payment networks have increased contactless payment limits to promote the use of this more hygienic payment method. Even though fraud criminals have a harder time cracking these kinds of payments, these fraud crimes have still seen an increase with the growth in these payments and the expanded transaction limits.

Here are some tips for mitigating this type of risk:

- If you are not offering contactless payments, block the POS entry mode
- Limit the dollar amount on contactless transactions
- Utilize a transaction limit to keep the exposure to a 24-hour timeframe
- Use a fraud monitoring system to help identify contactless authorizations

CARD PRESENT FRAUD

Q: Are the card processors looking to expand the merchant codes to be able to drill down on specific payment types?

A: The short answer: No.

Visa and Mastercard use the same Merchant Category Codes (MCCs) in the industry. If there is fraud or the potential for fraud, card processors may want to build strategies and rules around certain MCCs to help catch or address fraud, but the codes themselves will not be expanded. NACHA has also built ACH codes called Standard Entry Class codes (SECs) that identify information and transaction type for ACH credits and debits for corporate and individual accounts.

Q: Is it best for the fallback option on ATMs to be turned off?

A: Yes. Blocking non-EMV card use and fallback authorizations at your chip-enabled ATMs is key to mitigating attacks on these devices, while at the same time helping to ensure the fraud liability from any exposure is not shifted to your financial institution.

If you have ATMs that are not yet EMV capable, set transaction and dollar limits for cards used at these devices to reduce the chargeback liability if another financial institution's chip-enabled card is exposed on one of your non-chip enabled machines. If you have not already done so, update all of your ATMs to be chip-enabled to prevent self-retained fraud losses on these devices. Not setting all of your ATMs to be chip-enabled will almost certainly open you to preventable loss exposures, given that non-EMV machines are much easier for fraud criminals to break into. If your ATMs are not chip-enabled, you will retain any of the losses that occur from magnetic stripe fallback transactions occurring on EMV cards at your non-EMV ATMs.

Q: What other tips do you have to mitigate ATM card fraud risks?

A: With ATM cash-out and skimming risks to financial institutions, it is important to:

- Establish daily dollar and transaction limits
- Install security software and hardware to prevent and be notified of tampering on your devices (i.e., anti-skimming device or a code-protected locking mechanism)
- Perform daily inspections of these devices to find the installation of unauthorized devices or settings

Not setting all of your ATMs to be chip-enabled will almost certainly open you to preventable loss exposures.

Q: What is sequential card issuance fraud, and how can it be prevented?

A: Generally speaking, these brute-force attacks (previously known as "Credit Master Attacks") involve the use of auto-dialers to uncover issued card numbers, then find the expiration date and code once an issued card is uncovered. If card numbers within your BIN are issued in sequential order, versus random order, these attacks pose a much greater risk to your financial institution. If one card is exposed, all of the other issued cards within this BIN are more likely to be exposed.

The best way to prevent this kind of attack is to verify that none of your card BINs are issued in sequential order. If they are, it is in your best interest to reissue these cards to reduce the exposure risk from one of these brute force attacks.

Q: What are the best tips for combating brute force attacks, if the BIN is not sequential?

A: If BIN issuance is random, here are some best practices:

- Check expiration dates as some brute force attacks can occur on those as well. Expiration dates should also be random to manage risk
- Watch your card response and denial codes very closely. Inform your card merchants if there are repeated card authorizations attempted at a single merchant, as this is a key indication your issued cards have been exposed to a brute force attack
- Confirm you blocked key-entered authorizations on card present transactions. These could be a part of a brute force attack involving PIN attempts or authorizations at a POS or ATM after a counterfeit card has been created

Payment App Fraud

Q: What are some key detection and prevention methods for fraud on payments apps like Venmo, Zelle, and Cash App?

A: Every payment app varies in their limits and how much money can be sent on a daily/monthly basis. Be sure to look at your agreements with payment apps, particularly on layers of security in place for authentication before money goes out the door.

Detection methods include:

- Monitor activity surrounding "money transfer" type of authorizations (i.e., Merchant Category Code MCC 4829) if the payment app is set up with a debit card
- Confirm your fraud monitoring system is capturing and flagging these kinds of card authorizations, so you can monitor and block subsequent suspicious activity
- Offer text or email alerts to accountholders so they may detect and report any unauthorized transactions
- Validate if you offer the payment apps using the accountholders' account number versus a debit card. Make sure you are monitoring these two methods of how the funds leave your financial institution in the P2P environment

Prevention methods include:

- Establish strong identification requirements for all account access and information requests across all channels
- If an online password reset is requested, wait until the accountholder has approved this via email or text before authorizing any additional account changes (i.e., change of address, phone number, or email)
- Set daily velocity limits: a maximum number of ACH and debit card transactions within a 24-hour timeframe
- Set a maximum daily dollar limit for both ACH and debit card payment app authorizations

ACH Fraud

Q: What happens if an accountholder withdraws or sends funds prior to identifying an unauthorized ACH Credit deposit as fraud when our financial institution is acting as the RDFI?

A: Under the ACH rules, financial institutions acting as the RDFI do not take on the risk for fraudulent ACH Credits being deposited into your accounts. If the funds are already gone, the ODFI takes on 100% of the liability risk. If there are still funds in the accountholders' account, freeze the funds and request an indemnification letter from the ODFI before returning the funds to them. Perform name matching on ACHs to uncover any mismatches. If the name on the incoming ACH Credit does not match the name on the account it's coming into, return the ACH Credit back to the ODFI. Refer to NACHA's website for more information about these return rules.

Q: What ACH risks do ODFIs (Originating Depository Financial Institution) face today?

A: ODFIs face these risks:

- ACH Credit Fraud: Money sent out of your account and deposited into an account at the RDFI
- ACH Debit Fraud: Money deposited into your account from an account at the RDFI
- ACH Loan Fraud: ACH payment made from an account at the RDFI on your accountholder's HELOC or credit card loan
- ACH Payment App Fraud: Money sent or received from a payment app (i.e., Zelle, Venmo) using the account number instead of debit card information

Q: What are some ACH fraud prevention techniques for an ODFI?

A: Adopt these strategies to manage fraudulent ACH attacks:

- Adopt software that captures and reports potentially counterfeited checks
- Limit the dollar amount on outgoing ACH credits to the RDFI
- Set up multiple layers to authenticate ACH credit requests (e.g. passwords/passcodes, security questions, callbacks/text authorization)
- Don't provide immediate credit when pulling the funds in from the RDFI
- Place holds or block ACH payments on any line of credit disbursements
- Place a hold on any incoming ACH deposit and validate where and from whom the funds came

Q: After an online transaction or transfer is made the accountholder says the unauthorized charge was not them. Who is ultimately responsible for that kind of loss?

A: A couple things to consider here:

- For online ACH transactions where your FI initiates the credit, you warrant the risk
- The RDFI doesn't warrant the risk or have to give the money back to you
- Ask questions about your authentication layers like, "How are individuals authenticated?" and "What door did a scammer use to get into an account?" and "How was the transaction authenticated prior to money going out the door?" Many financial institutions are responsible for restitution due to unauthorized transactions
- Payment apps (such as Zelle, PayPal, Venmo) will result in a larger quantity of smaller losses

Q: What is the difference between A2A and P2P fraud attacks, and what are ways to prevent these attacks?

A: P2P payments involve the use of ACH credit to perform an external transfer via bill pay. P2P fraud attacks primarily occur via breached authentication layers for outgoing ACH credits, especially through the online and mobile environment.

A2A payments involve ACH transfers between an accountholder's own accounts.

There are several things financial institutions can do to amplify their protection layers and mitigate these attacks, such as:

- Set ACH daily dollar limits and transaction limits for P2P and A2A ACH transactions
- Use multiple layers to authenticate the ACH credit with your accountholder prior to release
- Work with your ACH association to help identify the fraud entry point and prevent future attacks
- Perform micro/mini deposit authentication prior to authorizing a P2P or A2A transaction
- For A2A, validate the name at the receiver to make sure it is going into your accountholders' account
- If possible, consider temporarily turning off P2P payments thru your vendor if an attack occurs
- Share practical ID theft and scam prevention tips with your accountholders to help them protect their information

Subscribe to receive more risk education: alliedsolutions.net/enews

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®