Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

SUMMARY

Financial institutions across the country continue to experience card-not-present (CNP) fraud at an alarming rate, and it is not stopping. Currently in the top fraud spot, this type of fraud occurs online and involves both credit and debit card numbers. Most of the CNP fraud is the result of 3-D Secure fraud formerly known as Verified by Visa (VBV) and MasterCard SecureCode (MCSC).

The CNP fraud starts with either the cardholder's information being shared by the cardholder, being phished, found on the dark web, through a data breach, or BIN attacks.

The big question is why is the card issuing financial institution retaining the fraud? Do you not have chargeback rights or were chargebacks/disputes not exercised? You, as the card issuer, need to dig deep to uncover the answers. Solutions are available to stop almost all this fraud.

HOW THE ATTACKS ARE OCCURRING

Since COVID, bad actors have transitioned to online fraud, and most financial institutions have implemented chips to help prevent and mitigate card present fraud. However, approximately 80% of card fraud for the coverage Allied produces for our clients involves CNP fraud.

In working with financial institutions having CNP online fraud, here is what we've learned:

- Card issuers are not participating in 3-D Secure.
- Card issuers are not on 3-D Secure 2.0 or greater. If you continue to be on 3-D Secure 1.0, this is the information that will be used for the (a) authentication and (b) subsequent authorization.
- Card issuers are not properly disputing and charging back the CNP online fraud to the acquirer's financial institution based on the available ECI (Electronic Commerce Indicator) codes.

- If card issuers are participating in 3-D Secure, the authentication layers being used are weak during the authentication of the cardholder prior to the authorization.
- Card issuers are not receiving the ECI code to be able to understand if the online CNP fraud can be disputed and charged back to the online merchants acquiring financial institution.
- Card issuers are being informed they have no chargeback rights.

RISK MITIGATION STEPS

To help prevent and mitigate CNP fraud, it's critical you validate and confirm the following risk mitigation steps now:

- Confirm your organization is signed up and participating in 3-D Secure 2.0 and obtain written confirmation of such.
- Note: In 2001 when VBV and MCSC were rolled out, many financial institutions did not sign up since many financial institutions said they were not experiencing CNP fraud. Are you still not participating?
- Validate the authentication layers being used by 3-D Secure and find out if the bad actor passed the authentication layers to obtain the subsequent 3-D Secure authorization approval. Multi-factor authentication is key: 1) something you know, 2) something you have, and 3) something you are. Strong consumer authentication layers are key for 3-D Secure. Find out what authentication layers you have in place as the card issuer for 3-D Secure. Confirm that they are strong and cannot be circumvented by the bad actor.
- You need to ask why you have no chargeback rights and what the ECI code is.
- Visa's ECI codes for who is liable in the event of fraud:
    - ECI 5: Fully authenticated – card issuer is liable – no chargeback rights
    - ECI 6: attempted authentication – card issuer not participating or system unavailable – card issuer is liable – no chargeback rights
    - ECI 7: merchant liable – chargeback rights
- MasterCard's ECI codes for who is liable in the event of online fraud.
    - ECI 00 3-D Secure authentication either failed or could not be attempted- merchant liable
    - ECI 1: attempted authentication – merchant liabl
    - ECI 2: fully authenticated- successful – issuer liable – no chargeback rights
    - ECI 6: applies to 3-D Secure 2.0 only – merchant liable – chargeback rights
- Confirm with the card associations on any changes or updates to the ECI codes.
- Confirm why you do not have available chargeback rights for 3-D Secure CNP online fraud.
- Confirm your disputes/chargebacks are being exercised during the timeframes per the card associations. Refer to the card association's rules and regulations.
- Set daily dollar limits to reduce online CNP fraud for both credit and debit cards used in a CNP environment.
- Confirm that your fraud monitoring strategies, parameters, and rules are in place to help prevent and detect online CNP fraudulent authorizations in a real-time fraud monitoring system.
- Card issuers could use a 6-digit code for authentication with the cardholder but make sure the cardholder does not share or give out this 6-digit code to anyone.

- Card issuers should confirm the velocity limit in place for the number of PINless debit authorizations within a 24-hour time frame.
- Validate and confirm you are supporting the 3-digit number known as CVV2/CVC2/CID if the online merchant is using the 3-digit code during the authorization for the online CNP authorization. We strongly recommend you look at moving to a dynamic validation of the 3-digit CVV2/CVC2/CID. Today, many CUs are using a static 3-digit number on the back of the card. If you are using a static solution for the CVV2/CVC2/CID, the bad actor can obtain the number and use it for a CNP transaction.
- Card issuers should be using dynamic security codes (dCVV2/dCVC2/dCID) for CNP authorizations. Dynamic CVV2/CVC2/CID reduces CNP fraud by more than 90%. CVVKey (dynamic solution) is usable with or without 3-D Secure.
- Validate and confirm you are supporting Address Verification Service (AVS) using a full unaltered address verification match. For any other type of AVS, you should have chargeback rights back to the online CNP merchant's acquiring financial institution.
- Validate and confirm you are using a biometrics solution to help combat online CNP fraud. This may be an option with 3-D Secure authentication layer.
- Keep an eye on CNP contactless fraud using mobile apps or mobile devices which uses a code of POS 07 for contactless authorizations.
- Educate your cardholders to only use secure sites when shopping online and to take extra caution even when doing so.
- Educate your cardholders to never share any personal or financial information through email, online chat, or unsolicited phone call, text, or social media.
- Work closely with your card processor and the card associations to find out what is being done to help minimize online CNP fraud since it continues to grow at an alarming rate.
- Confirm with the card associations the timeframes they are no longer going to be offering VBV and MCSC and moving to 3-D Secure and how they will be only supporting 3-D Secure 2.0.
- Continue to identify, validate and confirm the type of CNP fraud you are experiencing to help prevent or mitigate the CNP fraud.
- Reach out to your Allied representative to let them know what trends you are finding as you research your CNP fraud.

RISK MITIGATION RESOURCES

- Visit Allied's Risk Alerts Library
- CVV introduction (1-minute video)
- Prevention tips from Keyno
- Review Visa's Rules and Policies
- Review MasterCard's Identity Check™, 3-D Secure, and Rules (as of June 2022) pages

 LinkedIn  Instagram