Risk Checklist

Financial Institution

Card Security Measures

Card fraud exposures continue to increase in frequency and sophistication.

Follow these checklists to ensure your institution and vendors have adopted security practices that will help to prevent this growing fraud type.

Allied Solutions

May 2021

Card Security Checklist

Adopt the following security methods to help prevent card fraud exposures:

☐ Confirm you have strong card authorization strategies for magnetic stripe fallback authorizations at your ATMs and in-branch point-of-sale devices.

☐ Utilize chip-and-PIN for all card programs to help prevent magnetic stripe fraud.

☐ Consider adopting end-to-end encryption for transaction validation.

☐ Confirm CVV/CVC is working for all magnetic stripe authorizations and confirm the response code is set to decline.

☐ Confirm exact card expiration date is working effectively for both card present and card-not-present authorizations, and confirm the response code is set to decline.

☐ Confirm name matching is working for all magnetic stripe track 1 authorizations and confirm the response code is set to decline.

☐ Confirm Address Verification Service is being utilized when the merchant opts to transmit during the authorization.

Visit our website for more risk education: ***alliedsolutions.net/resources***

☐ Confirm daily dollar limits are being used for all card present and card-not-present authorizations, and confirm authorizations that exceed that limit within a 24 hour-time frame are set to decline.

☐ Confirm card activation is used on all new, renewal, replacement, and additional cards sent out to the cardholder.

☐ Verify the card activation methods do not use the last 4 digits of the cardholder's social security number.

☐ Require over-the-phone or online PIN activation.

☐ Confirm your financial institution supports and develops challenging enrollment criteria for Verified by Visa (VBV) and MasterCard SecureCode (MCSC) to add an additional layer of online shopping security to your cardholders.

☐ Validate and confirm your Fraud Monitoring System is working in real time and is utilizing 24/7/365 case management to instantly detect and prevent the first unauthorized attempt.

Card Vendor Security Checklist

Confirm your card vendors have the following risk measures in place to help prevent card fraud exposures:

□ dCVV/iCVV authorizations are being used for the chip validation.

□ The exact card expiration dates are working effectively for both card present and card-not-present authorizations, and the response codes are set to decline.

□ Name matching is working for all magnetic stripe track 1 authorizations, and the response code is set to decline.

□ The CVV2/CVC2 is working effectively if the merchant opts to transmit the CVV2/CVC2 in the authorization message. If the CVV2/CVC2 does not match when transmitted, decline the authorization.

□ An address verification service is being utilized when the merchant opts to transmit during the authorization.

□ Daily dollar limits are set for all card present and card-not-present authorizations, and that any transactions exceeding that dollar limit within the 24 hour time frame will not be authorized.

□ Secure card activation methods are being used on all new, renewal, replacement, and additional cards sent out to the card holder.

□ A fraud monitoring system is in place, and working in real time to help prevent any unauthorized payment attempt.

□ Validate your vendors' fraud strategies in place are both rules based and behavior based to help minimize unauthorized transactions.

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

Allied Solutions

GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

This checklist is for informational purposes only and is not to be considered legal advice.