Risk Checklist

Financial Institution

Best Practices to Prevent Card Fraud

Card fraud remains a top concern for financial institutions, with both card-present and card-not-present fraud rising. Follow this checklist to implement best practices for mitigating card fraud.

Allied Solutions

November 2021

Risk Checklist for Card-Present Fraud

- ☐ Establish daily dollar limits for point-of-sale credit card and debit card transactions.
- ☐ If magnetic stripe fallback was allowed, evaluate the compromised card number to help determine if the risk is high. A high risk involves the full, unaltered magnetic stripe data from track 1 and/or track 2. Utilize name matching if track 1 data was part of the breach.
- ☐ Turn off any active non-EMV cards and replace them with chip-enabled cards.
- ☐ Review card associations' alerts and act immediately on at risk card data outlined in alert.
- ☐ Analyze at-risk open card accounts to determine which cards are/are not still active.
- ☐ Review other card accounts to find out which cards are non-active and have already been closed due to fraud.
- ☐ Identify the fraud pattern to uncover where the breach took place, also known as the common point of compromise (CPP), and report it immediately.
- ☐ Block and reissue impacted, open card numbers when magnetic stripe has been compromised.
- ☐ Accelerate the reissuance of active cards 30-180 days prior to their expiration dates.
- ☐ Ask the card association(s) to take recovery action related to any expenses.
- ☐ Establish multi-layer authentication requirements for any financial transactions or sensitive information requests performed in-person.
- ☐ Report any card fraud to the Visa Fraud Reporting System and/or MasterCard's Safe System.
- ☐ Connect with your card processor to make sure they have velocity parameters in place for transactions requiring PINless debit authorizations.
- ☐ Regularly monitor cardholders' accounts for any suspicious activity.
- ☐ Implement card technologies, such as encryption, tokenization, and biometrics.
- ☐ Train employees on fraud detection methods and prevention strategies for card-present fraud.
- ☐ Invest in bond solutions that offer plastic card coverage.

Visit our website for more risk education: ***alliedsolutions.net/enews/risk-alerts***

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

Risk Checklist for Card-Not-Present Fraud

- ☐ Establish daily dollar limits for online credit card and debit card transactions.
- ☐ Ensure that your financial institution is set up on version 2.0 of 3D Secure
- ☐ Adopt strong remote authorization processes, including address verification, Geolocation, and dynamic CVV codes.
- ☐ Establish multi-layer authentication requirements for any financial transactions or sensitive information requests performed online.
- ☐ Adopt strong security layers to prevent chargeback from these card-not-present attacks, including:
  - Address verification service (AVS)
  - CVV2/CVC2
  - Fraud monitoring systems
  - Machine learning fraud analysis and prevention tools
- ☐ Monitor breached card accounts closely to prevent subsequent card-not-present fraud instances. (If the card was not blocked and reissued, close monitoring is extremely critical.)
- ☐ Conduct testing with synthetic information to determine where system vulnerabilities exist and promptly address them.
- ☐ Give accountholders the ability to opt into transaction notifications, so they can immediately catch and report any suspicious transaction activity.
- ☐ Report any card fraud to the Visa Fraud Reporting System and/or MasterCard's Safe System.
- ☐ Train employees on fraud detection methods and prevention strategies for card-not-present fraud.
- ☐ Send cardholders information about how and where to report any suspicions of fraud.

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

Allied Solutions
GROW, PROTECT AND EVOLVE YOUR BUSINESS.®

975-R5-11/21