Allegiance
MERCHANT SERVICES

Card Network Update

Chip (EMV) Acceptance in the United States At-A-Glance

Allegiance Merchant Services is committed to assisting you in navigating through the various considerations that you may face when making decisions about whether to invest in EMV-enabled payments solutions.

In August 2011, Visa announced its roadmap for EMV-enabled (chip) card acceptance in the United States, and mandated to processors that chip transactions be supported beginning in April 2013. In the year that followed, the other major card networks within the U.S. (MasterCard, Discover, and American Express) followed suit with their intentions to support chip card acceptance, as American Express made its announcements in July 2012. The card networks have introduced certain policies designed to incentivize participation in chip card acceptance (for example, with PCI validation relief for selected eligible merchants,) and discourage non-participation (with liability shift policies now placing additional financial liability on merchants for certain types of fraud when chip is not supported at the merchant location).

To help support you in your decision making, we have created an at-a-glance view below of how these policies compare between the different card networks. In order to view the expanded details and requirements for each Program Component click the component below:

<table>
<tr><th><i>Program Component</i></th><th><i>Effective Date</i></th><th>Visa</th><th>MasterCard</th><th>American Express</th><th>Discover</th></tr>
<tr><td>PCI Validation Relief</td><td><i>October 1, 2012</i></td><td colspan="4">Level 1 and Level 2 merchants eligible for relief from annual PCI validation if 75% of transaction count are processed through a dual interface chip-capable device</td></tr>
<tr><td rowspan="2">Liability Shift</td><td rowspan="2"><i>October 1, 2015</i></td><td colspan="4">Non-chip supporting party (Issuer or [<i>Acquirer/</i>]merchant holds liability for counterfeit fraud</td></tr>
<tr><td>N/A</td><td>MasterCard only: merchant will have liability for lost/stolen/never received issued fraud if the card is hybrid PIN-preferring and the terminal does not support PIN with the transaction, even when the terminal supports chip.</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Data Compromise Cost Liability Reductions</td><td><i>October 1, 2013</i>
<i>October 1, 2015</i></td><td>N/A at this time</td><td>For U.S. Account Data Compromises opened after Oct 1, 2013, merchants may be eligible for a 50% reduction in their liability of operational reimbursement (OR) and fraud recovery (FR) costs. After Oct 2015, compromised merchants will not be assessed for either OR or FR, if they meet the eligibility criteria.</td><td>N/A at this time</td><td>N/A at this time</td></tr>
</table>

PCI validation relief

As a merchant handling cardholder data, you are required to be compliant with PCI-DSS (Payment Card Industry Data Security Standards). For further information on PCI, please view the PCI Security Standards web site at https://www.pcisecuritystandards.org/index.shtml and as always please feel free to contact your Client Executive.

All merchants are assigned a classification level based on criteria related to the volume of account numbers processed, the acceptance channel, and any prior data compromise history. For merchants qualified at PCI Level 1 or 2, you may be eligible for relief from certain annual PCI validation requirements. The 75% threshold for EMV transactions is calculated by the number of aggregate transactions processed annually. (MasterCard's 75% threshold includes MasterCard and Maestro transactions.) Entities with Corporate-owned and franchise locations are evaluated based on structure. For example, if you have separate legal entities (multiple DBAs) for which you complete a separate Report on Compliance (ROC), one for your retail business and one for your e-commerce transactions, the card networks can calculate your transaction volume using just the retail portion of the business.

In order to qualify for PCI validation relief, a merchant must process 75% of their annual transactions through a dual-interface POS terminal. A dual-interface terminal is one which supports both contact EMV, where the EMV enabled card is inserted into the device for the chip to be read, and contactless EMV, where the EMV enabled card or payment device (e.g., a mobile phone,) is tapped on the point of sale terminal to be read via NFC (near-field communication). A merchant must also meet the following requirements in order to qualify:

VISA Technology Innovation Program (TIP):

- 75% of annual total U.S. acquired Visa transactions must be processed through dual-interface POS terminals.
- Previously validated PCI compliance within last 12 months (or submitted a remediation plan).
- Confirmation that sensitive authentication data (i.e., full contents of magnetic stripe, CVV2 and/or PIN data) is not stored, as defined in requirement 3.2 of the PCI DSS regulations.
- Although Visa may waive certain annual validation requirements for qualifying merchants, all merchants are still required to maintain on-going PCI DSS compliance.
- Visa reserves the right to require full PCI DSS validation of any compromised entities.
- Must not be involved in a breach of cardholder data (may qualify if have validated PCI-DSS compliance subsequent to a breach).
    - Fines, fees, or assessments are still applicable for an account data compromise event.

Additional Recommendations:

- Merchants may seek to limit the availability of all payment card data within their environment through technologies such as data field encryption and/or tokenization, which would aid in their PCI DSS compliance.
- Use of CVV2 (Card Verification Value) and VbV (Verified by Visa) to mitigate card-not-present fraud.

MasterCard PCI DSS Compliance Validation Exemption Program:

A qualifying Level 1 or Level 2 Merchant located in the U.S. region may participate in the MasterCard PCI DSS Compliance Validation Exemption Program (the "Exemption Program"), which exempts the Merchant from the requirement to annually validate its compliance with the PCI DSS.

In order to qualify or remain qualified to participate in the Exemption Program, a duly authorized and empowered officer of the Merchant will be required to certify to Allegiance Merchant Services in writing that they have satisfied all of the items listed below:

- Merchant validated compliance with the PCI DSS within the previous twelve (12) months or, alternatively, which has submitted to Allegiance Merchant Services, and Allegiance Merchant Services has submitted to MasterCard, a defined remediation plan satisfactory to MasterCard to ensure that the Merchant achieves PCI DSS compliance based on a PCI DSS gap analysis;
- Merchant does not store Sensitive Card Authentication Data. Allegiance Merchant Services must notify MasterCard through compliance validation reporting of the status of Merchant storage of Sensitive Card Authentication Data;
- Merchant has not been identified by MasterCard as having experienced an Account Data Compromise Event during the prior twelve (12) months.
- Merchant has established and annually tests an ADC Event incident response plan in accordance with PCI DSS requirements.
- At least 75 percent of the Merchant's annual total U.S.-acquired MasterCard and Maestro Transaction count is processed through a Dual Interface Hybrid POS Terminal, as determined based on the Merchant's transactions processed during the previous twelve (12) months via MasterCard's GCMS and/or Single Message System. Transactions that were not processed by MasterCard may be included in the annual U.S.-acquired Transaction count if the data is readily available to MasterCard.

Allegiance Merchant Services is required to retain all Merchant certifications of eligibility for the Exemption Program for a minimum of five years. Upon request by MasterCard, Allegiance Merchant Services must provide a Merchant's certification of eligibility for the Exemption Program and any documentation and/or other information applicable to such certification. Allegiance Merchant Services, as your card transaction acquirer, is responsible for ensuring that each Exemption Program certification is accurate.

A Merchant that does not satisfy the Exemption Program's eligibility criteria, including any Merchant whose Transaction volume is primarily from e-commerce and Mail Order/Telephone Order (MO/TO) acceptance channels, must continue to validate its PCI DSS compliance in accordance with the MasterCard SDP implementation schedule.

All Merchants must maintain ongoing compliance with the PCI DSS regardless of whether annual compliance validation is a requirement. Fines, fees, or assessments are still applicable for an account data compromise event.

We have compliance personnel and resources available to work with you if you need assistance in determining your eligibility for PCI validation relief. Please contact your Allegiance Merchant Services Account Executive for further details. For details specifically related to American Express and Discover please contact your respective account representative for each of those payment card networks.

Liability shift

Today in the United States, the card-issuing financial institutions shoulder most of the costs of counterfeit card fraud. With the introduction of Chip/EMV, new policies of Visa, MasterCard, and American Express will shift this liability to acquirers and their merchants in certain cases. The policies of these three networks now indicate that effective October, 2015, if *a contact chip card is presented to a merchant that has not adopted chip-reading terminals, the acquirer and their merchant will hold the financial liability for counterfeit card fraud. (Note: the liability shift for automatic fuel-*

dispenser has been announced as October 2017.) Counterfeit card fraud occurs when a fraudster copies payment card data which is then presented at a merchant's point-of-sale terminal. The concept behind this policy is to encourage both issuers and merchants to invest in chip technology, as the dynamic authentication process supported by the card embedded chip protects against fraud in a way that a magnetic-stripe read card cannot. In fact, a "chip-on-chip" transaction, one in which the card or device has a chip, and the EMV enabled point-of-sale device reads the chip, is considered one in which counterfeit fraud will simply could not occur. For lost/stolen/never-received or issued card fraud, generally the card issuer will hold the financial liability if the transaction occurs at a terminal which supports chip. MasterCard, however, expands on the policy by also pushing responsibility of lost/stolen/never-received or issued card fraud to the acquirer and their merchant if the leading cardholder verification method (CVM) established by the issuer is an offline PIN (whereby the terminal authenticates the PIN), and the merchant's device does not support PIN. It remains to be seen when and if issuers will widely adopt PIN and a component of their EMV card implementation, as the common expectation is that most U.S. card issuers will lead with cardholder signature when first introducing chip cards into the market.

Globally, in other regions and countries where EMV payment methodology has been adopted, significant decreases in counterfeit card fraud and other security losses have occurred. The United States is the last major economic region and country globally to adopt a liability shift for chip payments.

Data Compromise Cost Liability Reductions

Today, in the event a merchant's point of sale system experiences a data breach and cardholder data is compromised, the card brands have programs to determine whether the merchant should bear some financial liability of the issuers' losses and costs for increased card monitoring and/or re-issuance and ultimately counterfeit fraud. When considering whether compromised merchants should bear some of the costs associated with a data breach, the card networks may consider the PCI compliance of a merchant at the time of the breach, the number of cards considered at-risk and the issuer counterfeit fraud losses incurred. MasterCard is enhancing the available incentives for chip support in the U.S. by modifying its ADC program to offer a new or increased deductible under their ADC program which reduces a merchants' financial liability should a data compromise occur.

Under MasterCard's ADC program, a merchant may be responsible for Operational Reimbursement (OR), Fraud Recovery (FR) and a case management fee. Operational Reimbursement is the calculation of financial liability for an acquirer and their merchant based on the number and type of at-risk card accounts and may be further adjusted based on factors such as expiration dates and expiration cycles. Fraud Recovery is the calculation of financial liability for an acquirer and their merchant based on the at-risk timeframe for incremental counterfeit fraud to occur. With MasterCard's new incentive, there is an opportunity for the OR and FR to be reduced.

For ADC event investigation cases opened after October 1, 2013, U.S. merchants are eligible for a 50% reduction from the OR and FR calculation if the following qualification criteria are met:

- At least 75% of the merchant's total transactions, and at least 75% of the transactions within the scope of the Account Data Compromise (ADC) event, were processed through dual-interface chip accepting terminals
- No sensitive card authentication data was stored
- The merchant had not previously experienced an Account Data Compromise event in the prior 12 months

NOTE: For ADC event investigation cases opened after October 1, 2015, U.S. merchants are eligible for a 100% reduction from the OR and FR calculation if the following qualification criteria are met:

- At least 95% of the merchant's total transactions, and at least 95% of the transactions within the scope of the Account Data Compromise (ADC) event, were processed through dual-interface chip accepting terminals.
- No sensitive card authentication data was stored.

- The merchant had not previously experienced an Account Data Compromise event in the prior 12 months.

We appreciate your selection of Allegiance Merchant Services for your card processing services and we are available to assist you with any questions or additional concerns you may have regarding these upcoming changes. Please contact your Allegiance Merchant Services Account Executive for additional support or questions.