Visa Business News

VISA

**Risk Management** | Data Security 12 November 2015

# Best Practices for the Appropriate Use of Visa Account Data

**AP, Canada, CEMEA, LAC, U.S.** | *Acquirers, Processors, Merchants, Agents*

**Executive Summary:** Visa reminds acquirers and their merchants of the risks associated with incorrectly using Visa account data.

As card acceptance around the world migrates from magnetic stripe to EMV chip, Visa reminds merchants not to engage in practices that result in the unnecessary storage of sensitive authentication data.

One example of unauthorized Visa account use is when a merchant completes a secondary card read at the point of sale (POS) after the card has been used to obtain authorization during a chip-based transaction. This practice is often referred to as “double swiping,” even when the first card read is completed by dipping the chip card or via contactless transaction.

In most cases, the secondary card read is unrelated to completion of the transaction. Merchants usually complete this secondary card read to collect account data from the magnetic stripe and use it to create a separate record that supports the merchant’s accounting, reporting or customer-relationship management programs (e.g., loyalty and rewards).

## Risks of a Secondary Card Read

Visa reminds acquirers and their merchants of the significant risks associated with a secondary card read. The secondary card read often results in the merchant capturing and retaining static data encoded on the magnetic stripe—which violates the Visa Rules (ID#: 0002228)—and unnecessarily increases the merchant’s exposure to potential payment account data compromise.

Both the Visa Rules and the Payment Card Industry Data Security Standard (PCI DSS) prohibit storage of the full contents of the magnetic stripe after a transaction authorization (ID#: 0002228). This data, if compromised, can be used by criminals to create counterfeit cards and perpetrate fraud.

In addition, a secondary card read undermines investments that Visa clients and merchants have made in EMV chip technology, which has dynamic authentication capabilities that greatly reduce a criminal’s ability to commit fraud. Visa forensic investigations have found compromise cases in which merchants successfully implemented secure POS solutions but failed to secure systems that store sensitive authentication account data captured during the secondary card read.

## Visa Rules Compliance

Acquirers are reminded that merchants are not permitted to use or request Visa account data for any purpose that is not related to payment for goods and services (ID#: 0008585).

To ensure compliance with the Visa Rules and the PCI DSS, and to avoid being subject to possible non-compliance assessments, acquirers should require their merchants to immediately discontinue secondary card reads.

### Best Practices to Prevent Secondary Card Reads

Acquirers and merchants should implement the following to eliminate this practice:

| Acquirers | Merchants |
|---|---|
| • Communicate with merchants about the risks of a secondary card read and require that they discontinue this practice immediately<br>• Provide a list of vendors that offer compliant integrated payment solutions / software applications<br>• Update merchant agreements and/or online application forms to ensure merchants choose solutions that do not require a secondary card read | • Use alternative identifiers for loyalty and rewards programs (e.g., loyalty cards, transaction IDs, truncated primary account numbers) to link customer relationships<br>• Ensure all systems and applications that store, process or transmit Visa account data comply with the PCI DSS, including systems and applications that may have been used to capture data through a secondary card read<br>• Use service providers included on the Visa Global Registry of Service Providers and POS applications validated against the PCI Payment Application Data Security Standard (PA-DSS). |

All payment system participants are responsible for maintaining data security. Because criminals will continue to look for opportunities to steal cardholder data, acquirers and merchants must address known risks and minimize exposure to data compromise. Visa is committed to increasing data security awareness and providing communication, training and best practices to all payment system stakeholders to ensure they are aware of potential vulnerabilities and associated risks.

## Additional Resources

### Documents & Publications

"Acquirers Warned of Risks Associated With Double Swiping," *Visa Business News*, 3 May 2012

### Online Resources

Visa Global Registry of Service Providers

Visa Payment Security

PCI Security Standards Council

PCI SSC Validated Payment Applications

## For More Information

Contact your Visa representative. Merchants and third party agents should contact their issuer or acquirer.

Notice: This Visa communication is furnished to you solely in your capacity as a customer of Visa Inc. (or its authorized agent) or a participant in the Visa payments system. By accepting this Visa communication, you acknowledge that the information contained herein (the "Information") is confidential and subject to the confidentiality restrictions contained in the Visa Rules, which limit your use of the Information. You agree to keep the Information confidential and not to use the Information for any purpose other than in your capacity as a customer of Visa Inc. or a participant in the Visa payments system. You may disseminate this

Information to a merchant participating in the Visa payments system if: (i) you serve the role of “acquirer” within the Visa payments system; (ii) you have a direct relationship with such merchant which includes an obligation to keep Information confidential; and (iii) the Information is designated as “affects merchants” demonstrated by display of the storefront icon (🏪) on the communication. A merchant receiving such Information must maintain the confidentiality of such Information and disseminate and use it on a “need to know” basis and only in their capacity as a participant in the Visa payments system. Except as otherwise provided, the Information may only be disseminated within your organization on a need-to-know basis to enable your participation in the Visa payments system.

Please be advised that the Information may constitute material nonpublic information under U.S. federal securities laws and that purchasing or selling securities of Visa Inc. while being aware of material nonpublic information would constitute a violation of applicable U.S. federal securities laws. This information may change from time to time. Please contact your Visa representative to verify current information. Visa is not responsible for errors in this publication.