TO: **All Merchants**

FROM: **American Express®, Diners Club®, Discover® Card, JCB®, MasterCard® Canada Inc., Visa® Canada Association**

RE: **Merchant Requirements for Securing Cardholder Information**

The rising incidence of stolen cardholder account data is a major concern for all participants in the payment industry. As a result of these thefts, merchants and financial institutions suffer fraud losses and unanticipated operational expenses, and consumers are inconvenienced significantly. To protect your business, your customers (cardholders), and the integrity of the payment system, each of the card companies has in place a set of requirements governing the safekeeping of account information. This document gives a brief overview of the most critical aspects of those requirements.

Summary of Card Company Requirements Governing Cardholder Information Security

Storage of Cardholder Information	▪ Do not store the following under any circumstance: – Full contents of any track from the magnetic stripe on the back of the card. – Card-validation code—the three-digit value printed on the signature panel of a MasterCard®, Visa®, Discover®, JCB®, or Diners Club® card, and four-digit code printed on the front of an American Express® card. ▪ Store only that portion of the customer's account information that is essential to your business—i.e. name, account number or expiration date. ▪ Store all material containing this information (e.g., authorization logs, transaction reports, transaction receipts, car rental agreements, and carbons) in a secure area limited to authorized personnel.
Destruction of Cardholder Information	▪ Destroy or purge all media containing obsolete transaction data with cardholder information.
Use of Agents or Third Parties (Vendors, Processors, Software Providers, Payment Gateways, or Other Service Providers)	▪ Advise each merchant bank or processing contact (representing each of your card brands) of any agents that engage in, or propose to engage in, the processing or storage of transaction data on your behalf—regardless of the manner or duration of such activities. ▪ Make sure these agents adhere to all rules and regulations governing cardholder information security. Any violation by your agent may result in unnecessary financial exposure and inconvenience to your business.
Reporting a Security Incident	▪ In the event that transaction data is accessed or retrieved by any unauthorized entity, notify the merchant bank or processing contact for each card brand immediately. ▪ This report will not only minimize risk to the payment system, but protect your customers in the most responsible manner. Systems and procedures are in place to immediately stop the unauthorized use of compromised data, but are effective only when you do your part to promptly report a security incident.

We continue to work on your behalf to reduce payment card fraud, and offer this communication to enhance your awareness, minimize risk, and protect your customers. If you have any questions or would like to have more information, please visit our web sites or contact your representatives for any of the card brands sponsoring this correspondence.

www.americanexpress.com www.dinersclubus.com www.discovernetwork.com www.jcbusa.com www.mastercardmerchant.com www.visa.ca