An Update on Last Week's Visa and MasterCard Data Breach

April 2, 2012 - On Friday we informed our readers about a data breach that took place at a credit card processor - Global Payments, Inc. - that exposed credit card information for a large number of Visa and MasterCard customers. Since then, more information has become available that we thought you should know about.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 =

document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script');

po.type = 'text/javascript'; po.async = true;
po.src =

'https://apis.google.com/js/plusone.js';
var s =

document.getElementsByTagName('script')[0];

s.parentNode.insertBefore(po, s);
})();

Original reports of the breach said that as many as 10 million Visa and MasterCard accounts had been breached. The actual number, while still quite large, is considerably smaller. Global Payments is reporting that 1.5 million card accounts were exposed. They are also stating that so far, there has been no fraudulent activity reported on any of the breached accounts.

While the breach did include credit card account numbers, it did not include other personally identifiable information such as names, addresses, birth dates or Social Security Numbers. While this means that the accounts may subject to some false charges, it is likely to limit the usefulness of the breached data. Even in online transactions, most merchants now require the full name associated with the credit card as well as a security code that is printed on the card, prior to processing a transaction. If there is a data mismatch - such as the name on the account doesn't match the one being

used for the transaction, or the billing address is incorrect - the card processor should reject the purchase before it can be made.

Visa, MasterCard and the banks issuing their cards have begun notifying consumers who hold affected cards. Anyone who used one of these credit cards to pay for parking in New York City since the beginning of the year should be looking at their billing statements to make sure that they don't have any fraudulent charges on them.

The good news is that it doesn't look like the thieves involved with this breach will be able to benefit too much from their crime.

byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS