Newtek®
"The Small Business Authority®"

Newtekinsurance.com | 855-2-thesba

Newtek Breach Protection Program

Program Overview

The Newtek Breach Protection Program is a new and unique indemnification program acquired to reduce monetary exposure in the event of a data compromise of a merchant account. The Breach Protection Program is designed specifically to meet the expenses resulting from a suspected or actual breach of credit card data from a merchant account. Underwritten by Great American Insurance Group (www.greatamericaninsurance.com), a financially strong insurance organization whose insurance companies are rated "A" by independent third party rating agencies.

The Program Limits

Each merchant account is protected up to a maximum of $100,000 and there is NO deductible.

The Program Covers

- A mandatory forensic audit required by the Payment Card Industry Data Security Standard (PCI DSS) of a merchant when a data breach is suspected.
- The data breach can be either a system/network breach or the physical theft of the credit card data from stolen receipts, stolen computers, skimming, or even employee theft.
- Card replacement costs and related expenses resulting from the data breach.
- All Level 2, 3 and 4 merchants regardless of their level of compliance with the standard.

Program in Action:

A breach was suspected at the location of one of our clients, and Visa requested a forensic audit be complete at the merchants expense. The quote for the audit was $22,500 and once submitted to the carrier, the client received a check within 48 hours, so they could move forward with the audit. In this case no fines were assessed, but had the merchant been fined the program may have supplied some protection for them.

Frequently Asked Questions
Regarding the Newtek Breach Protection Program

Why do merchant accounts need this coverage?
If a merchant account suffers a suspected or actual data breach, the business responsible for the merchant account could incur thousands upon thousands of dollars of unexpected costs in the form of audit expenses, card monitoring and replacement expenses, and fines. These costs could significantly affect revenue…and even jeopardize the existence of a business. The Newtek Breach Protection Program reduces a protected merchant account's monetary exposure when a presumed or actual data compromise occurs, thus providing peace of mind!

What insurance company underwrites this program?
Great American Insurance Group (www.greatamericaninsurance.com) has collaborated with RGS to create this program. Great American is a well-established, financially strong insurance group whose insurance companies hold "A" ratings from independent third party rating agencies.

What is the the protection limit?
The maximum protection is $100,000 per incident, for each merchant account.

Is there any deductible?
There is NO deductible!

If a merchant agreement has multiple merchant accounts, is each account protected for $100,000?
The Newtek Breach Protection Program provides protection on a per-merchant account basis but an incident and annual limit of $500,000 does apply to a merchant agreement with ten or more protected merchant accounts.

Can any merchant account qualify for this program?
Any Level 2, 3 or 4 merchant account is eligible, provided it has not already suffered a data compromise. Level 1 merchant accounts are not eligible for this protection.

Must a merchant account be PCI DSS compliant in order to be protected under the Program?
No. However, if a merchant account experiences a breach, the merchant account must become compliant before that merchant account can participate in (or re-enter) the Program.

Level 4 merchant accounts aren't breached often are they?
Absolutely, they are! Nearly two thirds of all breaches occur at Level 4 merchant accounts. In fact, Eduardo Perez, VISA USA's Vice President of Payment Systems and Risk, stated at the 2007 Electronic Transactions Association trade show in Las Vegas, "Hackers are concentrating on the smaller merchants… that's where we see the greatest vulnerability."

If the transaction processing system used with a merchant account does not store magnetic stripe data, can it still have a data compromise?
Yes! While it is true that merchant accounts that store magnetic stripe data are the most vulnerable, there are a number of other risks. For example, missing or outdated security patches, using vendor supplied default settings and passwords, SQL injections by hackers, unnecessary and vulnerable services on your servers, stolen receipts, stolen computers, employee theft, and skimming can all lead to significant data compromises and subject the merchant account to audits, card replacement costs, and fines.

IF a merchant account is certified to be PCI DSS compliant. Does it still need to be in the Program?
Yes! Certification of PCI DSS compliance is not a guarantee that a breach will not occur. The analogy that best describes the situation is this: "You can have the best alarm system in the world, but it is useless if you don't turn it on." Also, the Program covers employee theft and the physical theft of data. PCI DSS compliance alone cannot prevent these losses.

How is a data compromise reported for the Program?
To report a data compromise you simply have to: (1) complete the online claim form; (2) submit (via the web or fax) the notice from the card brand or acquiring bank that stipulates there has been (or there is the suspicion of) a data breach at your covered location; and (3) submit (via the web or fax) a copy of the invoice provided by the certified PCI DSS auditor.

To submit additional expenses on an open claim you simply have to: (1) enter your claim number in the online claim form; and (2) submit (via the web or fax) a copy of the demand for payment from the card brand or acquiring bank that explains that these demanded reimbursements/fines were the result of an actual data breach.

If a merchant account does suffer a loss, how quickly will the claim be processed?
Quickly! Once the relevant documentation is provided, the requests for payments will be processed. Assuming that the documentation is in order, the request should be processed within thirty days.