Data Breach Security Program for Merchants

Frequently asked questions about the program designed to protect you from the potentially business-threatening costs of a data breach.

Q. What is the Data Breach Security Program for Merchants? Why do merchants need it?

A. The Data Breach Security Program for Merchants is designed specifically to help you meet the significant expenses resulting from a suspected or actual breach of credit card data. Depending on the severity of the breach, these expenses can include the costs for a forensic audit, replacement of compromised cards, and compliance fines—costs that can easily reach $25,000 to $50,000 for Level 4 merchants. In other words, costs that are more than enough to shut down a small business.

Q. Who offers this program?

A. The program is offered by Vantage Limited, the electronic payments industry experts, and is 100% underwritten by financially strong insurance organizations rated "A" by independent third-party rating agencies.

Q. What are the coverage amounts?

A. The basic coverage provides either $50,000 or $100,000 per merchant account per year and up to $500,000 for any one merchant per year.

Q. Some merchants have multiple locations. Is each location covered under policy limits?

A. Yes. Vantage Limited can provide coverage on either a per merchant basis or a per merchant account basis.

Q. Is there any deductible?

A. No. There is never any deductible.

Q. Can any merchant qualify for this protection?

A. Any Level 2, 3, or 4 merchant is eligible for coverage as long as they have not had a previous data breach. If a Level 2, 3, or 4 merchant has had a previous breach—or suffers one while covered—the merchant can become eligible (or re-eligible) for coverage once PCI DSS compliance is verified. Level 1 merchants are not eligible for this coverage.

Q. Does a merchant have to be PCI DSS compliant to be eligible for coverage?

A. No. However, we highly recommend that all merchants comply with PCI DSS. It is important to remember that a merchant that has been breached must become compliant before that merchant can enter (or re-enter) the program.

Q. Small merchants—Level 3 and 4—aren't really breached that often, are they?

A. Absolutely they are! In fact, industry experts report that Level 4 merchants are the source of 85% of identified data compromises. It makes sense—Level 3 and 4 merchants are more likely to have faulty or non-existent business procedures for preventing employee access to confidential data, leading to a much greater likelihood of data theft.

What's more, recent studies by leading security vendors show that Level 4 merchants have the highest risk of having data stored on their POS software without their knowledge. Jennifer Fischer, Visa's senior business leader, payment system security compliance, confirms, "Visa continues to see small merchants most frequently targeted by hackers."

Q. What about merchants that don't store magnetic strip data? Can they be breached?

A. Yes! While it's true that merchants storing magnetic strip data are particularly vulnerable, any merchant can be breached. Risks all merchants face include missing or outdated security patches, use of vendor-supplied default settings and passwords, SQL injections by hackers, unnecessary and vulnerable services on their servers, poor business practices that allow physical access to cardholder data, physical losses resulting from employee dishonesty or third-party theft, and employee negligence or error.

Q. PCI DSS compliant merchants can't be breached, can they?

A. Yes, they can! Although it makes a breach less likely, PCI DSS compliance is not a guarantee that a breach won't occur. Any system that relies on people-run processes is vulnerable to breach, whether through deliberate employee wrongdoing or an unintentional—but inevitable—human error. That's why sections 7 and 9 of PCI DSS focus on business systems and processes, not technology systems and processes.

What's more, PCI DSS compliance is only a periodic measurement at a point in time. Between measurements, a breach can occur at any time: for example, when networking equipment or a keylogger is installed or when a new employee is hired without a background check.

Q. How does a merchant submit a claim?

A. A merchant only has to complete three easy steps to submit a claim: (1) fill out an online claim form by following the easy-to-use link in the merchant portal, (2) upload or fax the notice from the acquiring bank that stipulates there has been a suspected or actual breach at the merchant's location and choose an authorized, qualified security assessor, and (3) when the forensic audit is complete, upload or fax a copy of the assessor's invoice. That's it!

If a merchant has a claim for card replacement costs and related expenses and/or assessments and fines, they simply upload or fax a copy of the demand for payment.

Q. How soon do merchants receive their reimbursements?

A. Within 30 days of submitting a claim, assuming all documents are in order.