Consequences of a Merchant Data Breach . . .

Most Likely, Worse Than You Imagine

FEW THINGS POSE MORE OBSTRUCTIVE CONSEQUENCES to a company than a perceived data breach. More than not a few inconvenient thoughts, more than hundreds of hours and thousands of dollars, it can cost you the reputation and even the survival of your business – and for something over which you may have had no control or, worse yet, which may not necessarily be legitimate.

According to The U.S. National Archives & Records Administration, of businesses that lose their critical data for ten or more days, 50% must immediately file for bankruptcy.

Consider that the average cost per record breached is $202 and that businesses accounted for nearly 40% (a conservative estimate, considering many businesses elect not to report), with small merchants in particular being targeted. Data pillagers often go after those businesses they know don't have the resources to pay for sophisticated security systems.

The average cost of a data breach for a Level 4 merchant runs between $36,0000 — $50,000.

However, 35% of reported data breaches aren't brought about by malicious hackers but by human error (i.e. lost laptops, inadvertent posting data online, files tossed in a dumpster, etc.).

Regardless of how it happens, if you're a merchant, there's something you should know: if and when you are even *suspected* of a breach, you could be in for a uniquely unsavory experience. Taking anywhere from a few days to several weeks, just how invasive and exhaustive the security examinations and assessments are is worth outlining:

- a thorough review of your security policy
- an internal network vulnerability assessment of every computer and network service
- an examination of your IP connection's network perimeter (i.e., examiners manually attempt to breach your network)
- a manual inspection of appropriate virus software running on all of your computer equipment, including servers, workstation, firewall, router, etc.
- a run-through of both unauthorized wireless accessibility and any potential security weaknesses in your corporate phone system

As this is going on, your business operations are ground to a halt. In addition to substantial monetary costs, which range on average between $8,000 to $20,000 for Level 4 merchants, you'll of course be forced to absorb the opportunity costs incurred by the disruption.

Should the examination reveal no legitimate breach has taken place, you still pay – the aforementioned audit costs and time expenditure, not to mention your company's reputation. This represents a sort best-case scenario.

A legitimate data breach saddles a merchant with all kinds of additional fees: card replacement ($3 to $10 per card), $5,000 to upward of $50,000 in compliance fees, plus all and sundry costs associated with any incidents of actual fraud.

Ultimately, the average cost of a data breach for a Level 4 merchant runs between $36,000 and $50,000 – potentially detrimental to a small business.

When an acquirer seeks to collect on these expenses, and you, the merchant, do not have the funds in your merchant account or cannot pay, they will come after your future transactions. Your business dealings will have become exacerbated due to the hit to your company's reputation, and deciding to close your account or declare bankruptcy will land you on a "match list," and that'll be the end of your company's ability to accept credit cards.

If your merchant account becomes depleted due to breach costs, you will no longer be able to accept credit cards!

Bankers Insurance Group
Global Institutional Solutions