



## ABOUT PCI COMPLIANCE

PCI FAQs

MERCHANTS

ACQUIRERS/ISOs

SECURITY TIPS

IMPORTANT LINKS

Quick Links

APPROVED SCANNING VENDORS (ASVs)

QUALIFIED SECURITY ASSESSORS (QSA)s

INTERESTED IN SUBMITTING AN ARTICLE?



## THE REAL COST OF DATA BREACH

**(It's more than you think—and you're more at risk than you know.)**

Confusion. Denial. Plain old wishful thinking. That's what we hear when we talk to people about the real cost of data breach. Whether you're an ISO, an acquirer, or a merchant, maybe you've even said (or at least thought) some of these things yourself:

- "There aren't really that many data breaches—the media just hypes the few that happen."
- "As long as we're only *suspected* of a breach, it's really no big deal."
- "Even if there is a breach, we'll figure it out pretty quickly. How expensive could it be?" (and, if you're not a merchant, maybe you've even thought, "Well, at least we won't have to pay for it.")

Written by:  
Robert Halsey  
Apr. 16, 2009



*Robert Halsey,  
President, Royal  
Group Services Ltd*

Unfortunately, that's just the kind of thinking that gets businesses into trouble—the kind of trouble that all too often ends in bankruptcy. (And that's not media **hype—the U.S. National Archives & Records Administration reports 50% of businesses that lose their critical data for 10 days or more have to file for bankruptcy immediately.**)

So, when it comes to data breach, what's the reality? Well, to start with, according to the Identity Theft Resource Center, **the number of data breaches actually rose nearly 50% in 2008, compromising the personal records of at least 35.7 million Americans.** What's more, nearly 40% of all breaches targeted businesses (and that's a conservative number, since many businesses fail to report their data breaches at all). **When you consider that the average cost per record breached is \$202, it becomes clear just how much we all stand to lose.**

Of course, you might think that at least small merchants are safe because hackers and thieves only target big businesses with high sales. Unfortunately, you'd be wrong. Thieves know that large businesses have the resources to spend on sophisticated security systems and instead target smaller merchants where security is likely to be less effective. Jennifer Fischer, Visa's senior business leader, payment system security compliance, confirms: **"Visa continues to see small merchants most frequently targeted by hackers."**

And it's not only hackers and thieves you have to worry about, not when 35% of reported data breaches are the result of human error: lost laptops, inadvertent posting of confidential data online, files mistakenly tossed in an open dumpster—you know, the kind of mistakes people make simply because they're human.

So, suppose you or your merchant is suspected of one of those inevitable human errors, or of being a victim of a hacker. As long as there isn't actually a breach, it's no big deal, right? Wrong. **Once a merchant is even *suspected* of a breach, a team of PCI-DSS certified forensics security examiners swoops in to review and inspect its business practices.** This examination can take anywhere from a few days to several weeks, depending on the complexity of the systems involved. If you're a merchant, here's what you can expect:

- A security policy review—your security policies will be thoroughly reviewed and evaluated.
- An internal network vulnerability assessment—every computer/server/network service will be tested for thousands of security weaknesses.
- Penetration testing—if you have an IP connection, your network perimeter will be reviewed and evaluated. Next, a complete vulnerability assessment will be conducted. Then, the examiners will manually attempt to penetrate the perimeter.
- A manual computer inspection— all of your equipment (server, workstation, firewall, router, etc.) will be tested manually to ensure it is



Call 800-825-3301 (678-534-3262  
outside of the U.S. and Canada)

running the appropriate software versions, and then all virus software and other critical software components will be manually inspected.

- Wireless security testing—if any computers in your network have wireless access, the examiners will look for wireless accessibility to unauthorized computers and data.
- Phone line testing—your corporate phone system will be searched for listening modems and other potential security weaknesses.

That means that for a *minimum* of several days, your business is brought to an absolute standstill while the examiners comb through your policies, records, computer and phone systems, and employees—and eat away at your productivity, sales, and profits. And, as if that's not enough, at the end you'll have to pay the costs of the forensics examination, whether there was an actual breach or not: somewhere between \$8,000 and \$20,000 if you're a Level 4 merchant.

And that's only when a breach is suspected. What happens when the examiners find that a breach has actually occurred? Well, that's when the costs really start to add up. In addition to the costs of the forensics audit (remember, that's between \$8,000 to \$20,000), you'll be responsible for

- \$3 to \$10 per card for replacement costs
- \$5,000 to \$50,000 (or more) in compliance fines
- Additional fines based on the actual fraudulent use of the cards, which will vary depending on the number of cards exposed

The bottom line? The cost of a data breach for a Level 4 merchant averages \$36,000 and can be as high as \$50,000 (or more). In other words, more than enough to cripple—or even destroy—a small business.

So, what happens next? If you're the merchant, your acquirer will try to collect all of these expenses. If you don't have enough money in your merchant account, the acquirer will recover funds from your future transactions (which may unfortunately be less than you hoped, since your reputation will probably have taken a serious hit as a result of the breach). If you close your account or declare bankruptcy, you'll be put on a "match list" and be unable to accept credit cards.

If you're an acquirer or an ISO, don't make the mistake of thinking you can breathe easy. You're responsible for *all* costs and fines if the merchant can't pay them, even if the merchant no longer has a contract with you. When you consider that it can take as long as one year from the time a consumer notices a fraudulent transaction until you're notified, you can begin to get a sense of just what your exposure must be.

So, we're back to where we started: what is the real cost of data breach? The short answer is more than you think, rising all the time, and more likely to hit you than you'd like to believe. And as uncomfortable as that reality is, this is one case where what you don't know can most definitely hurt you.

[Home](#) | [Privacy](#) | [Terms of Use](#) | [Site Map](#) | [Contact Us](#)