
DOZIER

The Law Of Data And Information Security

MERCHANTS ARE RESPONSIBLE; POSSIBLE "ECONOMIC RUIN"

BY JOHN DOZIER

I DON'T NEED TO RECITE THE many security breaches that have led to major financial losses for companies during the past 12 months. Every business should already know the risks of leaving credit card and account information exposed. Basically, the risk is total loss of your business, and possibly your personal assets as well. And the risks, of course, come from many directions. If you process credit cards, your contract mandates PCI DSS compliance on an ongoing basis with huge penalties flowing from breaches. The Federal Trade Commission could pursue website contract and privacy policy violations, just about any state attorney general could sue for violations of a state's data security disclosure laws, enterprising lawyers could file class action lawsuits and every customer could sue for damages. Data loss is just an ugly problem to have, often leading directly to economic ruin.

That is the problem. The solution, fortunately, has been laid out for you in the PCI DSS guidelines. These are rules issued by Visa, MasterCard, American Express and others with which you must comply in order to accept credit cards. The standards are somewhat burdensome, but not unduly so. I founded one of the first ecommerce companies focused on the electronic movement of credit card account information between hundreds of vendors in the early 1990s, and we ended up moving millions of transactions through the web for American Express, Citicorp, Sears, American General Finance and First USA. At the time, we implemented security standards far beyond the requirements of PCI DSS, so I have a pretty good perspective on the data security arena and how the laws and regulations have developed and are continuing to develop.

Basically, depending upon your business rating, which is determined by risk and transaction volume, you have a sliding scale of obligations. Everyone who accepts credit cards online must build and maintain a secure network, manage passwords proactively, protect stored data, encrypt transmissions, use quality anti-virus software, maintain secure systems and applications, restrict data access to need-to-know personnel, restrict physical access, monitor each authorized user independently, track all network resource access and cardholder data access, and maintain a written information security policy. Then, depending upon your merchant ranking, you will have to demonstrate ongoing compliance in a self-reporting mode, through internal auditing, or for high risk and high volume merchants, possibly through independent external auditing.

As your small or mid-size business struggles to grow revenue, increase margins, reduce overhead and maintain focus on all of the key financial metrics that drive success, you have yet another hoop to jump through in order to run your online business. There is no direct payback here in terms of becoming compliant with PCI DSS. It is a cost of doing business, without which you cannot accept credit cards, and without which you increase dramatically your risk of loss.

A final word of caution is in order. Compliance is not something to hand over to your "IT guy" for execution. The IT manager is all too often more than happy to undertake projects for which he is ill equipped to complete in a quality way. Keep in mind that he is the guy who built the systems, or at least manages them, and a quality review of your system vulnerabilities and implementation of compliance standards and requirements is not something he should be handling. That approach has conflict of interest written all over it. ■

Basically, the risk is total loss of your business, and possibly your personal assets as well. And the risks, of course, come from many directions.

John Dozier is president of Dozier Internet Law, PC, a law firm representing small and mid-sized online businesses. He can be reached at jwd@cybertriallawyer.com or online at Cybertriallawyer.com.

The information in this article is not intended to be legal advice. Always consult your attorney when faced with legal issues.