THE RISE OF CREDIT CARD DATA BREACHES: THE THIEVES AMONG US

If it can happen to Target, it can happen to your business: tech-savvy thieves hack into a supposedly secure company computer system, steal identity and credit card data, and leave the company to clean up (and pay for) the mess. The December 2013 Target breach by "an amorphous group of Eastern European hackers"[1] compromised personal information of as many as 100 million people and cost the company $148 million in related costs to date.[2]

Even if your business is smaller than Target, the costs of data breaches are significant. The average cost to a business in 2013 was $5.4 million.[3] The largest costs from these crises come from customer notification, governmental fines, legal and public relations costs, and lost business.

No company that relies on electronic networks to do business is immune to the threat of a data breach, regardless of whether it operates a transactional website or merely accepts credit card payments. Worse, in most cases you won't find out there is a problem until it's too late. First notice of a data breach may come from your credit card processing company, informing you that your business has been identified as a likely source of fraudulent credit card activity.

You then may be required to retain a computer forensic investigator to confirm whether a theft occurred. The incident could be anything from onsite theft by an employee to hacking of your wireless network or electronic intrusion into your computer network by a hacker nearby or abroad.

If a theft occurred, the credit card entity may demand that your business reimburse it for a share of the fraudulent activity that resulted from the theft. You will not obtain much by way of due process, but rather will most likely be told what sum your credit card processor will withhold from the payments that were otherwise due.

You can also forget about successfully keeping the situation under wraps and handling it internally. The laws of most states (including Minnesota) require you to notify the affected customers of the loss of their credit card data. After that, the banks that issued the affected credit cards may sue you; the Federal Trade Commission may investigate you; and the customers whose data was compromised may file a class-action lawsuit. At a minimum, you can expect the news of the theft to adversely affect your standing with customers. Target reported that its 2014 Q2 earnings were down 46% from the year prior—gently acknowledging that "results softened meaningfully following our December announcement of a data breach."[4]

What can you do to avoid such liability and lost business? First, you should attempt to comply with Payment Card Industry ("PCI") standards, which aim to reduce the risk of loss in the first place and to favorably affect the calculation the credit card entity uses to determine what share of the fraudulent activity you are required to pay.

Next, you should make sure that your business insurance package covers such losses. Unfortunately, you can't assume that your standard policies do the trick. Since data breach losses may take the form of fines and third-party liability to consumers, it is likely that neither your standard commercial general liability policy, nor the computer fraud portion of your property insurance policy, will cover such losses. Or, if your policy does provide such coverage, it probably has sublimits that are paltry compared to the fines or other damages your company can face in such circumstances.

A safer bet is purchasing a separate Cyber Liability or Network Risk policy specifically designed to cover both a direct financial loss due to theft by hacking, as well as any third-party liability for a data breach, including defense costs and the costs of the data breach investigation. Look for a policy that includes Crisis Management/Identity Theft Expenses coverage for such costs as notification, credit monitoring, and public relations expenses resulting from a data breach. Work with your insurance broker to make sure that the policy covers liability for fines and contains limits of liability ample enough to cover a significant data breach. While Target had cyber insurance before its breach,[5] it recently reported that only $38 million of the $148 million (and counting) breach-related costs are offset by its policies.[6]

The expense for a separate Network Risk policy may also be worthwhile—many shrewd contractors and customers are refusing to do business with firms that do not carry the specialized insurance required to cover the effects of data breaches. It is also possible that a data breach can arise from the negligent installation of software by a computer consultant or vendor. And while you may be able to recover some of your losses through legal action, most vendor contracts contain provisions limiting the vendor's liability for a data breach that prevent you from holding them responsible. Nonetheless, if you experienced a breach or are facing a substantial loss, it will probably be worth your while to have a lawyer help you take the necessary steps to mitigate your risk.

Data breaches are so common these days that it is prudent to think of them in the context of "when," not "if" they will occur. The thieves involved in a data breach are seldom caught, but the affected businesses rarely escape scot-free. The only questions will then be, how much are you liable for, how you will reduce your exposure, and who will bear that cost?

By Margo Brownell, Mike McCarthy, & Joe Ceronsky
Maslon Edelman Borman & Brand, LLP

MASLON

Margo Brownell focuses her practice on insurance coverage counseling and litigation, and has extensive experience representing policyholders in complex insurance disputes.

margo.brownell@maslon.com

Mike McCarthy represents business entities and individuals in appellate and complex business litigation (principally class actions) in areas such as consumer and securities fraud, fiduciary breach, antitrust, and environmental contamination.

mike.mccarthy@maslon.com

Joe Ceronsky practices in the area of general commercial litigation with a focus on insurance litigation and product liability.

joseph.ceronsky@maslon.com

[1] http://www.nytimes.com/2014/01/18/business/a-sneaky-path-into-target-customers-wallets.

[2] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html html?action=click&contentCollection=Business%20Day&module=RelatedCoverage&region=Marginalia&pgtype=article

[3] http://www.symantec.com/content/en/us/about/media/pdfs/b-cost-of-a-data-breach-us-report-2013.en-us.pdf

[4] http://investors.target.com phoenixzhtml?c=65828&p=irol-newsArticle&ID=1903678&highlight=

[5] http://www.businessinsurance.com/article/20140119/NEWS07/301199973#

[6] http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html