For More Information:

Barry Buchman
202.772.2305
buchmanb@gotofirm.com

Mickey Martinez
202.772.3994
martinezm@gotofirm.com

Ellen Katkin
202.772.1960
katkine@gotofirm.com

June 2012

Recent Credit Card Data Breach Once Again Demonstrates Need for Insurance Coverage

By Barry Buchman and Mickey Martinez [1]

Introduction

The recent data breach at Global Payments Inc., which has contracts to handle the processing of credit and debit card transactions, has again focused attention on the significant risk associated with storing or transmitting confidential data.[2] That breach potentially has compromised the accounts of hundreds of thousands of cardholders, and at least one lawsuit regarding the breach already has been filed.[3] Further, between 2005 and 2011, there were over 2,300 data breaches, exposing over 535 million records, at an average cost to the affected firms of $234 per compromised record.[4] The surge in data breaches last year alone caused some commentators to label 2011 "The Year of the Breach."[5]

Moreover, data security is no longer a concern only of large companies.[6] According to a study released last fall, "[t]he vast majority of risk management professionals believe information security and other cyber-related exposures pose a threat to their organization."[7] The problem has become pronounced enough that, in October 2011, the SEC directed publicly-traded companies to disclose the risk of cyber-security breaches if it is reasonably likely that such breaches would have a material financial impact.[8]

Although the first step in avoiding financial harm from a data breach is to ensure that your company has established, and is adhering to, industry best practices for data security, an additional and important means of protection exists in the form of commercial insurance policies. Indeed, in directing publicly-traded companies to disclose cyber-security risks, the SEC noted that it would be prudent to include a "[d]escription of relevant insurance coverage."[9] At least some coverage may be available under policies that many companies already have in place, namely general liability policies, professional liability (errors and omissions) policies, property damage/business interruption policies, and directors and officers policies. Moreover, specialty policies designed to cover cyber-security risks have become increasingly available. These policies may help avoid some of the disputes that have arisen under traditional coverage lines like general liability. Companies should review carefully, with the help of an insurance professional if necessary, the specifics of their insurance policies and how those policies may respond to losses arising from a data breach.[10]

Types of Losses

A company that suffers a data breach that compromises confidential consumer, client, or employee information faces a variety of potential losses. These losses can include the costs of complying with consumer notification laws, and the costs of providing credit monitoring for affected individuals. The potential losses also can include the costs of responding to any government investigations and any resulting fines. Companies also may suffer loss of intellectual property, and damage to, or suspensions of, their online systems and resulting business interruptions. And, companies can face substantial litigation costs, as well as potential judgments or settlements, in connection with third-party lawsuits brought by persons whose data has been compromised. Insurance policies can help offset at least some of these losses.

Coverage Issues Arising Under Traditional Policies

Insurers often dispute whether there is coverage under traditional commercial policies like general liability policies, which are designed to respond to third-party lawsuits brought against the policyholder. For example, insurers often assert that lawsuits brought by individuals whose data has been compromised do not constitute claims for "personal and advertising injury" within the meaning of standard-form general liability policies. The standard "personal and advertising injury" provision typically covers the "[o]ral or written publication, in any manner, of material that violates a person's right of privacy."[11] Insurers may argue, however, that the term "publication" requires a disclosure that is widespread, and that a data breach claim often does not qualify because the data is not disseminated to the general public.

Insurers have likewise disputed whether property damage/business interruption policies cover so-called "first-party" losses arising from data breaches, such as damage to, or interruptions of, an insured company's online systems, and expenses such as the costs of credit monitoring and mandatory consumer notifications. The issue in these disputes typically is whether the insured has suffered "property damage," which is necessary to trigger coverage under the policy, including coverage for business interruption losses and coverage for mitigation expenses such as credit monitoring costs. Such disputes also can arise under liability policies when consumers or other affected third-parties allege that the loss of their credit card information, for example, constituted damage to their property.

Courts have reached different results in these disputes, with policyholders prevailing in several of them.[12] Thus, companies that suffer data breaches should not assume that they do not have coverage under their traditional commercial policies, and they should not accept coverage denials from their insurers at face value.

Instead, companies carefully should review their policies, applicable case law, and the individual circumstances of their data breach, and consult with coverage experts if necessary.

The disputes over these issues are only now proliferating, and additional court decisions are likely. In the past several months, insurers for two large companies have filed lawsuits seeking rulings that there is no coverage for losses arising out of recent data breaches suffered by those companies. Zurich sued Sony seeking a declaration that there is no coverage under Sony's general liability policies for losses resulting from the April 2011 breach involving Sony's PlayStation and Qriocity services, one of the largest data breaches ever.[13] And, Michaels Stores was sued by one of its insurers, which asserts that its general liability policies do not cover losses arising from thefts of customers' credit and debit card numbers.[14]

Further, insurers, in response to pro-policyholder decisions, have begun to constrict their policy language in an effort to preclude coverage for losses arising from data breaches. Some insurers have inserted provisions expressly providing that electronic data is not tangible property for purposes of the "property damage" provisions of their policies, and some insurers have inserted exclusions for claims based on various privacy statutes. However, the scope of privacy statute exclusions remains largely untested, and companies have strong arguments that such exclusions do not bar coverage, at least for litigation costs incurred in defending claims, when the claims allege *both* statutory *and* common law privacy liability.[15]

Standalone Coverage for Cyber Risk

Because of the continued uncertainty surrounding the scope of coverage provided by traditional commercial policies, companies increasingly are looking to cyber-security insurance policies to provide protection from the potential losses associated with data breaches.[16] Such specialty coverage is becoming increasingly available.[17]

The coverage provided by these cyber policies tends to vary more than the coverage available under traditional commercial policies, which are generally based on forms promulgated by organizations like Insurance Services Office, Inc. ("ISO"). For example, some cyber-security insurance policies cover only third-party claims, e.g., ones brought by affected consumers, while others cover the cost of responding to government investigations and any resulting fines, as well as mitigation costs, such as those associated with providing notice to, and credit monitoring for, affected consumers. Other policies may also cover damage to a company's own systems and resulting business interruption losses, and even expenses incurred to deal with public relations issues arising from a breach.

However, companies should examine proposed policy terms carefully to make sure that they understand the true scope of coverage and to avoid potential pitfalls. For example, some cyber policies may preclude coverage where there is evidence, or even allegations, that the company was not sufficiently diligent in protecting against cyber attacks – vague language that could lead to a company simultaneously having to fight both with its insurers, and with third parties who bring claims, about its cyber-security measures. There are also policy forms that purport to preclude coverage for data breaches arising from a computer or other device that was not connected to a network at the time of the breach, such as a laptop or notebook computer, or a mobile device – not uncommon sources of data breaches in recent years. Indeed, both of these types of provisions may be particularly problematic for companies that use cloud computing to store sensitive information, unless that practice is addressed as part of the underwriting process and the policy language is crafted carefully to allow coverage for losses arising out of that practice. Thus, the due diligence involved in purchasing cyber coverage is an area in which it would be particularly valuable to consult with insurance coverage professionals.

Some Important Reminders for Preserving Coverage Rights

Regardless of whether a company has suffered a data breach and any corresponding losses, there are steps that all companies can take now to put themselves in the best possible position to potentially secure insurance coverage if and when the need arises. First, collect and safeguard all of the company's insurance policies, including policies from prior policy periods. Second, consider involving outside coverage counsel to review the organization's current insurance portfolio to confirm that the company has the most complete and cost-effective coverage available. Third, the company should give notice promptly to all of its insurers of any data breach, absent any relatively rare, case-specific circumstances that may justify refraining from giving such notice. Fourth, the company should set up protocols for communicating both internally and externally about any breaches. Because data breaches often involve fluid situations, and because of the nuances in the coverage issues involved, such protocols are important to help protect against inadvertent characterizations regarding the nature or cause of losses, for example, that insurers might use later if a coverage dispute arises. Thus, companies should consider involving their in-house and/or outside counsel in such communications.

Conclusion

The coverage provided by commercial insurance policies can be an extremely valuable corporate asset to companies dealing with cyber-security issues. Companies can maximize the benefits of this asset by acting proactively to analyze their insurance portfolio now, and by being willing to question, and challenge where appropriate, coverage denials from their insurers.

[1] Barry Buchman is a partner, and Mickey Martinez is an associate, in the Washington, DC office of Gilbert LLP, where they represent corporate policyholders in a wide variety of insurance matters.

[2] Robin Sidel and Andrew R. Johnson, *Data Breach Sparks Worry*, WALL ST. J. (Mar. 30, 2012), http://online.wsj.com/article/SB10001424052702303816504577313411294908868.html; Julianne Pepitone and Leigh Remizowski, *"Massive" Credit Card Data Breach Involves All Major Brands*, CNNMONEY (Mar. 30, 2012), http://money.cnn.com/2012/03/30/technology/credit-card-data-breach/index.htm.

[3] Greg Ryan, *Cardholders Sue Global Payments Over Massive Data Breach*, LAW360 (Apr. 6, 2012), http://www.law360.com/articles/327403/cardholders-sue-global-payments-over-massive-data-breach.

[4] Mark Seifert, Joe Carberry, and Brandon Borrman, *Once More Unto The Breach*, BRUNSWICK REVIEW (Winter 2011) at 60, http://www.brunswickgroup.com/files/html/brunswickreviewIssue5/once_unto_breach.html.

[5] Karl S. Vasiloff and Christine T. Phan, *2011 – The Year Of The Breach*, LAW360 (Aug. 8, 2011), http://www.law360.com/articles/262849/2011-the-year-of-the-breach.

[6] Chad Hemenway, *Markel: Data Breaches Not Just Aimed At Large Companies Any More*, PROPERTY CASUALTY 360 (Oct. 12, 2011), http://www.propertycasualty360.com/2011/10/13/markel-data-breaches-not-just-aimed-at-large-comp.

[7] Judy Greenwalk, *Information Security, Other Cyber Exposures Threaten Businesses: Survey*, BUSINESS INSURANCE (Oct. 18, 2011), http://www.businessinsurance.com/article/20111018/NEWS07/111019903.

[8] *SEC Wants Cyber Attack Reports*, INSURANCE NETWORKING NEWS (Oct. 14, 2011), http://fpn.advisen.com/articles/article157706494-81681510.html; *SEC Asks Companies to Disclose Cyber Attacks*, INSURANCE JOURNAL, (Oct. 14, 2011), http://www.insurancejournal.com/news/national/2011/10/14/220050.htm.

[9] *See* CF Disclosure Guidance: Topic No. 2 (Oct. 13, 2011), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm.

[10] This article provides an overview of general principles and a non-exhaustive set of examples of the issues and arguments that may arise. Actual legal advice should be based upon an evaluation of all the facts and circumstances, including specific policy language and the law of the pertinent jurisdiction(s).

[11] Jean-Paul Jaillet, *Insurance Coverage For Cyber-Risky Business*, LAW360 (Feb. 21. 2012), http://www.law360.com/articles/311174/insurance-coverage-for-cyber-risky-business.

[12] *See, e.g., Norfolk & Dedham Mut. Fire Ins. Co. v. Cleary Consultants, Inc.*, 958 N.E.2d 853 (Mass. App. Ct. 2011) (transmittal of employee's private information to co-workers satisfied "personal and advertising injury" provision of general liability policy); *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797, 802, 804 (8th Cir. 2010) (underlying lawsuit was covered under both general liability policy and technology errors and omissions policy); *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185 TUC ACM, 2000 U.S. Dist. LEXIS 7299 (D. Ariz. Apr. 18, 2000) (loss of data on computer system constituted physical "property damage" under property damage/business interruption policy, even though computer that housed data still functioned).

[13] John Doernberg, *Sony and Dropbox Cases Highlight Cyberliability Insurance Coverage Issues*, WGA INSUREBLOG (Aug. 15, 2011), http://blog.wgains.com/2011/08/15/sony-and-dropbox-cases-highlight-cyberliability-insurance-coverage-issues/.

[14] Carla Salvatore, *Michaels' Insurer Sues Over Card Data Theft Coverage*, LAW360 (Feb. 6, 2012), http://www.law360.com/articles/306606/michaels-insurer-sues-over-card-data-theft-coverage.

[15] *See, e.g.*, Allison Grande, *TCPA Exclusions Not Enough To Avoid Text Blasting Claims*, LAW360 (Feb. 15, 2012), http://www.law360.com/articles/300837/tcpa-exclusions-not-enough-to-avoid-text-blasting-claims.

[16] *See, e.g.*, Bibeka Shrestha, *Cos. Eye Data Breach Policies as CGL Exclusions Multiply*, LAW360 (Mar. 13, 2012), http://www.law360.com/articles/308403/cos-eye-data-breach-policies-as-cgl-exclusions-multiply.

[17] Nicole Perlroth, *Insurance Against Cyber Attacks Expected To Boom*, N.Y. TIMES (Dec. 29, 2011), http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/; Rodd Zolkos, *Cyber Liability Insurance Market Maturing*, BUSINESS INSURANCE (Sept. 13, 2011), http://www.businessinsurance.com/article/99999999/NEWS070101/399999950.