CLM 2016 Cyber Liability Summit
October 5, 2016 in New York City

Handling Cyber – An Insider Look at the Real World of Managing the Resolution of a Cyber Claim

First Party Costs

Privacy breach expenses coverage (sometimes called Privacy Event Management) affords coverage for costs incurred directly as a result of a Privacy Incident so long as the incident occurs during the policy period. Since these costs can be specific, insurers will often specifically define what is included within the policy's definition of "expenses". One policy defines these costs as:

> [R]easonable and necessary fees, costs, charges and expenses incurred by the Company in the event of a Privacy Incident for the purposes of retaining an accountant, attorney, public relations consultant or other third party to:
>
> 1. gain access to a privacy breach coach … to create a privacy breach response plan to:
>
> (a) determine if the Insured is obligated to notify affected individuals or applicable government agencies of such Privacy Incident;
> (b) examine the Insured's indemnification rights and obligations under any written contract with respect to a Wrongful Act by the Service Provider in connection with such Privacy Incident; and
> (c) review compliance with any Privacy Regulation under the applicable Privacy Regulation most favorable to the individuals affected by such Privacy Incident;
>
> 2. conduct a computer forensic analysis to investigate the Insured's Computer System to determine the cause and extent of such Privacy Incident. Such forensic expenses shall be sub-limited to the amount stated on the Declarations Page of this Policy, Section 4D;
> 3. plan, implement, execute and manage a public relations campaign to counter or
> minimize any actual or anticipated adverse effects of negative publicity from such
> Privacy Incident or to protect or restore the Insured's business reputation in response to negative publicity following such Privacy Incident;
> 4. notify the Insured's affected clients and customers and applicable government agencies of such Privacy Incident and establish new account numbers for the Insured's affected clients and customers, with prior written consent by the Insurer, such consent not to be unreasonably withheld;

5. procure identity monitoring, credit monitoring, call center and identity restoration services for individuals affected by such Privacy Incident with the prior written consent of the Insurer, such consent not to be unreasonably withheld.
6. procure credit freezes and/or credit thaws sealing and/or unsealing credit reports for individuals affected by such Privacy Incident with the prior written consent of the Insurer, such consent not to be unreasonably withheld.
7. reimburse the Company for monetary assessments, contractual fines and penalties levied by a card association against the Company where insurable by law, as the direct result of such Privacy Incident with the prior written consent of the Insurer, such consent not to be unreasonably withheld.

Privacy Breach Expenses do not include:

1. remuneration, salaries, wages, fees, expenses, overhead or benefit expenses of any Insured;
2. any cost or expenses incurred to update, restore, replace, modify or otherwise improve Digital Assets or any Computer System of the Company to a level beyond that which existed just before the Interruption in Service or Loss event;
3. any costs or expenses to correct any deficiencies, identify or remediate Software errors or vulnerabilities, or costs to update, replace, modify, upgrade, restore, maintain or improve any security system or Computer System of the Company;
4. any expense incurred to research and develop Digital Assets, including trade secrets;
5. the economic or market value of Digital Assets, including trade secrets;
6. loss arising out of liability to any third party.

Importantly, notice how privacy breach expenses do not include "betterment" meaning that the policyholder cannot end up with a better network or system than what it originally had before the breach.

Investigation of a Network Breach

The primary focus of an investigation is to confirm the indicated avenue of the event and identify the post event network activity related to system infiltration and data exfiltration. Additionally, the compromise investigation identifies additional compromised endpoints and user accounts.

- Understand potential breadth and scale of the incident
- Identify locations of potentially compromised systems
- Identify and examine logs available for the incident
- Determine any priority systems or logs with a tier based system for further collection and examination
- Identify if an immediate, remote assessment or collection is required.

Damage Assessment

The damage assessment focuses on ascertaining the data accessed or exposed, as well as providing an understanding of what the adversary sought, and what relevant issues will need to be addressed in future actions. The damage assessment can also provide further guidance on the impact of the data exfiltration on the victim's operations.

- Files accessed
- Indicators of file use and adversary intelligence gathering
- Files potentially or actually exfiltrated
- Adversary's next steps

The PCI Forensic Investigation

The PCI Forensic Investigator (PFI) program establishes and maintains rules and requirements regarding eligibility, selection and performance of companies that provide forensic investigation services to ensure they meet PCI Security Standards. The PFI program aims to help simplify and expedite procedures for approving and engaging forensic investigators by:

- Providing a single set of requirements for forensic investigators upon which market participants may align
- Maintaining a list of Council-approved forensic investigators for compromised entities to choose from
- Providing guidance on how investigations are to be conducted and reported

While your client or insured pays for the PFI, the PFI reports to the PCI and is not looking out for your client or insured's best interests.

Role of Breach Counsel

A significant concern of organizations is that the written reports generated at the culmination of security risk assessments, whether conducted internally or by an external party, may provide a roadmap for an adversary in some future proceeding. It is important for organizations seeking to protect such reports from unwanted discovery.

Organizations can attempt to cloak a risk assessment from disclosure by employing legal counsel to manage the review process.

In this scenario, Breach Counsel would be retained by the organization to provide legal advice regarding data security exposures, and to develop a strategy for risk minimization. As part of this process, counsel, rather than the organization, would retain an independent cyber consultant to assist in the due diligence analysis and in the preparation of a cyber risk assessment report detailing the organization's vulnerabilities, threats and lack of controls, as well as recommendations for addressing these issues. The report would be addressed to counsel, which would then be incorporated into a more comprehensive report for the organization.

Cyber Extortion

Coverage for cyber extortion traces its historical root to traditional “crime” insurance and certain ambiguities when crime policy provisions were applied in the cyber context.

Cyber extortion coverage affords coverage for expenses incurred as a result of an extortion event or a security event. These are typically defined terms in a cyber policy. Consider the following definitions related to cyber extortion:

> “[S]ecurity Threat" means any threat or connected series of threats to commit an intentional attack against a Computer System for the purpose of demanding money, securities or other tangible or intangible property of value from an Insured.
>
> *** *** ***
>
> “Network Extortion Threat” means a credible threat or connected series of credible threats made by a natural person to an Insured where such natural person:
>
> 1. introduces or threatens to introduce Malicious Code into the Company's Computer System;
> 2. interrupts or threatens to interrupt the Company's Computer System through a Denial of Service Attack; or
> 3. disseminates, divulges, or improperly utilizes or threatens to disseminate, divulge or improperly utilize any Non-Public Personal Information or Confidential Corporate Information obtained from the Company's Computer System.
>
> *** *** ***
>
> “Cyber Extortion Threat” means an Event triggered by any credible threat or series of related threats by anyone other than a principal, officer, partner or director of the Named Insured or by anyone other than someone induced or assisted by a principal, officer, partner or director of the Named Insured, including the demand for Cyber Extortion Loss, which actually affects or threatens to negatively affect the Named Insured's Computer System or Website by means of, including but not limited to, a breach of the Named Insured's Security Systems; the proliferation of Malicious Code; a Denial of Service Attack; or theft or unauthorized use of the Named Insured's Data Assets. Cyber Extortion Threat does not include Privacy Breaches, Data Assets Breaches, any other Event or any Error. A Cyber Extortion Threat does not mean or include any Claim.

Electronic Business Interruption

As we constantly set forth above, businesses today are nearly entirely dependent on computers and networks to maintain their respective operations. We earlier discussed that while there has always been first party insurance coverage available for “business interruption,” there were many uncertainties left to the policyholder when traditional business interruption policies were applied in the cyber context.

Similar to other coverages, the scope of coverage depends entirely on the particular policy definitions relevant to this risk. Because claims for business interruption can tend to be creatively asserted to emphasize a businesses profitability, insurers tend to underwrite this risk with great caution and specifically and narrowly define the scope of coverage. Consider the following examples.

This policy covers the "loss" caused by a network interruption. Important, "loss" is limited to costs incurred within 120 days after the end the business interruption and limited to:

(1) costs that would not have been incurred but for a Material Interruption; and

(2) the sum of all of following, which shall be calculated on an hourly basis:

(a) Net Income (Net Profit or Loss before income taxes) that would have been earned; and

(b) Continuing normal operating expenses incurred, including payroll.

Other policies similarly define the interruption loss as net profits or losses plus expenses. Examine how the following definition then limits the scope of what is covered.

Business Interruption Income Loss does not include:

(a) any cost or expenses incurred to update, restore, replace, modify or otherwise
improve Digital Assets or any Computer System of the Company to a level beyond that which existed just before the Interruption in Services or Loss event;

(b) any costs or expenses to correct any deficiencies, identify or remediate Software errors or vulnerabilities, or costs to update, replace, modify, upgrade, restore, maintain or improve any security system or Computer System of the Company;

(c) any expense incurred to research and develop Digital Assets, including trade secrets;

(d) the economic or market value of Digital Assets, including trade secrets;

(e) loss arising out of liability to any third party;

(f) any contractual penalties;

(g) any Claim, Claim Expenses, Damages, Digital Asset Expenses, Extortion Payments, Extortion Expenses, Extra Expenses, Network Extortion Threat, Network Security Incident, Privacy Breach Expenses, Privacy Incident or Regulatory Proceeding; or

(h) any other consequential loss or damage.

Third Party Issues

Litigation & Article III Standing

On April 14, 2016, the Court of Appeals for 7th Circuit reinstated plaintiffs' action against P.F. Chang's restaurant chain that arose out of the well-reported breach of payment card information. The action was previously dismissed by the District Court for the Northern District of Illinois, Eastern Division, on the basis of what the lower Court ruled was the plaintiffs' lack of Article III standing.

As this Blog has discussed, P.F. Chang's notified its customers of a PCI data breach in June 2014. Plaintiff Kosner dined at the P.F. Chang's restaurant in Northbrook, Illinois. Some time later he incurred fraudulent credit card charges and associated them with the P.F. Chang's breach.

Kosner cancelled the credit card in question and retained a credit monitoring company to monitor his accounts. Plaintiff Lewert also dined at P.F. Chang's in Northbrook, IL, but did not incur fraudulent charges. He monitored his card statements and credit reports for any fraudulent charges himself.

Kosner and Lewert sought to represent a class action of P.F. Chang's customers who paid with credit cards and whose data may have been stolen. The District Court previously dismissed their claim based upon lack of standing and the plaintiffs appealed.

Article III of the Constitution requires plaintiffs to show that they "suffered a concrete and particularized injury that is fairly traceable to the challenged conduct, and is likely to be redressed by a favorable judicial decision." *Hollingsworht v. Perry*, 133 S. Ct. 2652, 2661 (2013). In reversing the District Court's dismissal, The 7th Circuit Court of Appeals found that Plaintiffs meet constitutional standing requirements and remanded the matter for further proceedings.

In reaching its decision, the Court expressly relied upon its prior decision *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). In *Remijas*, the 7th Circuit Court of Appeals found that customers whose data was breached suffered sufficiently concrete and particularized injuries under Article III to support standing. The injuries identified by the Remijas Court were an increased risk of fraudulent charges and an increased risk of identity theft.

The Court of Appeals found that Remijas' alleged injuries were "certainly impending" – the future harm required to establish standing. The Court noted that the customers should not have to wait until hackers commit identity theft or credit card theft in order to have standing because "objectively reasonable likelihood" exists that such injury will occur. The Court also found that the time and money spent resolving fraudulent charges and identity theft were sufficient injuries for purposes of standing.

Applying the foregoing reasoning, the Appellate Court concluded that because Plaintiffs' credit card data had already been stolen, the injuries to Kosner and Levert fall under the same categories as set forth in Remijas – increased risk of identity theft and credit theft. The 7th Circuit also found that Plaintiffs already suffered sufficient injuries to convey standing in the form of fraudulent charges and credit monitoring.

As to the remaining criteria for standing, causation and redressability, the Court also found in favor of the Plaintiff determining with respect to causation that while a dispute exists as to the extent of the breach, that in itself does not destroy standing and will be the subject of discovery during litigation. With regard to redressability, the Court found that a favorable judgment would compensate Plaintiffs for their injuries via reimbursement of costs related to credit monitoring, and loss of accrual of points on the credit card while awaiting its replacement.

Courts are now squarely pitted in different directions on this issue and the Spokeo case – where the U.S. Supreme Court may decide whether Article III standing is conferred upon a plaintiff who suffers no concrete harm, and could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on the mere violation of a federal statute – is still outstanding.