FINTECH LAW REPORT
E-Banking, Payments & Commerce in the Mobile World
Mar/Apr 2014 ■ Volume 17 ■ Issue 2

Thoughts on Cyber Security—Liability, Damages & Insurance

BY ALAN FRIEDMAN, MARK F. MEYER, ARTHUR H. ROSENBLOOM & HOWARD SCHNEIDER

The authors are economists and consultants with Charles River Associates. Collectively, they have decades of experience advising companies on litigation, regulatory, and financial-related matters. Alan Friedman has 25 years of financial consulting experience and has provided expert testimony in numerous complex commercial litigations in federal and state courts, arbitrations, and mediations. Dr. Mark F. Meyer has more than 20 years of experience applying economic theory and quantitative methods to a range of complex business litigation and regulatory matters. Arthur H. Rosenbloom has more than 40 years of experience providing valuation and litigation support to companies. He has also provided expert testimony on executive compensation, securities fraud, and other financial issues. Howard Schneider has extensive legal and consulting expertise in derivatives/futures, corporate, and securities issues. He has been legal counsel in both the derivatives/futures and securities fields, as well as in general corporate, mergers and acquisitions, corporate governance, and legal ethics matters. *The authors acknowledge, with thanks, the assistance provided by Jason Sugarman, an Analyst at Charles River Associates, and Keith Palumbo, Esq., Vice President, Legal Affairs of Cylance, Inc., in the preparation of this article.*

There is little question today that individuals and businesses[1] (which, in this context, we call "Potential Victims") face meaningful cyber security exposures.[2] While the headlines today go to the credit card victims at major retailers and other businesses, there are numerous, less visible attackers and victims. Cyber security breaches can be initiated by: (*i*) criminals trying to monetize information, such as credit card data, or maliciously interfering with the Potential Victim's systems;[3] (*ii*) entities on their country's behalf (a number located outside of the U.S.) engaging in commercial espionage; or (*iii*) internal personnel or practice lapses.

Potential Victims can suffer first-party damages, such as the expense of cleaning up after the breach, loss of company confidential information, and loss of business. More worryingly, the Potential Victim of a cyber security breach often finds that the interests of third-parties may have been compromised by the cyber breach by:

- The disclosure of information that, in the hands of criminals, exposes third parties to fraud (the most prominent of which is loss of "Personally Identifiable Information" or PII) contained in financial, personnel, and health records);

CONTINUED ON PAGE 3

Article REPRINT

Reprinted from the Futures & Derivatives Law Report. Copyright © 2014 Thomson Reuters. For more information about this publication please visit www.west.thomson.com

WEST®

West LegalEdcenter

LOG ON.
LOOK UP.
LEARN.

Quality legal training and
CLE - online, anytime

westlegaledcenter.com
1.800.241.0214

WEST®
Part of Thomson Reuters

© 2014 Thomson Reuters. This publication was created to provide you with accurate and authoritative information concerning the subject matter covered, however it may not necessarily have been prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651)687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

For subscription information, please contact the publisher at: west.legalworkspublications@thomson.com

Editorial Board

EDITOR-IN-CHIEF:
GREGG WIRTH
Legal Insights & Analytics
Thomson Reuters

CHAIRMAN:
DUNCAN B. DOUGLASS
Partner & Head, Payment Systems Practice
Alston & Bird LLP
Atlanta, GA

MEMBERS:
DAVID L. BEAM
Partner
K & L Gates LLP
Washington, DC

ROLAND E. BRANDEL
Senior Counsel
Morrison & Foerster LLP
San Francisco, CA

RUSSELL J. BRUEMMER
Partner & Chair, Financial Institutions Practice
Wilmer Hale LLP
Washington, DC

ELLEN D'ALELIO
Of Counsel
Steptoe & Johnson
Washington, DC

CHRIS DANIEL
Partner & Chair, Payment Systems Practice
Paul Hastings LLP
Atlanta, GA

RICHARD FRAHER
VP & Counsel to the Retail Payments Office
Federal Reserve Bank
Atlanta, GA

GRIFF GRIFFIN
Partner
Sutherland Asbill & Brennan LLP
Atlanta, GA

PAUL R. GUPTA
Partner
DLA Piper LLP
New York, NY

ROB HUNTER
Executive Managing Director & Deputy
General Counsel
The Clearing House
Winston-Salem, NC

SYLVIA KHATCHERIAN
Managing Director
Legal Department
Morgan Stanley

MICHAEL H. KRIMMINGER
Partner
Cleary, Gottlieb, Steen & Hamilton
Washington, DC

ANDREW OWENS
Partner
Davis Wright Tremaine
New York, NY

JANE E. LARIMER
Exec VP & General Counsel
NACHA—The Electronic Payments Assoc
Herndon, VA

KELLY MCNAMARA CORLEY
Sr VP & General Counsel
Discover Financial Services
Chicago, ILL

C.F. MUCKENFUSS III
Partner
Gibson, Dunn & Crutcher LLP
Washington, DC

STUART G. STEIN
Partner & Global Co-Head,
Corporate Practice
Hogan Lovells LLP
Washington, DC

R. JASON STRAIGHT
Sr VP & Chief Privacy Officer
UnitedLex
New York, NY

DAVID TEITALBAUM
Partner
Sidley Austin LLP
Washington, DC

RICHARD M. WHITING
Executive Director & General Counsel
The Financial Services Roundtable
Washington, DC

DAMIER XANDRINE
Senior Counsel
Wells Fargo & Co
San Francisco, CA

Fintech Law Report
West LegalEdcenter
610 Opperman Drive
Eagan, MN 55123

© 2014 Thomson Reuters

One Year Subscription ■ 6 Issues ■ $752.04
(ISSN#: XXXX)

For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, USA (978) 750-8400; fax (978) 646-8600 or West's Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651) 687-7551. Please outline the specific material involved, the number of copies you wish to distribute and the purpose or format of the use.

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered. However, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdication. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

Copyright is not claimed as to any part of the original work prepared by a United States Government officer or employee as part of the person's official duties.

CONTINUED FROM PAGE 1

- The misappropriation of competitively sensitive information from customers or suppliers; or
- The loss of services that the Potential Victim is contractually obligated to provide to others.

The costs of cyber security breaches can be significant. An analysis found that the average total cost of a data breach in the U.S. in 2012 was more than $5.4 million dollars, with an average cost per record breached of approximately $190.[4]

The purpose of this article is to provide some thoughts to those advising Potential Victims impacted by cyber-attack from four perspectives: (*i*) understanding the nature of claims made against those Potential Victims because of assertions that they improperly disclosed customer confidential information (including PII) as part of their business or, due to a breach of the Potential Victim's computer networks; (*ii*) initiating actions against identifiable credit-worthy perpetrators of the breach or, without regard to the defendant's credit standing, enjoining the perpetrators' activities; (*iii*) damage theories and how cyber case damages might be computed; and (*iv*) ideas relating to cyber insurance as a means by which to transfer cyber security risks.

Our analysis leads us to believe that:

1. Liability questions and defenses are currently being shaped in class actions and Potential Victims are not without remedies against hackers.
2. Damages can be measured on the basis of well-known common law theories applicable in civil litigation generally.
3. Cyber security insurance, as a means to mitigate damages, is in its infancy and has the potential to grow dramatically.

Liability

Litigation and the Role of Class Actions

Some of the cases brought against Potential Victims are class actions, asserting that the Potential Victims improperly disclosed customer or subscriber PII to others in violation of various Federal statutes[5] (or simply because their cyber security systems were insufficiently robust) and common law theories.[6] To the extent these cases survive motions to dismiss and a class is certified, outcomes will often depend on the contractual disclosures made to customers of the potential uses to which the customers' information might be put.

Class actions help frame these issues.[7] In recent examples against large retailers, plaintiffs cite not only insufficiently robust cyber security systems, but also defendants' failure promptly to notify card-holders of the hacking incident. The second of their two allegations has not been lost on the retail community. We are seeing examples now of retailers warning their customers of a possible attack on their data security before undertaking a fuller investigation.[8]

Litigation by Potential Victims

Potential Victims can go on the offensive against their hackers. The major difficulty is the technological ability to trace the parties who inflicted the damage. However, governmental agencies such as Homeland Security, Federal Energy Regulatory Commission (FERC), the Secret Service, and the FBI can help. After an attack, it would likely be prudent to seek advice from appropriate governmental agencies. There are also private company professionals with the capacity to trace intruders back to their source.[9] If the intruders are going concerns or state-sponsored operations, the potential for a lawsuit to recover damages exists. If a state-sponsored operator is involved, it would be advisable to consult with the State Department. Suits in the U.S. against state-sponsored actors may be possible only if a Potential Victim can establish jurisdiction under one or more of the exceptions to sovereign immunity set forth in the United States Sovereign Immunities Act.[10]

One possible approach, a lawsuit by a Potential Victim against the hackers for injunctive relief to prevent future invasions of the Potential Victim's computer systems, is exemplified by a case brought by LinkedIn Corp.,[11] which seeks to enjoin unidentified hackers into its systems to prevent further breaches of such systems. LinkedIn asserts a variety of statutory and common law

© 2014 THOMSON REUTERS

claims including breach of contract, trespass and misappropriation.

Another approach, where the Potential Victim's objective is damages and not injunctive relief, the ultimate business questions for a Potential Victim may be: (*i*) whether the action would adversely affect the Potential Victim's other business relationships in the state-sponsoring country; (*ii*) the time and complexity such a lawsuit will entail; and (*iii*) the collectability of a judgment at the end of the process, should the Potential Victim prevail.

More specifically, in today's global marketplace, a Potential Victim has to decide whether a lawsuit against a state-sponsored actor will detrimentally affect its other significant business relationships with the state actor, such as, for example, in China or Russia. Moreover, the U.S. State Department, for policy reasons, may oppose suits against certain sovereign entities. At the end of the day, this will be a cost/benefit question for the Potential Victim to sort out.

Lawsuits can go on for years. In this situation, the difficulty of proof in tracing the cyber activity back to the defendants is compounded by questions of foreign entities conducting business in the U.S. via cyber space, sovereign immunity, and the overall complexity and novelty of the issues before the court. This type of case could drag on well beyond the ordinary commercial case in a federal court. Again, the plaintiff will have to decide whether the time, effort, and cost is worth the potential for relief of whatever type might be contemplated—monetary, declaratory, or injunctive.

If the objective is neither deterrent nor protective, and the Potential Victim seeks to recover its losses, the question of collectability of a judgment looms large. Obviously, if an investigation cannot tie the hackers to a commercial or state-sponsored entity, there is little chance that the hackers will have independent means by which to satisfy a judgment. Thus, collection of monetary damages would be futile. Again, this is a call that the Potential Victim needs to weigh at inception.

A Potential Victim would be well advised to have its data categorized and available to the professionals it will call upon to assist it in making its cyber system more resistant to hackers or provide damage control should a breach occur.

One can confidently predict a substantial increase in the kinds of cases brought, dismissed and settled. Ultimately, some of these will be tried, providing a body of case law by which counsel to the Potential Victims may provide informed advice, defenses and what works best when going on the offense. Given today's climate, additional legislation at the federal and state levels of the sort currently contemplated seem likely to be enacted.

Damages

In this section, we present various approaches to determining damages in situations in which the Potential Victim has been the subject of a cyber-attack by a hacker. We will not discuss criminal prosecutions for cyber-theft, although they are plentiful, nor discuss damages related to other cyber-related events, such as those caused by employee carelessness (*e.g.* leaving the Human Resources laptop on the train), or government agency compliance actions (*e.g.* the Federal Trade Commission for failing to document or install proper security procedures for PII). Such happenings are certainly serious and not uncommon, but outside the scope of our discussion.

The maintenance of detailed records by the Potential Victim before, during, and after a cyber-security breach is vital to an accurate measure of damages.

Focusing on hacker/Potential Victim situations, we identify four basic scenarios and a damages approach for each. These scenarios include:

1. The Malicious Hacker who breaks into the Potential Victim's systems to disrupt its business activities.
2. The Hacker Thief who breaks into the Potential Victim's systems to steal valuable third-party information, such as retail customer credit or debit card for PII.
3. The Competitor Hacker who steals the Potential Victim's customer, product, or process data for competitive purposes.
4. The One-Off Competitor Hacker who steals information pertaining to the Potential Victim's upcoming transaction or contract bid information.

© 2014 THOMSON REUTERS

Each of these scenarios can cause serious damage. Assuming liability, a credit-worthy defendant, a recovery net of insurance proceeds and without double-counting, we now examine approaches to measuring those damages in a litigation setting:

1. **Malicious Hacker**—Since the Malicious Hacker has damaged the Potential Victim's cyber system, the Potential Victim can seek general damages equal to the:

   Costs to investigate, identify and repair the damage to its systems and data files (general damages), plus consequential damage that includes the Potential Victim's lost profits resulting from the interruption to its business and lost profits on revenues that would have been achieved but for the hacking. For example, consider damages to an airline whose computers were hacked resulting in its inability to sell seats and the likelihood of grounded flights. In addition to the lost profits from lost ticket sales, one could also include the cost of replacing credit or debit cards compromised by the hacking, although such a suit could more logically be brought by banks and credit card users against Potential Victims.

2. **Hacker Theft**—Since the Hacker has stolen third-party (*e.g.*, customer) data, the Potential Victim's customers could have been, or are, at risk of being damaged due to improper use of that information. In addition, the Potential Victim itself has likely suffered increased costs, a loss of reputation, and the resulting lost revenues and profits. The damages that the Potential Victim could seek from the Hacker include:
   a. the costs to investigate, identify and repair the damage to its systems and data files (and/or the potential cost of the replacement of credit cards compromised by the hacking);
   b. the costs to repair its diminished reputation with its customers through advertisements, giveaways, free credit protection services and other inducements required to retain them; and
   c. reimbursement for reasonable costs related to the defense of lawsuits from the Potential Victim's customers or its shareholders in class actions or derivative suits.[12] These costs may include actual damages incurred by the Potential Victim to settle, or try its case with its customers. Here, the Potential Victim should be able to demonstrate that these costs are reasonable and were not incurred improvidently.

3. **Competitive Hacker (Customers or Products)**—The Hacker in this scenario is the Potential Victim's competitor, who appropriates the Potential Victim's customer or proprietary product data in order to benefit its own business. In addition to the costs associated with unauthorized system access, the Potential Victim is damaged due to the loss of its customer and product information and likely revenues and profits from that loss. On that basis, additional damages to the Potential Victim may be seen as the theft of trade secrets, resulting in damages that would include:
   a. the costs to investigate, identify and repair the damage to its systems and data files;
   b. Hacker's unjust enrichment from appropriating the Potential Victim's customer or product data, which allowed Hacker to add new customers or enjoy additional revenues from customers in common with its Potential Victim's competitor. This information might include pricing, quantities, specifications, special services provided or the Potential Victim's trade secrets from its proprietary product data. The quantification of that additional profit would usually involve identification of customer or product revenue switching from the Potential Victim to Hacker, or new customers from other competitors, and the higher profit margins achieved by Hacker;
   c. Hacker's future unjust enrichment can also be estimated based on the historical

© 2014 THOMSON REUTERS

retention rate of similar customers and product life and past sales trends. After applying the incremental profit margins, that future stream of earnings could be discounted at an appropriate weighted average cost of debt and equity capital in order to estimate the present value of that future stream of earnings for damage purposes;

d. if Hacker sells the business unit that benefited from the theft or simply sells the stolen data after increasing its revenues and profits, it may be possible to estimate the gain in value of the business unit due to Hacker's actions. This would be in lieu of the stream of future lost profits after the sale date. Damage causation questions may provide challenges to Potential Victims in this circumstance;
e. the lost profits of the Potential Victim due to the loss of customers, products and revenues to third-party competitors. This element may only be relevant if losses are not duplicative of other damage claims;
f. future lost profits of the Potential Victim, which could be computed based on the historical retention rate of similar customers and products' past sales trends. After applying the incremental profit margins, that future stream of earnings could be discounted at an appropriate weighted average cost of debt and equity capital in order to estimate the present value of that future stream of earnings for damage purposes; and
g. if the Potential Victim actually sells its affected business unit or simply sells stolen data after suffering the loss of revenues and profits due to the activities of the Hacker, it might be possible to estimate the loss in value of the business unit due to Hacker's theft. This concept may be allowed in place of the future lost profits after the sale date but, will suffer the same challenges as those noted in example *d*. above in which the malefactor was the Hacker.

An alternative way to measure the Potential Victim's lost profits or Hacker's unjust enrichment is to ascribe a reasonable royalty to the stolen technology, especially if the stolen technology (or similar technology) has been licensed in the past.

Reasonable royalties are recoverable by plaintiffs in those jurisdictions that have adopted the Uniform Trade Secrets Act. The Restatement (Third) of Unfair Competition defines the term "reasonable royalty" as "the price that would be set by a willing buyer and a willing seller for the use made of the trade secret by the defendant." Thus, a method by which a reasonable royalty may be computed is to consider a hypothetical negotiation between a willing licensor and a willing licensee. The royalty is based on the commercial considerations existing at that time.[13] To calculate reasonable royalties either as liquidated damages or as actual periodic royalty payments, practitioners customarily search for royalties paid for similar kinds of intellectual property (a market approach), the benefits derived by a holder of that property (an income approach) or the cost of designing a competitive alternative product (a cost approach). In the case of liquidated damages, the royalty rate established is multiplied by the number of units of the purloined products sold by defendant.

4. **One-Off Competitor Thefts**—In this scenario, Hacker is a competitor who steals the Potential Victim's bid data for a large order of widgets to be sold to a customer of the Potential Victim that Hacker would like to win. Or, Hacker steals the Potential Victim's bid data for an acquisition prospect that Hacker also wishes to buy. As a result of this illicit activity, Hacker is successful in obtaining the order or completing the M&A transaction instead of the Potential Victim. In this case, the Potential Victim has claims that could include:
   a. the costs to investigate, identify and repair the damage to its systems and data files;

© 2014 THOMSON REUTERS

b. the Hacker's present and future unjust enrichment;
c. Hacker's gain on sale of information or business unit (if applicable);
d. the Potential Victim's present and future lost profits; and
e. loss on sale of the Potential Victim's business unit (if applicable).

In the case in which an acquisition transaction was lost to the Hacker, the analysis could account not only for the direct benefits of the transaction, but also for synergistic benefits of the transaction which either accrued to the Hacker (unjust enrichment) or which were lost to the Potential Victim (lost profits). Ideally, this will be based on the acquired company's actual post-acquisition performance, adjusted appropriately, and discounted at an appropriate discount rate to the relevant date in order to determine the present value of the amounts claimed. Of all of the damage theories described, the synergy loss is the one most likely to be challenged.

The damage approaches shown above are surely not an exhaustive list, but rather present some common approaches used to compute and present damages, and the data to consider mining and collecting in order to carry out those computations and presentations. Clearly, the laws in each jurisdiction in which cases may be brought will influence the selection of approaches that will be deemed admissible.

Insurance—Is It Available? What Does It Cover? What Does It Cost?

As a result of actual and threatened cyber-events, insurance products have been created to respond to them. Since they come in a variety of forms and coverage levels, it is important to understand existing offerings and the degree to which they can mitigate the negative effects of a cyber-attack.

As shown above, the risks posed by breaches of cyber-security have not been lost on the insurance industry and are a prominent and growing concern to Potential Victims.[14]

The danger posed by cyber-security breaches can be both extensive and expensive. The Potential Victims can suffer losses of equipment, intellectual property, confidential information, access to business records and social media, and business interruption or diversion of time to remediate. While data breaches arising from malicious cyber-attacks often dominate the news coverage, research shows that this type of cyber event constituted 37% of the 2012 data breaches, while 35% are due to a negligent employee or contractors and 29% involve system problems that included both IT and business process failures.[15]

First-party losses due to cyber-security breaches have, in some cases, been covered under traditional commercial property, business owners, or business interruption insurance.[16] There have also been attempts to claim for losses to third parties under commercial liability or directors' and officers' (D&O) coverage.[17] Starting in the late 1990s, specialist cyber insurance policies have been developed and offered as stand-alone coverage.[18] "Each policy is tailored to the specific needs of a company, depending on the technology being used and the level of risk involved. Both first- and third-party coverages are available."[19] Cyber-risk coverage might include:

- **Loss/Corruption of Data**—Covers damage to, or destruction of, valuable information assets as a result of viruses, malicious code and Trojan horses.
- **Business Interruption**—Covers loss of business income as a result of an attack on a company's network that limits the ability to conduct business, such as a denial-of-service computer attack. Coverage also includes extra expenses, forensic expenses and dependent business interruption.
- **Liability**—Covers defense costs, settlements, judgments and, sometimes, punitive damages incurred by a company as a result of:
  - breach of privacy due to theft of data (such as credit cards, financial or health related data);
  - transmission of a computer virus or other liabilities resulting from a computer attack, which causes financial loss to third parties;

© 2014 THOMSON REUTERS

- failure of security which causes network systems to be unavailable to third parties; and
- allegations of copyright or trademark infringement, libel, slander, defamation or other "media" activities in the company's website, such as postings by visitors on bulletin boards and in chat rooms. This also covers liabilities associated with banner ads for other businesses located on the site.

- **D&O/Management Liability**—Newly developed and specially tailored D&O products that include liability risks faced by directors, including cyber risks, are covered.
- **Cyber Extortion**—Covers settlement of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down and negotiate with blackmailers.
- **Crisis Management**—Covers the costs to retain public relations assistance or advertising to rebuild a company's reputation after an incident. Coverage is also available for the cost of notifying consumers of a release of private information, as well as the cost of providing credit-monitoring or other remediation services in the event of a covered incident.
- **Criminal Rewards**—Covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of a cyber-criminal who has attacked a company's computer systems.
- **Data Breach**—Covers the expenses and legal liability resulting from a data breach. Policies may also provide access to services helping business owners to comply with regulatory requirements and to address customer concerns.
- **Identity Theft**—Provides access to an identity theft call center in the event of stolen customer or employee personal information.
- **Social Media/Networking**—Insurers are looking to develop products that cover a company's social networking activities under one policy. Some cyber policies now provide coverage for certain social media liability exposures such as online defamation, advertising, libel and slander.[20]

Although the market has "grown 80% in the past three to four years," estimated premiums were still a modest $1 billion in 2012.[21] In late 2013, there were around 40 insurers and Lloyd's syndicates offering cyber-insurance coverage.[22] Despite recognizing the risks posed by breaches of cyber security, surveys indicate that only 20% to 30% of U.S. firms purchase cyber coverage and non-US coverage is even lower.[23] Recent events, however, seem to have prompted a spike in the demand for cyber coverage—at least in the U.S.—and cyber coverage among the larger, more exposed firms is thought to be much more prevalent.[24]

The economic terms of cyber coverage are quite varied and still evolving. As an A.M. Best briefing states:

> **The range of exposures continues to evolve rapidly. The cyber insurance market has a short history of claims experience, and the available data on uninsured losses are believed to be incomplete because of underreporting. Pricing cyber insurance, therefore, remains very much a judgment call. Some companies base the rates on miscellaneous E&O rates, while others attempt more specific analyses. Most policies are priced based on the insured's revenues, a basis that is inexact at best because revenues are not always directly correlated to potential cyber loss exposure.[25]**

The coverage limits are a crucial element of the economics of cyber policies. One broker reported average aggregate cyber coverage limits of $16.9 million in 2012, with higher limits for industry groupings such as communications, media and technology ($33.4 million) and financial institutions ($26.0 million). When company revenues exceed $1 billion, coverage limits average 50% to 80% higher than overall industry averages.[26] Note that at an average cost of $200 per record, a $25 million limit would be exhausted with a data breach involving 125,000 records. If a plaintiff class obtained a judgment under a state statute that imposes $1,000 in damages for each claim-

© 2014 THOMSON REUTERS

ant, a $25 million limit would be exhausted with a 25,000 record data breach.[27]

As outlined above, a cyber insurance policy often includes many different claims triggers and most cyber policies "impose sub-limits on some coverages, such as for crisis management expenses, notification costs, or regulatory investigations. These sub-limits are not always obvious and they are often inadequate. They should be scrutinized carefully and set realistically."[28] One may confidently assume that the future will see increasing numbers of coverage filings by insurers, such as Zurich Insurance against Sony,[29] seeking to avoid having to cover losses resulting from class action lawsuits against companies whose customers' PII was obtained by Hackers.

Cyber insurance is a small but rapidly growing and evolving insurance product. Its future will undoubtedly be determined by changes in technology, legislation and regulation. Insurers are currently quite enthusiastic about the prospects for cyber insurance. If loss exposures can be limited in the face of burgeoning cyber-attacks, the insurers' confidence may be justified. The question is whether it will evolve into a viable and valuable means for the Potential Victims to transfer risk to insurers, or, turn out to be economically unsustainable due to adverse selection and excess costs, as happened in the long-term care market.

Conclusion

Evidence abounds that computer networks are under assault from within and from without. An array of Federal and State civil and criminal statutes and common law causes of action are already in play, as relief is sought by Potential Victims from perpetrators that may include businesses, individuals or foreign governments.

The ability to proceed with cases brought by or against the Potential Victims in cyber security matters will depend on how the case and statutory law develops and what actions are taken by Federal and State regulators. However, it is clear that the Potential Victims will have to be increasingly resilient in their ability to recover once an attack occurs, as well as vigilant about how they protect their cyber systems.

In weighing options with respect to liability, damages and insurance, Potential Victims should seek professionals who can help assess the choices and who can advise on appropriate steps. As is usually the case, the sooner experts are called in to assist, the more helpful they can be in achieving the objectives sought by Potential Victims.

NOTES

1. The entities potentially affected include, but are not limited to, commercial banks, building societies, credit unions, trust companies, mortgage lenders, investment companies, insurance companies, pension funds, hedge funds, investment banks, broker/dealers, futures commission merchants, as well as social media networks, search engines, print media, and major retailers and others (hereinafter "Potential Victims").
2. If confidential customer data (known as "PII" or personally identifiable information) is consciously disclosed to third parties seeking marketing opportunities among those customers, or inadvertently disclosed to the world at large, including those with criminal intent, as a result of a hacking incident, an employee's negligence, or a malfunctioning computer network, there may well be exposure to customers. Conversely, Potential Victims, as plaintiffs, may directly attempt to seek relief from hackers or others by instituting a suit against actors from the private sector or state sponsored entities for hacking or similar allegations of misconduct. They may also act indirectly by informing Federal or State officials. Such officials are, among other elements, armed with authority to enjoin hackers. See related stories on the vulnerability of the U.S. power grid, *The New York Times*, Aug. 17, 2013, at A11 and *The New York Times*, Sept. 11, 2013, at A17.
3. Hackers, as one manifestation of a criminal effort, may be motivated by political or social agendas (*see, e.g.*, Wikileaks and Anonymous). From the hacker's standpoint, the breach may be made merely to demonstrate that the hacker was clever enough to break into a company's system or to appropriate illicitly its victim's property.
4. Ponemon Institute, *2013 Cost of Data Breach Study: Global Analysis* (May 2013), Figure 3 and Figure 2, respectively, both on p. 5 *at* https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf, accessed January 2014. This study excludes data breaches in excess of 100,000 records on the basis that those are not representative and would skew the results. Consequently, the numbers cited here would not include the large data breaches at major retailers. Another study by the same firm using earlier data found

© 2014 THOMSON REUTERS

that equipment damage constituted 5% of the costs in 2012 while revenue loss was 19% and business disruption costs were 30%. The largest component of cost was information loss at 44%. Ponemon Institute, *2012 Cost of Cyber Crime Study: United States* (October 2012), Figure 14, at p. 14 *at* http://www.ponemon.org/local/upload/file/2012_US_Cost_of_Cyber_Crime_Study_FINAL6%20.pdf, accessed January 2014. This study did not distinguish between costs incurred by the affected organization itself (first party costs) and costs that the organization paid for damages suffered by third parties such as customers, employees, etc.

5. These would include Federal statutes such as Electronic Communication Privacy Act (18 U.S.C. § 2510 (1986) et seq.); the Stored Communications Act (18 U.S.C. § 2701 (1986)et seq.); the Telephone Consumer Protection Act (47 U.S.C. § 227 (1991); and the Fair Credit Reporting Act (15 U.S.C. § 1681 (1970) et seq.). Other Federal statutes not likely to be the subject of class actions include the Health Insurance Portability and Accountability Act (HIPAA) (45CFR Part 160 and Subparts A and E of Part 164), and the Gramm Leach Bliley Act (15 U.S.C. § 6801 (1999) et seq., Section 6801). The SEC requirement for publicly held companies to disclose cyber breaches, potential exposures and remedial actions is also significant in this context.
6. These include negligence, breach of contract, breach of implied contract, breach of the covenant of good faith and fair dealing, conversion, trespass, unjust enrichment and bailment.
7. Causes of action asserted in these class actions include negligence, conversion, breach of contract, breach of implied contract, breach of an implied bailment, and breaches of federal and state privacy statutes including one titled computer trespass.
8. *The New York Times*, Jan. 27, 2014, at B3.
9. *See, for example*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf;http://www.crowdstrike.com/sites/ all/themes/crowdstrike2/css/imgs/platform/crowdstrike_global_threat_report_2013.pdf.
10. United States Sovereign Immunities Act, 28 U.S.C. § 1602 (1976), et seq. *See, in particular*, Section 1605.
11. *LinkedIn Corporation v. Does, 1 through 10, Inclusive* (U.S. Dist. Ct., N.D. Cal. CV14-0068, January 6, 2014).
12. A New "Target" On Their Backs: Target's Officers and Directors Face Derivative Action Arising Out Of Data Breach, *see* http://fpn.advisen.com/articles/article212600760-1648454639.html.
13. For a more extensive discussion of reasonable royalties, see Patrick J. Flinn, *Handbook of Intellectual Property Claims and Remedies*, Walter Klewers, 9-46 (2008).
14. The Lloyd's Risk Index 2013, a global survey of 588 C-suite and board level executives, identified "Cyber Risk" as the third greatest risk to their business, exceeded only by "High Taxation" and "Loss of Customers/ Cancelled Orders." See Lloyd's Risk Index 2013, Chart 2, at p. 5 *at* http://www.lloyds.com/~/media/Files/News%20and%20Insight/Risk%20Insight/Risk%20Index%202013/Report/Lloyds%20Risk%20Index%202013report100713.pdf, accessed January 2014. Prior editions of Lloyd's Risk Index placed "Cyber Attacks" as the twentieth greatest business risk in 2009 and the twelfth greatest business risk in 2011. *Id*, at p. 33. Allianz, a global insurer, reported that "Cyber crime, IT failures, espionage" jumped to eighth on its list of the "Top 10 global business risks for 2014," a jump of seven places from the fifteenth spot in the 2013 analysis. Allianz, Allianz Risk Barometer 2014, at pp. 1 & 3 *at* http://www.agcs.allianz.com/assets/PDFs/Reports/Allianz-Risk-Barometer-2014_EN.pdf, accessed January 2014. The Allianz listing is based on a survey of over 400 corporate insurance experts from more than 30 countries. Both surveys demonstrate that cyber security is of significantly increasing concern.
15. Op. Cit., *2013 Cost of Data Breach Study: Global Analysis*, *supra* note 2, Figure 5, at p. 7.
16. "This means that in the event electronic data is destroyed or damaged as the result of a covered cause of loss, the insurer will pay the cost to replace or restore it. Causes of loss that apply to this coverage include a computer virus, harmful code or other harmful instructions entered into a computer system or network to which it is connected. There is no coverage, however, for loss or damage caused by the actions of any employee." Robert P. Hartwig & Claire Wilkinson, *Cyber Risks: The Growing Threat, Insurance Information Institute* (April 2013), at p. 14, http://www.iii.org/assets/docs/pdf/paper_CyberRisk_2013.pdf, accessed January 2014.
17. A.M. Best's News Service, *Lawyer: Claimants Increasingly Seek Cyber Liability Coverage From Non-Cyber Policies*, (May 22, 2013), http://www3.ambest.com/ambv/bestnews/newscontent.aspx?refnum=165684&altsrc=23, accessed January 2014.
18. A.M. Best's News Service, *Cyber Risk Insurance, An Opportunity For Growth, but Not Without Concerns* (May 22, 2013), http://www3.ambest.com/DisplayBinary/DisplayBinary.aspx?TY=P&record_code=212835&URatingId=1821808, accessed January 2014. Also, *supra* note 16, at p. 14.
19. Op. Cit., *Cyber Risks: The Growing Threat*, *supra* note 16, at pp. 14-15. "Given the bewildering variety and lack of standardization in cyber insurance, buying an off-the-shelf policy can result in disaster. Instead, partner with experienced professionals to help you place and negotiate tailored coverage." Rene Siemens & David Beck, *How to Buy Cyberinsurance*, Risk Management (October 2012), http://www.rmmagazine.com/2012/09/28/how-to-buy-cyberinsurance/,

© 2014 THOMSON REUTERS

accessed January 2014. "No standard cyber insurance policy language currently exists, and coverage varies significantly from one policy to another. Because case law tied to technology-related insurance claims is extremely limited, it's not uncommon for policies to have as many as five pages of coverage exclusions, as well as an exhaustive list of definitions for items such as breach, data, claim and vendor that vary among policies." *supra* note 18, at p. 3.

20. Op. Cit., *Cyber Risks: The Growing Threat, supra* note 16, at pp. 15-16.
21. Op. Cit., *Cyber Risk Insurance, An Opportunity For Growth, but Not Without Concerns, supra* note 18, at p. 1.
22. A.M. Best's News Service, Best's Review, *Webinar Extract: The Cyber Effect* (December 2013), at p. 86, http://viewer.zmags.com/publication/39a952e3#/39a952e3/89, accessed January 2014. Also *supra* note 18, at p. 2.
23. Op. Cit., *Cyber Risk Insurance, An Opportunity For Growth, but Not Without Concerns*, at pp. 1-2.
24. A.M. Best's News Service, *A.M. Best TV: Cyber Liability Seen as Huge Growth Market* (June 27, 2013), http://www3.ambest.com/ambv/displaycontent/video.aspx?vid=cyberliability613, accessed January 2014.
25. Op. Cit., *Cyber Risk Insurance, An Opportunity For Growth, but Not Without Concerns*, *supra* note 18, at p. 2.
26. Op. Cit., *Cyber Risks: The Growing Threat*, *supra* note 16, at pp. 17-19.
27. Op. Cit., *How to Buy Cyberinsurance, supra* note 19.
28. Op. Cit., *How to Buy Cyberinsurance, supra* note 19.
29. *Zurich American Insurance Co et. al v. Sony Corp of America et. al*, N. 651982 (S.Ct. N.Y. County, July 20, 2011).

© 2014 THOMSON REUTERS