COUGHLIN DUFFY LLP

ATTORNEYS AT LAW

The Cyber-Wave Continues – Insurance Coverage for Cyber Attacks, Breaches and Lawsuits

11 October 2012

Adam M. Smith, Esq.
Daniel L. Pascoe, Esq.

350 MOUNT KEMBLE AVENUE
P.O. BOX 1917
MORRISTOWN, NEW JERSEY 07962-1917
PHONE: (973) 267-0058
FACSIMILE: (973) 267-6442

WALL STREET PLAZA
88 PINE STREET, 28TH FLOOR
NEW YORK, NEW YORK 10005
PHONE: (212) 483-0105
FACSIMILE: (212) 480-3899

WWW.COUGHLINDUFFY.COM

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE COST OF CYBERCRIME GLOBALLY 2

III. DATA BREACHES 4

1. Global Payments 5

2. Zappos 7

3. Apple 7

4. Social Networking Sites 7

5. Internet and Email Providers 8

IV. RECENT COVERAGE CASES 9

1. Commercial Crime Policy 9

2. Personal and Advertising Injury 13

3. Property Damage 17

V. CONCLUSIONS 19

I. INTRODUCTION

Over the past year the use of the internet to communicate and transact business has continued to grow, which has left individuals and businesses more and more vulnerable to attacks on the systems and infrastructure that support these interactions. Despite the rise in awareness of cyber-attacks and the increase of resources being devoted to combat the problem, there has been a surge in the incidences of cybercrime affecting individuals and businesses using the internet. As a result, the number of cyber liability claims has also risen in 2012.

In a recent report, nearly all major industries are affected by cybercrime, with companies in the "accommodation and food services," "retail trade" and "finance and insurance" industries being hit particularly hard in 2012.[1] In fact, just this year, some of the most successful businesses in the world, such as Google, Apple, Visa® and Amazon, have been victims of data breaches. Further, as major social networking sites have gained popularity those sites have increasingly been targets of cyber-attacks in 2012, with Twitter and LinkedIn being the latest victims. These attacks expose a variety of individuals' personal information to criminals and result in businesses scrambling to gauge the scope of the breach so they can inform their customers while attempting to limit the damage to their reputations. It is not uncommon for lawsuits, whether filed individually or as class actions, to be filed against the businesses who suffered the cyber-attacks within weeks or even days of such breaches.

The costs of cybercrime and the amount of money expended in an effort to prevent it are astronomical. In one recent report, cybercrime is estimated to cost consumers $21 billion in the United States and $16 billion in Europe annually.[2] Another recent report

concludes that businesses globally expend approximately $10 billion annually in efforts to curtail cybercrime, which includes firewalls, intrusion detection systems, software maintenance and deployment, and user training.[3]

Given the proliferation of cyber-attacks over the last decade and the rising costs associated with cybercrime, insurance coverage for cyber liability claims is itself in flux and evolving as cybercrime grows and becomes more sophisticated. In previous papers we have discussed general trends in cyber liability claims and the rise of specialty cyber-risk insurance products. This paper focuses on the cost of cybercrime, the latest major data breach claims in 2012, and recent cases analyzing whether cyber liability claims are covered under traditional insurance policies, including commercial crime policies and commercial general liability policies.

II. THE COST OF CYBERCRIME GLOBALLY

A recent collaborative report prepared by researchers from a number of prestigious universities in England, Germany, Netherlands and the United States, led by the University of Cambridge, measured the direct costs, indirect costs and defense costs of cybercrime globally and appears to be the first comprehensive report of its kind.[4] The report distinguished between: (1) traditional crimes that are now labeled "cyber" because they are conducted online, such as tax fraud; (2) transitional crimes whose *modus operandi* have evolved as a result of the move online, such as credit card fraud; (3) new crimes that owe their existence to the internet, such as hacking; and (4) platform crimes, such as the use of malicious software, like botnets, which facilitate other crimes.[5]

According to the report, below are some examples of the cost of cybercrime annually:

TYPE OF CYBERCRIME	GLOBAL ESTIMATE
Cost of Genuine Cybercrime	
Online banking fraud	
- phishing	$320 million
- malware (consumer)	$70 million
- malware (business)	$300 million
- bank technology countermeasures	$1 billion
Fake antivirus	$97 million
Copyright-infringing software	$22 million
Copyright-infringing music etc.	$150 million
Patent-infringing pharma	$288 million
Fake escrow scam	$200 million
Advance-fee fraud	$1 billion
Cost of Traditional Cybercrime	
Online credit card fraud	$4.2 billion
Indirect costs of credit card fraud	
- loss of confidence (consumers)	$10 billion
- loss of confidence (merchants)	$20 billion
Cost of Traditional Crimes Becoming 'Cyber'	
Welfare fraud	$20 billion
Tax fraud (including individual and corporate)	$125 billion
Costs of Cybercrime Infrastructure	
Expenditure on antivirus	$340 million

Cost to industry on patching	$1 billion
Cost to users of clean-up	$10 billion
General defense measures by corporations (e.g., firewalls, intrusion detection systems, software maintenance and deployment, user training)	$10 billion[6]

While calculating estimates of the cost of cybercrime on a global level will never be an exact science, the sheer size of the estimates of this report reflects just how large of a problem cybercrime is in today's digital world and the amount of resources businesses are expending to combat it.

III. DATA BREACHES

In 2011, there were a number of high profile cybercrime attacks, including the infamous Sony PlayStation® Network data breach that affected approximately 77 million subscribers. As our paper from last year discussed, media outlets were quick to name 2011 "the year of the data breach."[7] Verizon's recent 2012 Data Breach Investigations Report, prepared by Verizon's RISK Team, in conjunction with the United States Secret Service and the Dutch High Tech Crime Unit, supports that conclusion.[8] The Verizon report found that in 2011, "[t]he number of compromised records … skyrocketed back up to 174 million after reaching an all-time low … in last year's report of four million" and "2011 boasts the second-highest data loss since [Verizon] started keeping track in 2004."[9]

The Report outlines the following entities involved in data breaches in 2011:

98% stemmed from external agents (+6% from prior year)

4% implicated insiders (-13% from prior year)

<1% resulted from business partners (no change from prior year)

58% of data theft tied to activist groups

Verizon found that in 2011, activist groups stole more data than any other group and, as a result, "[w]hile good old-fashioned greed and avarice were still the prime movers, ideological dissent and schadenfreude took a more prominent role across the caseload." [10] Some of the more notorious of these "hacktivist" groups include LulzSec, AntiSec and Anonymous.[11]

The circumstances of the data breaches in 2011 can be classified as follows:

81% utilized some form of hacking (+31% from prior year)

69% incorporated malware (+20% from prior year)

10% involved physical attacks (-19% from prior year)

7% employed social tactics (-4% from prior year)

5% resulted from privilege misuse (-12% from prior year)

The Verizon report suggests that data breaches in 2011 stemming from hacking and malware continue to become the cybercrime of choice, while more traditional insider employee data breaches have fallen to an all-time low. [12]

As set forth above, there were significantly more cyber-attacks in 2011 than 2010. Moreover, reports from the first nine months of this year suggest that the number of data breaches is not slowing down. The details of some major and high-profile data breaches in 2012 are described below.

1. Global Payments

Likely the most serious cyber-attack of 2012 to date is the Global Payments data breach.[13] Global Payments, Inc. is one of the largest processors of Visa® and MasterCard® card transactions, and also processes a sizable number of transactions for Discover® and American Express®.[14] In March 2012, hackers were able to obtain credit

card information for at least 1.5 million card holders and potentially 5.5 million additional card holders.[15] According to reports, the hackers obtained cardholders' names and account information, which would allow cyber criminals to clone the credit cards.[16]

As of 26 July 2012, Global Payments estimates that the breach has cost it $84.4 million.[17] Of this amount, Global Payments states that $19 million represents the costs it incurred through 31 May 2012 for legal fees, fees of consultants and other professional advisors engaged to conduct the investigation, in addition to various other costs associated with the investigation and remediation.[18] Further, Global Payments states that $67.4 million represents its estimate of fraud losses, fines and other charges that will be imposed upon it by the card networks.[19]

In corporate filings, Global Payments has stated that it may have coverage for the data breach under a Professional and Technology Based Services, Technology Products, Computer Network Security, and Multimedia and Advertising Injury Insurance Policy issued by Lloyd's Underwriters and a follow form Excess Liability Policy issued by State National Insurance Company that have combined policy limits of $30 million.[20] Global Payments has disclosed that, as of 26 July 2012, it has recovered $2.0 million in insurance payments.[21]

In April 2012, a putative class action lawsuit was filed against Global Payments in federal court in Georgia.[22] The plaintiffs allege that Global Payments failed to maintain adequate procedures to protect their personally identifiable information which they allege resulted in fraudulent credit card charges.[23] Further, the plaintiffs assert that Global Payments failed to timely notify the public of the data breach.[24] The complaint includes causes of action for negligence, negligence per se, breach of third-party beneficiary

contract, breach of implied contract, and violation of the federal Stored Communications Act, Fair Credit Reporting Act and Georgia's Unfair and Deceptive Trade Practices Act.[25]

2. Zappos

In January 2012, Zappos, one of the most successful online shoe and apparel merchants, was hit by a cyber-attack that exposed the personal information of approximately 24 million Zappos customers.[26] The attack exposed the customers' names, e-mail addresses, addresses, phone numbers and partial credit card numbers.[27]

Just one day after Zappos announced the breach, a putative class action suit was filed in federal court in Kentucky against Zappos' parent company, Amazon.com, which seeks not only unspecified damages but also a court order requiring Amazon.com to pay for credit monitoring and identity theft insurance.[28] Eight other putative class action suits were subsequently filed against Amazon.com.[29] In June 2012, a federal court in Nevada consolidated the nine putative class action suits into one class action suit.[30]

3. Apple

Just last month, in September 2012, over one million Apple user identifications were hacked and posted online.[31] Initially, the hackers claimed that the Apple data was taken from the Federal Bureau of Investigations (the "FBI"), which allegations the FBI quickly denied. After further investigation, it was discovered that the data breach of the Apple user identifications came from a small application software company that Apple worked with, called Blue Toad.

4. Social Networking Sites

As social networking has become an integral part of peoples' daily lives, social networking sites have increasingly become targets of cyber-attacks. Since the beginning

of the year, a number of social networking sites have been victims of data breaches, including LinkedIn and Twitter.

A. LinkedIn

LinkedIn operates the world's largest professional network on the internet and has over 175 million members in over 200 countries.[32] In June 2012, LinkedIn was hacked resulting in the exposure of approximately 6.5 million subscribers' passwords.[33] According to media reports, LinkedIn failed to use "best practices" for protecting the data and only used a basic technique for encrypting the passwords which left the data vulnerable to attack.[34] LinkedIn has indicated that the forensic investigation and other recovery costs of the data breach could exceed $1 million.[35]

Less than two weeks after the announcement of the breach, on 15 June 2012, a putative class action suit was filed against LinkedIn in federal court in California seeking $5 million in damages.[36] Three other class action suits were subsequently filed. The four class action suits were consolidated on 29 August 2012 in federal court in California.[37]

B. Twitter

Twitter is a real-time information network with approximately 200 million members that connects people to the latest stories, ideas, opinions and news in 140 characters or shorter.[38] In May 2012, approximately 60,000 members' account information was hacked and then released publically, including members' user names and passwords.[39]

5. Internet and Email Providers

Major internet and email providers have not been spared from data breaches in 2012.

A. Yahoo Voice

In July 2012, Yahoo's user-generated content site, Yahoo Voice, was hacked into, resulting in the release of personal information of 450,000 customers, including email addresses, user names and passwords.[40]

In August 2012, a putative class action was filed against Yahoo in federal court in California. The plaintiffs allege that Yahoo failed to "deploy even the most rudimentary of protections for certain users' personal information."[41]

B. Google's Gmail Service and Other Email Providers

The same hackers who breached the accounts of Yahoo Voice also hacked the email accounts of 106,000 Gmail users, Google's email service, 55,000 Hotmail users and 25,000 AOL users.[42] The hackers publically released the affected users' email addresses, user names and passwords.[43]

IV. RECENT COVERAGE CASES

Because many companies are still not protected by cyber-risk policies or, if they are, those policies are quickly exhausted, companies are continuing to seek coverage for cybercrime under more traditional insurance policies. In this paper we discuss cases from 2012 that have analyzed whether there is coverage for data breaches under: (1) a commercial crime policy; (2) a commercial general liability policy as an advertising injury; and (3) a commercial general liability policy as property damage.

1. Commercial Crime Policy

On 28 August 2012, the Sixth Circuit Court of Appeals sent shockwaves through the cyber-risk insurance industry when it found coverage for a cyber-attack under a blanket crime policy. *See Retail Ventures, Inc. v. DSW Shoe Warehouse, Inc.*, 2012 U.S.

App. LEXIS 17850, 2012 FED App. 027P (6th Cir. 2012). The case stemmed from a highly publicized cyber-attack in 2005 on DSW Shoe Warehouse, Inc. ("DSW"), a national shoe retailer chain.[44] In February 2005, hackers accessed DSW's main computer system through a store's local wireless network and downloaded credit card and checking account information of 1.4 million customers from 108 different stores.[45] The hackers then used the information to make fraudulent credit card charges.[46] As a result of this breach, DSW spent over $5 million in connection with customer communications, public relations, customer claims, lawsuits and governmental investigations.[47] Of that amount, more than $4 million was the result of fines by the affected credit card companies.[48]

DSW sought coverage from National Union Fire Insurance Company ("National Union") under a "Computer & Funds Transfer Fraud Coverage" endorsement (the "Fraud Endorsement") in a blanket crime policy.[49] The Fraud Endorsement provided, in relevant part, that National Union would pay DSW for "[l]oss which the [DSW] shall sustain resulting directly from…" "[t]he theft of any [DSW] property by Computer Fraud…"[50] "Computer Fraud" was defined as:

> [T]he wrongful conversion of assets under the direct or indirect control of a Computer System by means of: (1) The fraudulent accessing of such Computer System; (2) The insertion of fraudulent data or instructions into such Computer System; or (3) The fraudulent alteration of data, programs, or routines in such Computer System.[51]

The Fraud Endorsement also provided that coverage applies "only with respect to … Money or Securities or Property located on the premises of the Insured."[52] Further, the Fraud Endorsement included an exclusion that provides that "[c]overage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind."

National Union denied the claim on the grounds that the loss was excluded under the exclusion contained in the Fraud Endorsement because the loss was related to the theft of proprietary confidential customer credit information. Additionally, while National Union did not dispute that the unauthorized access and copying of the customer information stored on DSW's computer system involved the "theft of any [DSW] property by Computer Fraud," National Union argued that DSW's loss did not qualify as a loss "resulting directly from" the theft of DSW's property.[53]

As a result of National Union's denial, DSW filed a declaratory judgment in the United States District Court, Southern District of Ohio.[54] The district court granted summary judgment in favor of DSW finding coverage under the blanket crime policy and awarding DSW the full amount of the loss, plus interest.[55] The district court, however, denied DSW's bad faith claims against National Union.[56] National Union appealed to the Sixth Circuit Court of Appeals.[57]

The Sixth Circuit first ruled that a proximate cause standard should be applied to determine whether DSW's loss "resulted directly from" the theft of DSW's property.[58] By doing so, the court rejected National Union's position that the blanket crime policy was basically a traditional fidelity bond that does not provide third-party coverage.[59] The court stated that the terms of the policy, as opposed to the title of the policy, govern the coverage provided and determined that different provisions of the policy contemplated third-party coverage.[60] Further, the court rejected National Union's argument that the phrase "resulting directly from" unambiguously means that the data breach had to be the sole cause of DSW's loss.[61] Instead, the court held that the phrase "resulted directly from" only required that the data breach be the proximate cause of DSW's loss.[62] Accordingly,

the court concluded that DSW's loss "resulted directly from" the data breach as required by the crime policy.[63]

The Sixth Circuit then turned its attention to National Union's argument that the exclusion contained in the Fraud Endorsement barred coverage because DSW's loss was related to the theft of proprietary confidential customer credit information.[64] The court ruled that even assuming that copying of the customer information qualified as a "loss," it was not a loss of "proprietary information … or other confidential information of any kind."[65] The court reasoned that the customer information was not "proprietary information" because the information is owned or held by many parties, including the customer, the financial institution and the merchants to whom the information is provided in the stream of commerce.[66] As a result, the court determined that "other confidential information of any kind" could not be interpreted so broadly to mean any information belonging to anyone that is expected to be protected from unauthorized disclosure, because to do so "would swallow not only the other terms in [the] exclusion but also the coverage for computer fraud."[67] Additionally, the court held that the exclusion applied to the insured's confidential information which is used in the insured's business, not to customer's information which does not involve the manner in which the business is operated.[68] For these reasons, the court held the exclusion was not applicable.[69]

The Sixth Circuit's ruling has been the subject of considerable legal debate and is likely to be far-reaching in the world of cyber coverage as it provides policyholders with similar policies a roadmap to seek coverage for cyber-attacks under a traditional commercial crime policy.

2. Personal and Advertising Injury

While the question of whether a cyber-attack can be deemed a personal and advertising injury under a commercial general liability policy has been raised in several cases,[70] the issue has yet to be decided by any court. This issue was litigated this year in the United States District Court, Northern District of Illinois in a case called *Arch Insurance Company v. Michaels Stores*.[71] Although this case settled in September 2012, before the issue of coverage could be decided by the court, the papers filed by both sides in support of cross motions of summary judgment are instructive on the differing viewpoints on this issue.

The case arose from a cyber-attack on Michaels, Inc. ("Michaels"), a craft supply retail chain, in 2011.[72] A group of criminals tampered with ninety Personal Identification Number ("PIN") pad terminals in eighty Michaels' stores throughout the United States, allowing the criminals to steal financial information of customers who made credit and debit card purchases.[73] The criminals then used the data to make purchases of their own and also sold the data to third-parties.[74]

As a result of the cyber-attack, victims of the data breach filed seven putative class actions against Michaels.[75] Michaels tendered the lawsuits to Arch Insurance Company ("Arch"), Michaels' commercial general liability carrier, and Arch denied coverage.[76] In March 2012, Arch filed a declaratory judgment action against Michaels seeking a declaration that there was no coverage under the commercial general liability policy that Arch issued to Michaels (the "Arch CGL Policy").[77] In June 2012, Michaels and Arch filed cross motions for partial summary judgment as to whether Arch owed Michaels a

duty to defend the underlying class actions.[78] Both parties agreed that Texas law applied.[79]

A. Michaels' Motion for Partial Summary Judgment

In Michaels' moving papers, Michaels argued that the underlying class actions allege "personal and advertising injury" caused by an offense arising out of Michaels' business.[80] The Arch CGL Policy defined "personal and advertising injury" as "injury … arising out of … [o]ral or written publication, in any matter, of material that violates a person's right to privacy."[81] Michaels argued that the Arch CGL Policy does not define "publication" and, thus, that term must be given its plain and ordinary meaning which is "to disclose, circulate, or prepare and issue printed material for public distribution."[82] Likewise, Michaels asserted that the Arch CGL Policy does not define "privacy" and, therefore, that term must be given its plain and ordinary meaning which encompasses interest in both secrecy of private information and seclusion.[83]

Michaels then argued that the allegations in the underlying class actions claim injuries caused by the publication of their private information constituting personal and advertising injury because: (1) the complaints characterize the financial information at issue as private; and (2) the complaints allege the "dissemination" of customer's private information and, according to Michaels, "dissemination" is synonymous with "to publish."[84] Michaels argued that the fact that the class action complaints allege publication by the criminals and not Michaels is immaterial because "personal and advertising injury" is defined broadly to mean injury arising out of oral or written publication "in any matter."[85] Michaels also argued that other exclusions in the Arch CGL Policy specifically exclude conduct carried out "by or at the direction of the insured" and

the omission of similar language from the coverage provision for personal and advertising injury illustrates that such limitation is not included in the coverage grant for personal and advertising injury.[86]

Michaels next argued that the personal and advertising injury was caused by an offense arising out of Michaels' business.[87] Michaels stated that "arising out of" means originating from, having its origin in, growing out of or flowing from.[88] Given that the underlying plaintiffs alleged they were injured by the data breach when they were making purchases at the store, Michaels argued that the alleged injuries had their origin in Michaels' business of selling craft supplies.[89]

Michaels then concluded that Arch owed it a duty to defend because the underlying class actions sought "damages because of "personal and advertising injury,'" [since]: (1) the underlying class actions seek statutory damages that constitute "damages" under the Arch CGL Policy; and (2) those damages were allegedly suffered because of "personal and advertising injury." [90]

B. Arch's Motion for Partial Summary Judgment

Arch began its analysis by stating that "personal and advertising injury" is defined to include injury arising out of certain enumerated offenses and the only offense conceivably implicated by the underlying class actions is the offense for "oral or written publication, in any matter, of material that violates a person's right of privacy."[91] Arch then argued that the claims from the underlying class action are not covered under this offense because: (1) the underlying class actions do not allege "oral or written publication"; and (2) the plaintiffs in the underlying class action do not seek damages "because of" the right of privacy offense.[92]

As to the "oral or written publication" argument, Arch asserted that Michaels was sued for its failure to prevent criminals from stealing customers' financial information and its subsequent failure to provide those customers with notice of the data breaches.[93] Arch argued that this conduct does not involve "oral or written publication" of material.[94] Indeed, Arch noted that while there may be isolated allegations that Michaels' "knowingly divulged" customer financial information, there were no specific factual allegations regarding how Michaels' divulged the data and, thus, the court cannot read facts into the underlying class action complaints to conclude they involve "oral or written publication."[95] Further, Arch argued that the "personal and advertising injury" coverage provides "offense" based coverage for the conduct of the insured, not third-parties and, as a result, Arch asserted that the actions of third-party criminals cannot implicate the right of privacy offense.[96] Finally, Arch argued that the term "publication", as used in the right of privacy offense, requires "public distribution" and there are no allegations in the underlying class actions that the customers' financial data was "publically distributed."[97]

As to whether the underlying class actions seek damages "because of" the right of privacy offense, Arch argued that the damages sought by the underlying plaintiffs are not "because of" any oral or written publication of material that violated the underlying plaintiffs' privacy rights.[98] Instead, Arch asserted that the court must look to the gravamen of the underlying class action which indicates the damages sought by the underlying plaintiffs are "because of" Michaels' alleged failure to safeguard its PIN pad terminals and to provide adequate notice of the data breaches.[99] As a result, Arch concluded that it does not owe Michaels a duty to defend the underlying class actions.[100]

C. The Settlement

On 7 September 2012, Arch and Michaels settled their coverage dispute before the parties' motions for summary judgment were decided.[101] Although it is disappointing that there was no decision, the parties' motion papers illustrate the opposing arguments in this novel coverage issue in which insureds are seeking coverage for data breaches under personal and advertising injury coverage. We note nonetheless that Michaels' excess insurer, XL Insurance America Inc., filed its own declaratory judgment action against Michaels in New York state court in June 2012 in connection with coverage for the same 2005 data breaches.[102] Further, in June 2011, Zurich American Insurance Company filed a similar declaratory judgment action against Sony which involves whether there is personal and advertising injury coverage for the Sony PlayStation® Network data breach under a commercial general liability policy.[103] Thus, it is likely we will see developments in this area over the course of next year that may provide guidance to insurers and their insureds in this emerging area of coverage.

3. Property Damage

Another avenue insureds have explored in an effort to obtain coverage for data breaches is to characterize the breaches as property damage. A recent case decided this year out of the United States District Court for the Southern District of Illinois captioned *Nationwide Insurance Company v. Hentz* explored this very issue.[104]

This case arose after a CD-ROM was stolen from Jeanne Hentz's ("Hentz") car on October 31, 2010.[105] The CD-ROM contained the names and personal information of approximately 30,000 participants and beneficiaries of Central Laborers Pension Fund ("Central Laborers").[106] As a result of the theft, Central Laborers notified the participants

affected and contracted for credit monitoring services and insurance.[107] These efforts cost Central Laborers approximately $200,000.[108] Central Laborers then sued Hentz to recover those costs.[109]

Hentz tendered the underlying suit to Nationwide Insurance Company ("Nationwide"), Hentz's homeowner's insurer.[110] Nationwide denied coverage and brought a declaratory judgment action against Hentz arguing that it does not owe her a duty to defend in connection with the underlying action.[111]

The first question the court examined was whether the theft of the CD-ROM consituted property damage.[112] The homeowner's insurance policy that Nationwide issued to Hentz (the "Nationwide Policy") states that Nationwide will provide a defense if a suit is filed against Hentz "for damages because of … 'property damage.'"[113] "Property damage" is defined as "physical injury to, destruction of, or loss of use of tangible property."[114] The court noted that if someone had hacked into Hentz's computer and stolen the data, Hentz would not have suffered any tangible property damage.[115] But given that the medium on which the data was stored, i.e. the CD-ROM, was itself stolen, the court concluded that Hentz had suffered tangible property damage.[116]

The court then turned to whether the underlying damages were suffered "because of" the property damage.[117] The court determined that Central Laborers' alleged damages, while intangible economic damages, might trigger coverage as long as they resulted from covered property damage.[118] The court held that the underlying suit did contain allegations that Central Laborers were damaged as a result of the theft of the CD-ROM, Hentz's property damage, so Nationwide's duty to defend was potentially triggered.[119]

Next, the court examined whether the Nationwide Policy's "property in care of insured" exclusion barred coverage.[120] The exclusion stated there is no coverage for property damage "to property … in the care of the 'insured.'"[121] The court noted that the intent of such an exclusion is "to prevent general liability insurance, which 'is designed to indemnify the insured from liability to third persons resulting from the breach of some duty by the insured…' 'from becoming tantamount to property insurance when property … in the custody and control of a named insured and therefore subject to damage or loss due to the named insured's own acts or omissions.'"[122] The court examined the allegations of the underlying complaint to determine whether the CD-ROM was in Hentz's care.[123] The court ruled that the complaint alleged that the CD-ROM had been in Hentz's possession and Hentz left the CD-ROM in her own car.[124] As a result, the court held that the exclusion applied and Nationwide had no duty to defend Hentz in the underlying action.[125]

The *Nationwide* case is significant as it illustrates that while data breaches may technically fall within a coverage grant, common exclusions may still bar coverage. We anticipate that insureds' efforts to seek coverage for data breaches as property damage will decline as cyber-crime continues to evolve and the physical theft of the medium holding the data becomes less and less prevalent.

V. CONCLUSION

As set forth above, in 2012, the number of cyber-attacks has continued to grow as people are becoming increasingly reliant on the internet, not only to communicate, but also to transact business. The estimated costs of cybercrime and the resources spent to combat it are enormous. At the same time, the cost of specialty cyber policies remains

high, and the limits of the cyber policies are often inadequate. As a result, more and more insureds are seeking creative ways to obtain coverage for data breaches under traditional insurance products, such as commercial crime policies and commercial general liability policies.

---

[1]Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit and United States Secret Service, "2012 Data Breach Investigations Report" (hereafter "Verizon 2012 Report").
[2] "2012 Norton Cybercrime Report."
[3] Ross Anderson, et al., "Measuring the Cost of Cybercrime," 11th Annual Workshop on the Economics of Information Security 2012 (hereafter "WEIS 2012 Report").
[4] *Id.*
[5] *Id.*
[6] *Id.*
[7] For example, Karl Vasiloff, et al., "2011 - The Year of the Breach," law360.com, Aug. 8, 2011.
[8] Verizon 2012 Report.
[9] *Id.*
[10] *Id.*
[11] Geoff Duncan, "Rise of the Hacktivist: Activists Now Outsteal the Thieves," digitaltrends.com, Mar. 23, 2012.
[12] Verizon 2012 Report.
[13] Trevis Team, "Global Payments Data Breach Exposes Card Payments Vulnerability," Forbes, April 3, 2012.
[14] *Id.*
[15] Linda Foley, "Global Payments breach increased to 7 million records," examiner.com, May 4, 2012.
[16] Greg Ryan, "Cardholders Sue Global Payments Over Massive Data Breach," law360.com, April 6, 2012.
[17] Andrew Johnson, "Global Payments Take Charge of $84 Million for Data Breach," Wall Street Journal, July 26, 2012.
[18] Market Watch, "10-K/A: Global Payments Inc.," Wall Street Journal, Sept. 28, 2012.
[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] David Goldman, "Zappos Hacked, 24 Million Accounts Accessed," CNN Money, Jan. 16, 2012.
[27] *Id.*
[28] Karen Gullo, "Amazon.com Sued by Customer Over Hackers' Theft of Zappos Data," Bloomberg Businessweek, Jan. 18, 2012.
[29] Basil Katz, "LinkedIn Sued for $5 Million Over Data Breach," Reuters.com, June 20, 2012.
[30] *Id.*
[31] Vivian Kuo, "App Publisher Takes Blame for Massive Apple ID Hack," CNN, Sept. 10, 2012.
[32] "About Us," LinkedIn.com.
[33] Jim Finkle, et al., "LinkedIn Suffers Data Breach," Reuters.com, June 6, 2012.
[34] Nicole Perlroth, "Lax Security at LinkedIn is Laid Bare," New York Times, June 10, 2012.
[35] Warwick Ashford, "LinkedIn Data Breach Costs More Than $1M," ComputerWeekly.com, Aug. 6, 2012.
[36] *Supra*, n. 17.
[37] Linda Chiem, "LinkedIn Privacy Class Actions Over Data Breach Merged," law360.com, Aug. 30, 2012.
[38] "About," Twitter.com.

[39] Laurie Segall, "Twitter Hack Breaches Thousands of Accounts," CNN Money, May 8, 2012.
[40] Paul Wagenseil, "450,000 Yahoo Voice Passwords Stolen in Data Breach," MSNBC, July 12, 2012.
[41] Christopher Brook, "Yahoo Sued By User Following Breach of 450,000 Passwords," ThreatPost.com, Aug. 3, 2012.
[42] Nicole Perlroth, "Yahoo Breach Extends Beyond Yahoo to Gmail, Hotmail, AOL Users," New York Times, July 12, 2012.
[43] *Id.*
[44] *Retail Ventures*, 2012 U.S. App. LEXIS 17850 at *2-3.
[45] *Id.* at *3.
[46] *Id.*
[47] *Id.* at *4.
[48] *Id.*
[49] *Id.* at 10.
[50] *Id.*
[51] *Id.*
[52] *Id.* at *10-11.
[53] *Id.* at *26.
[54] *Id.* at *6.
[55] *Id.*
[56] *Id.*
[57] *Id.* at *7.
[58] *Id.* at *21-22.
[59] *Id.* at *14-15.
[60] *Id.*
[61] *Id.* at *23.
[62] *Id.* at *25.
[63] *Id.*
[64] *Id.* at *25-26.
[65] *Id.* at *28-29.
[66] *Id.* at *28.
[67] *Id.* at *30.
[68] *Id.* at *31-32.
[69] *Id.* at *32.
[70] *Zurich Am. Ins. Co. v. Sony Corp. of Am., et al.*, N.Y. Sup. Crt., N.Y. Co., Index No.651982/2011.
[71] *Arch Ins. Co. v. Michaels Stores, Inc.*, No. 1:12-cv-00786 (N.D. Il. 2012).
[72] Derek Hawkins, "Michaels' Insurer Sues Over Card Data Theft Coverage," law360.com, Feb. 6, 2012.
[73] *Id.*
[74] *Id.*
[75] *See* Michaels Stores, Inc.'s Memorandum of Law in Support of its Motion for Partial Summary Judgment dated June 8, 2012 and available on the United States District Court's PACER system as document 27 filed under Case No. 1:12-cv-00786 ("Michaels' Memo. of Law").
[76] Michaels' Memo. of Law at p. 4.
[77] *Id.*
[78] Michaels' Memo of Law; Arch's Memorandum of Law in Support of its Motion for Partial Summary Judgment dated June 8, 2012 and available on the United States District Court's PACER system as document 30 filed under Case No. 1:12-cv-00786 ("Arch's Memo. of Law").
[79] *Id.*
[80] Michaels' Memo of Law at p. 6.
[81] *Id.*
[82] *Id.*
[83] *Id.* at p. 7.
[84] *Id.*
[85] *Id.* at p. 8.
[86] *Id.*

[87] *Id.* at p. 9.
[88] *Id.*
[89] *Id.*
[90] *Id.* at pp. 10-11.
[91] Archs' Memo. of Law at p. 7.
[92] *Id.* at pp. 7 & 10.
[93] *Id.* at p. 7.
[94] *Id.*
[95] *Id.* at p. 8.
[96] *Id.*
[97] *Id.* at p. 9.
[98] *Id.* at pp. 10-11.
[99] *Id.* at p. 11.
[100] *Id.* at p. 12.
[101] Linda Chiem, "Michaels, Arch Settle Data Theft Coverage Fight," law360.com, Sept. 10, 2012.
[102] Bibeka Shrestha, "Michaels Has Edge In Data Theft Coverage Suit, Attys Say," law360.com, June 11, 2012.
[103] *Zurich Am. Ins. Co. v. Sony Corp. of Am., et al.*, N.Y. Sup. Crt., N.Y. Co., Index No.651982/2011.
[104] *Nationwide Ins. Co. v. Hentz*, 2012 U.S. Dist. LEXIS 29181, Case No. 11-cv-618-JPG-PMF (S.D. Il. 2012).
[105] *Id.* at *2.
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.* at *3.
[110] *Id.*
[111] *Id.* at *4.
[112] *Id.* at *7.
[113] *Id.* at *11.
[114] *Id.* at *7.
[115] *Id.* at *10-11.
[116] *Id.* at *11.
[117] *Id.*
[118] *Id.* at *12.
[119] *Id.* at *13.
[120] *Id.*
[121] *Id.*
[122] *Id.* at *14.
[123] *Id.* at *15.
[124] *Id.*
[125] *Id.* at *16.