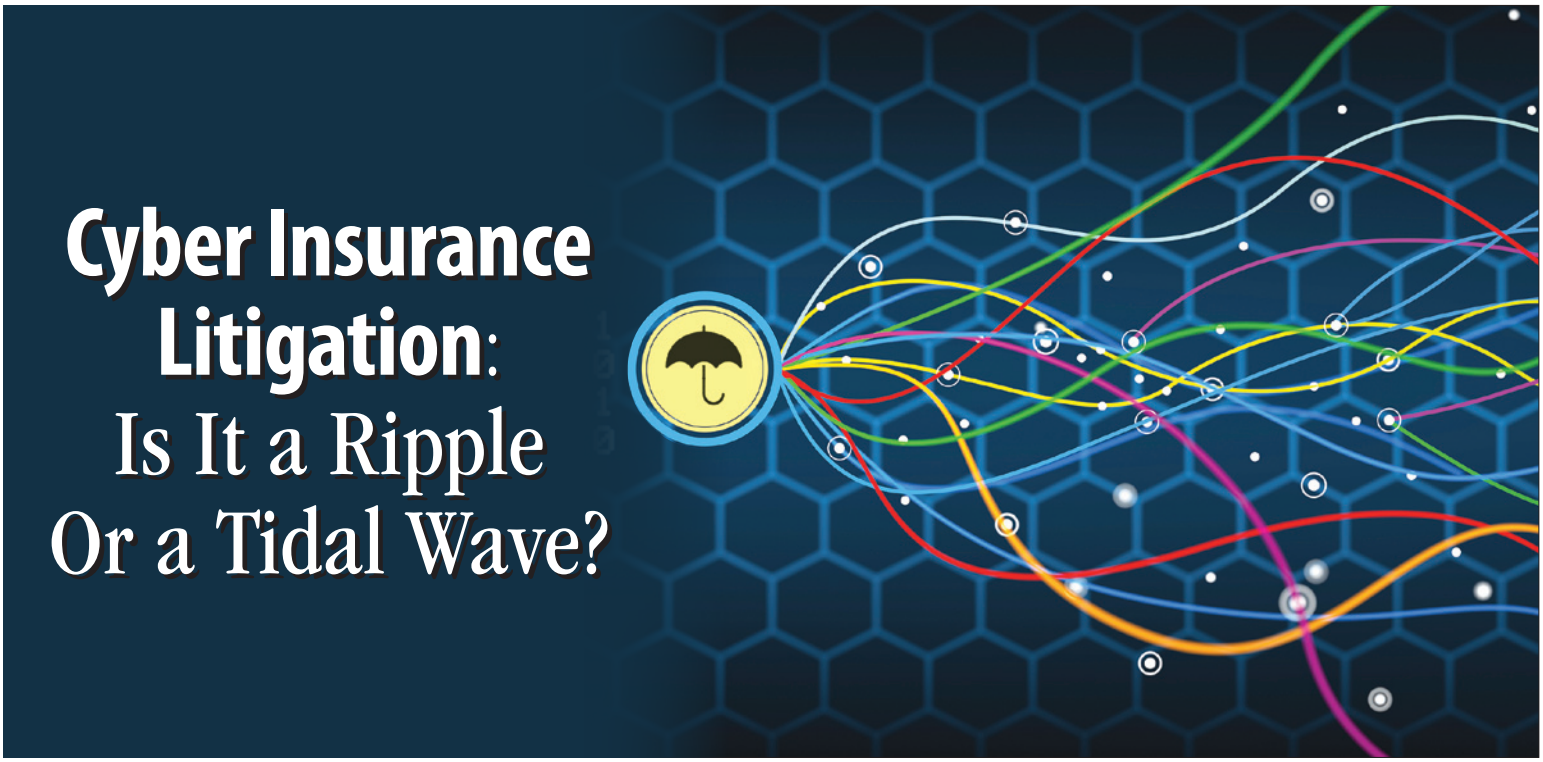
New York Law Journal
A NEW YORK LAW JOURNAL SPECIAL SECTION
An ALM Publication
Litigation
WWW.NYLJ.COM
MONDAY, FEBRUARY 22, 2016



Cyber Insurance Litigation: Is It a Ripple Or a Tidal Wave?

BY ROBERT D. CHESLER AND ANNA M. PIAZZA

On Sept. 9, 2015, Excellus BlueCross BlueShield announced a data breach that compromised about 10.5 million people's personal information, including Social Security numbers and medical and financial information. Excellus discovered the data breach during an investigation of its computer system. The breach had occurred on Dec. 23, 2013. A class action has already been filed, and Excellus is cooperating with the FBI.

One of the most interesting circumstances arising from the Excellus data breach is the "ho-hum" attitude with which most readers will greet it. Data breach has become a fact of corporate life. Phishing, malware, cyber extortion, and hacking are now terms with which we are all familiar. Readers do not need another article to warn them of the dangers of data breach.

Federal courts recently have done little to protect corporate data breach victims. In *Remijas v. Nieman Marcus Group*, 794 F.3d 688 (7th Cir. 2015), for example, class action plaintiffs were not required to show that they incurred any direct damage as a result of identity theft. In *Federal Trade Commission v. Wyndham Worldwide*, 799 F.3d 236 (3d Cir. 2015), the court held that the FTC maintained enforcement power over data breaches and could find, as a basis of liability, that the company's internal privacy network was inferior to what was portrayed in its public statements. Finally, in the *Target Corporation Customer Data Security Breach Litigation*, Case No. 0:14-md-02522 (D. Minn.), the court certified a class action of banks and other credit card issuers for the damages that they incurred in replacing credit cards.

In times of financial danger, corporations turn to their insurance companies for protection. All too often, however, those insurance companies fail their policyholders. This pattern began with environmental insurance litigation. The passage of Superfund confronted corporate America with hundreds of millions of dollars of exposure to environmental claims. When policyholders sought coverage under their general liability policies, their insurance companies rebuffed them. The environmental insurance wars that followed have lasted until the present, often with vicious litigation that has cost untold hundreds of millions of dollars and seems never-ending.

ROBERT D. CHESLER *and* ANNA M. PIAZZA *are shareholders in Anderson Kill's insurance recovery group in the Newark and New York offices, respectively.*

Policyholders believe that insurance companies invented any reason, no matter how farfetched or intellectually dishonest, to deny coverage. Of course, insurance companies believe that policyholders proffered equally unrealistic and unsupported reasons in favor of coverage.

How insurance companies will react to cyber claims presents a big question. These claims share key characteristics with environmental claims. In both situations, any company could find itself a victim. Both risks involve potentially huge amounts. The courts are setting forth rigorous standards of liability. How will the insurance companies respond to a possible flood of claims?

Policyholders have made claims for data breach damages under three types of policies: traditional general liability policies; cyber policies; and computer endorsements or riders to crime, banker's bond, or executive risk policies. Litigation quickly ensued under general liability policies, but that avenue of coverage has essentially closed with the advent of total cyber exclusions. Whether the insurance industry will honor their cyber policies or another insurance coverage litigation bloodbath will follow remains to be seen. Anecdotally, insurance companies have made payments under cyber policies. However, that trend could change. For the first time, an insurance company has sued its policyholder under a cyber policy.

Junk-Fax Insurance Coverage Litigation

"Junk-fax" insurance coverage litigation presents an important and instructive prelude to cyber insurance litigation. Pursuant to the Telephone Consumers Protection Act (TCPA), a company that sends an unrequested fax (or robocall) faces liability of $500 per offense. If the company sends 50,000 faxes, for example, it faces a $25,000,000 exposure. Some companies have sent hundreds of thousands of unrequested faxes.

The availability of such damages has led attorneys to seek out plaintiffs and to bring suits seeking statutory damages. The defendants have turned to their insurance companies, setting forth a torrent of litigation. Maniloff & Stempel, General Liability Insurance Coverage (2d ed.) lists about 50 junk fax insurance coverage cases that have gone to judgment. Plaintiffs continue to file new junk fax cases, and now junk robocall cases. However, new exclusions in general liability policies may put a halt to insurance coverage for junk-fax litigation going forward.

The junk fax insurance litigation centered on two insurance policy terms—"privacy" and "publication." The general liability policy grants coverage for a "publication" that invades "privacy." Insurance companies asserted that "privacy" had two meanings—secrecy and seclusion. They further argued that the insurance policy's use of the term "privacy" applied only to the invasion of a person's right to secrecy because the insurance policy couples "privacy" with "publication." Insurance companies then argued that junk-faxes involved only the injured party's receipt of the fax, which implicated only seclusion—the right to be left alone. *Valley Forge Ins. v. Swiderski Electronics*, 860 N.E. 2d 307 (Ill. 2006).

Policyholders contended that courts should give "privacy" its ordinary meaning, as a typical policyholder would understand it. Such a person would not distinguish between secrecy and seclusion, but would construe "privacy" as a broad grant of coverage. The majority of courts have agreed. *Penzer v. Transportation Ins.*, 29 So. 3d 1000 (Fla. 2010).

The junk fax coverage litigation demonstrates that the construction of a single word can unleash a wave of litigation. For example, in the environmental insurance coverage setting, almost every state litigated the meaning of the term "damages." Further, policyholders will construe terms broadly, as indeed the rules of insurance policy construction demand in almost every jurisdiction. Insurance companies will construe policy terms narrowly, in an attempt to repel new liabilities. While the general liability policy was supposed to be elastic to adapt to new exposures, the opposite has proven true. These trends have been true in every type of coverage litigation.

Data Breach Insurance Coverage

If "privacy" was the key term of contention in the fight over insurance coverage for junk-fax liability, then "publication" served the same purpose in the struggle for insurance coverage for data breach under general liability policies. Only about six decisions address this issue. Whether other claims settled or whether new cyber exclusions choked off further claims remains unknown.

Zurich American Insurance v. Sony, No. 615982/2011 (N.Y. Sup. Ct. March 4, 2014) is a leading case in this area. The trial court held that a general liability policy did not cover data breach caused by hacking because the term "publish" required an affirmative act by the policyholder, and the data breach involved no such act. The case settled on appeal after oral argument.

Only one state supreme court case has addressed data breach under a general liability policy. That case—*Recall Total Info. Mgmt. v. Federal Insurance*, 115 A.3d 458 (Conn. 2015)—involved unusual facts, as will often be the case with cyber liability. Computer tapes containing personal information fell out of the back of a truck. When people went back to recover the tapes, they were gone. However, the tapes never surfaced, and no complaints arose that the loss compromised anyone's personal information. The court held that no evidence of "publication" existed, and therefore, the policy provided no coverage. But see *Travelers Indem. Co. of Am. v. Portal Healthcare Solutions*, 35 F. Supp. 3d 765 (E.D. Va. 2014) (publication occurs when information is "placed before the public," not when it is viewed).

The emerging TCPA and cyber exclusions follow a pattern wherein the insurance industry excludes a risk from general liability coverage and formulates a specialty policy to cover that risk when the insurance industry thinks it has sufficient actuarial data. Certain of these policies, such as employment practices and pollution legal liability, have enjoyed a measure of success. The issue

now is whether the insurance industry can develop cyber insurance policies that meet the needs of their customers.

Computer Coverage by Endorsement

In recent months, at least four cyber insurance coverage cases have been filed or decided under the computer endorsements to financial institution bonds, crime policies, and executive risk policies. All of these cases involved "phishing," a type of hacking wherein the phisher contacts a company employee and convinces him or her, under false pretenses, to send money to a third party—which is, of course, the phisher. The insurance companies in these cases have all denied coverage for these phishing claims. The insurance companies distinguished between an outside party hacking into the policyholder's computer network, which they admit is covered, and a third party effecting a funds transfer by the company through phishing. Of course, the victim is defrauded regardless of the approach the hacker takes.

In *Universal Am. v. National Union Fire Insurance Co. of Pittsburgh, Pa.*, 37 N.E.3d 78 (N.Y. 2015), the New York Court of Appeals interpreted a rider to a financial institution bond that stated:

> COMPUTER SYSTEMS
> It is agreed that:
> 1. The attached bond is amended by adding an Insuring Agreement as follows:
> COMPUTER SYSTEMS FRAUD
> Loss resulting directly from a fraudulent
> (1) entry of Electronic Data or Computer Program into, or
> (2) change of Electronic Data or Computer Program within the Insured's proprietary Computer System
> …
> provided that the entry or change causes
> (a) Property to be transferred, paid or delivered,
> (b) an account of the insured, or of its customer, to be added, deleted, debited or credited, or
> (c) an unauthorized account or a fictitious account to be debited or credited

While the court's factual exposition is sparse, this case appears to concern phishing—an authorized user's entry of fraudulent data resulting in an $18,000,000 loss. The insurance company asserted that the rider applied only to a third party's—as opposed to an authorized user's—fraudulent entry of false data. The court held that the rider was not ambiguous, and ruled in the insurance company's favor. But see *Apache Corporation v. Great American Ins.*, No. 4:14-CV-237, 2015 U.S. Dist. LEXIS 161683, at *9 (S.D. Tex. Aug. 7, 2015) (finding coverage where phishing fraud constituted the "direct" cause of the loss).

Certainly, policyholders will challenge this decision, and argue that the rider is ambiguous in the context of fraudulent users versus fraudulent content. Several other cases with similar facts are pending. This issue could produce an outbreak of coverage litigation. It bears on the key aspect of coverage litigation—an insurance company narrowly construing its policy to evade emerging liabilities.

'Columbia Casualty': Ripple or Tidal Wave

Columbia Casualty Company v. Cottage Health System, Case No. 2:15-cv-03432 (C.D. Cal. filed May 7, 2015) involves the first complaint filed under a cyber policy addressing a specifically cyber issue. Cottage was sued for a data breach resulting from its failure to encrypt data that was Internet-accessible.

Columbia Casualty's policy had a "Minimum Required Practices" provision, which required Cottage to maintain the procedures and risk controls that Cottage had identified in its application. The policy also had a provision stating that, inter alia, the representations in the application were material and that Columbia Casualty had relied on them. In its complaint, Columbia Casualty alleged that some of the answers in Cottage's application were false.

Many policies contain provisions similar to Columbia Casualty's. Since most cyber liability results from a risk control system's failure, the Minimum Required Practices provision often comes into play. An insurance company has the right to ask objective questions about system security in its application. Such objective questions must be distinguished from subjective exclusions that require the policyholder's system to be "reasonable," "current," or "up-to-date." Such exclusions invite insurance coverage litigation.

Conclusion

Certainly, the trajectory of insurance company denials under general liability and other insurance policies raises concerns. However, cyber policies are designed specifically for these risks. As noted anecdotally, insurance companies have been paying on these claims. However, cyber losses are growing in frequency and intensity. Insurance companies are reportedly tightening underwriting standards and increasing premiums on cyber policies. Will they also issue more coverage denials?

Cyber policies differ in critical ways from general liability policies. Although the insurance industry will deny it, they purposely drafted general liability policies broadly to respond to emerging risks, which the policies have failed to do. This phenomenon causes the majority of coverage litigation.

Insurance companies argue that they write cyber policies narrowly on purpose, to expose themselves only to known risks. A policy may contain over 50 definitions and 30 exclusions. As cyber liability grows and transmutes, it may slacken the insurance industry's appetite for cyber risks. Currently, the coverage battle over phishing best illustrates this trend. The insurance industry was familiar with hacking. It was a known risk that the industry was willing to underwrite. To the corporation, no essential difference existed between hacking and phishing—both resulted in the same loss. To the insurance companies, the difference was crucial. They understood the risk of hacking and intended to write coverage for it. Phishing presented a new risk that they did not intend to cover. This is an example of why cyber insurance litigation may develop in the near future. Policyholders will look for broad constructions of cyber policies to provide coverage for emerging risks, while insurance companies will attempt to hold the line at a narrow construction of the policy limited to enumerated claims.