THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

The IDC Monograph

Patrick D. Cloud
Heyl, Royster, Voelker & Allen, P.C., Edwardsville

William K. McVisk
Tressler LLP, Chicago

Seth D. Lamden
Neal, Gerber & Eisenberg LLP, Chicago

Georgia L. Joyce
Bodell Bove LLC, Chicago

Jamie L. Hull
Kaufman Dolowich & Voluck LLP, Chicago

C. William Busse, Jr.
Busse & Busse, P.C., Chicago

Henry W. Goldman
Busse & Busse, P.C., Chicago

Rise of the Machines: Cyber-Based Liability and Its Attendant Coverage Questions

I. INTRODUCTION

In modern America, interconnected data networks have quickly become ubiquitous and essential to economic life. However, as these interconnected networks have risen, new risks of loss have arisen as well. Today, news outlets are filled with stories of computer fraud and network hacking. The manner in which liability for the losses caused by these new risks is spread among potentially responsible parties and their insurers continues to evolve in novel ways. This paper provides an overview of an insured company's potential liability to third parties for data breaches or other cyber risks and whether and to what extent these risks may or may not be covered by the company's insurer on either a first-party or third-party basis.

THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

II. Overview of Cyber-Related Claims Associated with Security Breaches

A. Substantive Theories of Data Breach Claims

The increased potential liability for cyber-related and data breach claims against an insured business has tracked the rise of the interconnected electronic data systems in today's modern internet-focused economies. These claims typically stem from the penetration or breach of a network and the exploitation or theft of personal, confidential information. Defendants implicated in cyber-related claims include almost any business that uses computer networks subject to unauthorized infiltrations, such as grocery stores,[1] consumer merchant retailers,[2] email service providers,[3] credit reporting agencies,[4] financial institutions,[5] and even video game producers.[6] Plaintiffs typically pursue these claims as class actions,[7] and, although the plaintiffs in these claims are usually individuals,[8] businesses occasionally assert them.[9]

In pursuing these claims, plaintiffs utilize a variety of liability theories, such as negligence and negligence *per se*, contract or quasi-contract, state consumer fraud, and other state-specific statutes.[10] However, the relatively modern and novel nature of these claims sometimes makes them an ill fit for traditional legal paradigms and can create a number of hurdles that the parties must face. *In re Michaels Stores Pin Pad Litigation*[11] illustrates many of the issues that can affect the substantive theories pursued in these cases. In this case, consumers filed a purported class action against Michaels Stores (a specialty arts and crafts retailer) after it was discovered that hackers had tampered with approximately 90 credit card and debit card PIN pads in up to 80 Michaels stores across 20 different states.[12] The consumers asserted that Michaels failed to use appropriate safeguards to protect against PIN pad tampering, failed to adequately protect their credit card and debit card information, and failed to promptly and properly notify consumers of the security breach.[13] According to the consumers, Michaels failed to adhere to the standards and requirements established by members of the payment card industry, such as VISA, to protect against PIN pad tampering.[14] The consumers further asserted that the PIN pad tampering resulted in unauthorized withdrawals from their bank accounts and unauthorized bank fees.[15]

In *Michaels Stores*, the consumers' complaint asserted a variety of causes of action, including a purported violation of the Stored Communications Act, the Illinois Consumer Fraud and Deceptive Business Practices Act (Illinois Consumer Fraud Act), negligence, negligence *per se*, and breach of implied warranty.[16] Michaels moved to dismiss this complaint, which the District Court for the Northern District of Illinois granted in part and denied in part.

The court dismissed the plaintiffs' claims under the Stored Communications Act, which prohibits a provider of "electronic communication service" or "remote computing service" to the public from "knowingly divulg[ing] to any person or entity" contents of communications stored, carried, or maintained by the service provider.[17] The court reasoned that it could not find that Michaels–a retailer of arts and crafts–qualified as either a provider of "electronic communication service" or "remote computing service" within the meaning of the Stored Communications Act.[18]

The court also dismissed the plaintiffs' negligence and negligence *per se* claims. The court rejected Michaels' argument that the hackers' intervening criminal acts broke the chain of causation. Although the court recognized that generally "a defendant will not be held liable for negligence if an intervening criminal act causes the plaintiff's injury," the court also noted that "an exception exists where the defendant's acts or omissions create a condition conducive to a foreseeable intervening criminal act."[19] The court concluded that the allegations of the complaint satisfied this exception because Michaels' alleged failure to follow the standards established by the payment card industry to protect against PIN pad tampering "created a condition conducive to a foreseeable criminal act."[20]

Nevertheless, the court found that the economic loss doctrine precluded the negligence claims. It was undisputed that the plaintiffs sought to recover purely economic losses, and, in Illinois, the "economic loss rule bars a plaintiff from recovering for purely economic losses under a tort theory of negligence."[21] The plaintiffs argued that their claims fell within an exception to the economic loss doctrine[22] because "Michaels breached a duty owed to plaintiffs independent of any contractual obligation or warranty."[23] The district court rejected this assertion, finding that this exception to the economic loss doctrine "only applies to professional malpractice claims where the ultimate result of the defendant's work is intangible," and "[p]laintiffs' negligence claims do not relate to professional malpractice and the ultimate result of the transaction was the sale of products to [p]laintiffs, not the provision of intangible services."[24]

The plaintiffs, however, fared better on their Illinois Consumer Fraud Act and implied contract claims. For plaintiffs' Illinois Consumer Fraud Act claim, the district court sided with Michaels that plaintiffs failed to allege the presence of a "deceptive practice" within the meaning of the Illinois Consumer Fraud Act because "a plaintiff cannot maintain an action under the [Illinois Consumer Fraud Act] for a deceptive practice absent some communication from the defendant, either a communication containing a deceptive misrepresentation or a deceptive omission."[25]

But, the court did agree that plaintiffs set forth an unfairness claim. According to the court, under the Federal Trade Commission criteria for unfair conduct, a company's lack of cyber security measures coupled with a failure to timely notify of a security breach could constitute "an unfair practice because such conduct is systematically reckless, 'aggravated by [a] failure to give prompt notice when lapses were discovered internally, and causing very widespread and serious harm to other companies and to innumerable consumers.'"[26] The court found that the allegations against Michaels supported the presence of an unfairness claim under this theory.[27] Similarly, the district court found that a violation of the Illinois Personal Information Protection Act can constitute an unfair practice under the Illinois Consumer Fraud Act, and the court found that a violation of the Illinois Personal Information Act was adequately plead.[28]

Finally, the court found that plaintiffs stated a claim for a breach of an implied contract. Following the reasoning adopted by other courts, the court noted "that a jury could reasonably find an implied contract between the defendant and its customers that the defendant would take reasonable measures to protect the customers' financial information."[29] As such, the court found sufficient allegations to "demonstrate the existence of an implicit contractual relationship between [p]laintiffs and Michaels, which obligated Michaels to take reasonable measures to protect [p]laintiffs' financial information and notify [p]laintiffs of a security breach within a reasonable amount of time."[30]

B. The Damages Framework for Data Breach Claim

In addition to navigating the application of traditional substantive causes of action, another key question that courts must consider in data breach cases is whether the plaintiff alleged a sufficient injury to establish standing. Article III standing requires the demonstration of the presence of "a concrete and particularized injury that is fairly traceable to the challenged conduct and is likely to be redressed by a favorable judicial decision."[31] However, it is certainly arguable that some victims of a data breach never suffer any actual damages. For example, in some circumstances, the bank or credit card company will decline a fraudulent charge. Some credit card companies offer a "zero liability" feature. Oftentimes, the victim is reimbursed for a fraudulent charge.[32]

Several cases from the Court of Appeals for the Seventh Circuit have grappled with these issues in the context of standing for data breach cases.[33] Each has set the bar relatively low for a victim of a data breach to establish damages for standing. In *Remijas v. Neiman Marcus Group*,[34] the Seventh Circuit addressed the question of standing and damages in

a class action lawsuit that arose from a data breach at a Neiman Marcus store where approximately 350,000 credit card numbers were exposed to hackers' malware.[35] The plaintiffs alleged several theories of damages, including (1) recovery for lost time and money resolving the fraudulent charges, (2) recovery for lost time and money protecting themselves against future identity theft, (3) recovery for the financial loss of buying items at Neiman Marcus that they would not have purchased had they known of the store's careless approach to cybersecurity, and (4) recovery for lost control over the value of their personal information.[36] The plaintiffs also alleged that they had standing based on two imminent injuries: (1) an increased risk of future fraudulent charges and (2) greater susceptibility to identity theft.[37] The district court dismissed the suit for lack of Article III standing, finding that the plaintiffs could not properly plead damages to establish standing.[38]

In its review of the case, the Seventh Circuit noted that Article III's standing requirement meant that the plaintiffs must allege that the data breach caused a concrete, particularized injury to them; that Neiman Marcus caused that injury; and that a judicial decision could provide redress for them.[39] According to the Seventh Circuit, allegations of future harm can also establish Article III standing if that harm is "certainly impending," but "allegations of possible future injury are not sufficient."[40]

In reversing the district court and finding that the plaintiffs established standing, the Seventh Circuit reasoned that standing could be "based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."[41] In this case, according to the court, it would certainly be plausible to infer that the plaintiffs have shown a substantial risk of harm from the data breach since the very purpose of the hack was, sooner or later, to make fraudulent charges or assume those customers' identities.[42] Indeed, according to the court, requiring the plaintiffs to wait for the threatened harm to materialize in order to sue would create other problems for the plaintiffs. For instance, the more time that passes between a data breach and an actual instance of an identity theft, the more latitude a defendant has to argue that the identity theft is not, "fairly traceable" to the defendant's data breach.[43]

The court also rejected the defendant's argument that mitigation expenses do not qualify as actual injuries where the harm is not imminent. Distinguishing the Supreme Court's decision in *Clapper v. Amnesty International*, the Seventh Circuit noted that, in *Clapper*, the Supreme Court addressed a speculative harm based on something that may not even happen to some or all of the plaintiffs.[44] Conversely, in this case, the plaintiffs' risk of harm was not speculative because the defendant conceded that the security breach took place.[45]

The Seventh Circuit dealt with similar issues in *Lewert v. P.F. Chang's China Bistro, Inc*.[46] In *Lewert,* two diners at P.F. Chang's restaurants who used a credit or debit card to purchase dinner brought a putative class action against P.F. Chang's after it announced its computer system had been breached and that some consumer credit and debit card information had been stolen.[47] One plaintiff alleged that fraudulent charges were made using his debit card after the breach. Although his bank did not put the charges through, he immediately canceled the card and then purchased a credit monitoring service for $106.89 to protect him against identity theft.[48] The other plaintiff did not discover any fraudulent charges or cancel his card, but, after the breach was announced, he allegedly spent time and effort monitoring his card statements and his credit report to ensure that no fraudulent charges had been made and that no fraudulent accounts were opened in his name.[49]

The district court dismissed the case for lack of standing, and the Seventh Circuit reversed. Relying on *Remijas*, the Seventh Circuit found that the plaintiffs alleged types of damages that established standing.[50] The plaintiffs alleged an increased risk of fraudulent charges and identity theft because their data had been stolen. One was at risk for both fraudulent charges and identity theft. Although the other had already canceled his debit card, he was still at risk of identity

theft.[51] Additionally, although neither plaintiff lost any money as a result of the breach, one of the diners expended funds to obtain a credit monitoring service while the other spent time and effort monitoring his card statements and his credit report after the breach.[52] The court held that these were the same type of damages that the plaintiffs in *Remijas* had suffered and were enough to allege the damages required for Article III standing.[53]

III. Presence of Coverage for Cyber-Related and Data Breach Claims

Understanding the basic contours of cyber-related and data breach claims, the question is whether they are covered. Like any insurance coverage question, whether and the extent of coverage for cyber-related or data breach claims (either on a first party or third party basis) depends on the particular language of the policy. However, from a broad view, the coverage picture can be driven by whether the policy contains endorsements or other language addressing the particular risks presented by cyber-related or data breach claims.

A. Coverage of Cyber-Related and Data Breach Claims Under Commercial Property and Commercial General Liability Policies

i. Cyber-Related and Data Breach Claims Under First-Party Policies

Although there are now insurance products specifically designed to cover cyber risks, companies whose property or business operations are impaired by reason of such events may also potentially obtain coverage under their traditional property/casualty insurance policies, such as standard-form first-party property and business interruption policies. These types of potential exposures are referred to in the insurance industry as "silent cyber"—the coverage of cybersecurity-related losses under traditional insurance policies that are not expressly designed to cover cyber losses. An example under a first-party property and business interruption policy would be a ransomware attack that caused computer systems to be inoperable resulting in business interruption.

The courts have split on the issue of whether lost data or software is covered under traditional first-party property policies. Some courts have held that electronically stored data does not constitute tangible property for purposes of property or business interruption coverage.[54] Other courts have found to the contrary, holding that the destruction or impairment of electronic data is sufficient to constitute "direct physical loss of or damage to property."[55] In addition, some cases have held that the inability to use a computer due to damaged data may constitute a "loss of use" and thus covered property damage under a first-party policy.[56] For instance, in *Lambrecht & Associates v. State Farm Lloyds*, the court specifically held that "physical damage" was not restricted to physical destruction to the computer's circuitry but also included loss of access, loss of use, and loss of functionality.[57]

In response to decisions finding coverage for lost or damaged data as property damage under traditional first-party property policies, many insurers responded by taking steps to exclude electronic data from the definition of tangible property and provide coverage under an optional "Additional Coverage" that is subject to a low sublimit. The Insurance Services Office (ISO) 2007 Commercial Property Form exempts "electronic data" from the definition of "Covered Property" and provides coverage under an "Additional Coverage" that is limited to "$2,500 for all loss or damage sustained in any one policy year, regardless of the number of occurrences of loss or damage or the number of premises, locations or computer systems." Moreover, the 2007 ISO standard form Business Income (and Extra Expense) Coverage

Form excludes coverage for electronic data under the main coverage part and provides coverage under an "Additional Coverage" subject to a $2,500 limit for "all loss sustained and expense incurred in any one policy year, regardless of the number of interruptions or the number of premises, locations or computer systems involved." Accordingly, even assuming the property policy provides coverage for damage to electronic data, the policy will afford only a small amount of coverage.

Crime policies also generally insure against first-party losses against various forms of theft as well as third-party losses for theft, forgery, and various other crimes injuring a third party. Insureds are increasingly looking to their crime policies for coverage in cases involving hacking and social engineering losses, *i.e.* losses that result from a criminal tricking a policyholder into wiring funds to a criminal's bank account (phishing, spear phishing, and whaling). Once again courts are split on these issues with some courts finding coverage.[58]

While another recent decision found a lack of coverage under the crime policy, the matter was remanded for the trier of fact to decide whether the insurer's disclaimer contained in its insurance quote was sufficient to rebut what the court found was "misleading language" contained in the quote and the suggestion that a loss from a computer hacker was covered.[59] Accordingly, at least in some instances, an insurer will need to review its marketing language to avoid the potential that such language could be utilized by an insured to assert a fraudulent inducement argument against the insurer to create coverage that typically does not exist.

Other courts have found no coverage under crime policies for cyber-related losses, holding that the use of email in a fraudulent scheme is not enough to trigger such coverage if the email use was "merely incidental" to the fraud.[60] Courts have also determined no coverage is afforded for cyber-related losses based on various exclusions contained in the crime policies.[61] Additionally, as with property coverage, some insurers are now addressing these cyber-related risks by offering specific endorsements that address social engineering risks with more specificity and with various sublimits.

ii. Cyber-Related and Data Breach Claims Under Commercial Liability Policies

Policyholders often seek coverage for cyber-related and data breach claims under third party liability coverage forms, with little success. The standard commercial liability policy provides two forms of coverage: Coverage A – Occurrence-Related Property Damage or Bodily Injury Coverage and Coverage B – Personal and Advertising Injury Coverage.[62] Neither coverage provides fertile grounds for cyber-related and data breach claims.

1. Coverage A: Occurrence-Related Property Damage and Bodily Injury Coverage

The standard CGL policy drafted by ISO provides coverage for damages because of bodily injury or property damage caused by an "occurrence."[63] "Property damage" includes both physical injury to tangible property and the loss of use of tangible property that is not physically injured.[64] Prior to 2001, CGL policies were silent as to whether data constituted tangible property.[65]

When coverage disputes began to arise in the late 1990s and early 2000s regarding whether CGL policies cover cyber liability and data-related claims, ISO issued a series of amendments to the CGL policy form designed to limit or eliminate coverage for such claims. For example, disagreements arose between insureds and their insurers with regard to whether data loss could constitute covered "property damage" under the pre-2001 edition CGL forms. Although most courts held that data was not "tangible property," and thus not covered, some courts disagreed and found coverage.[66]

In response to this uncertainty over whether data was considered covered tangible property, ISO amended the definition of "property damage" to specify that electronic data is not tangible property in the October 2001 edition of the ISO CGL form.[67] The 2001 amendment to the definition of "property damage" did not completely eliminate coverage for claims involving computer programs and software. While liability for damage to data itself may not be covered under the tangible property limitation included in 2001, claims seeking damages due to the loss of use of tangible property (*e.g.*, a computer or server) caused by damage to data (*e.g.*, software) still could be covered.[68] Even after the 2001 amendment, coverage for claims alleging loss of use of tangible property arising out of the insured's software or data would be covered unless "the repair, replacement, adjustment or removal" of the insured's software, without more, would completely restore the claimant's property; in this case, the "impaired property" exclusion would eliminate coverage.

ISO decided to further strengthen the intent to remove coverage for damage to data in the 2004 revision to the CGL policy. This time, a specific exclusion for data-related loss of use claims was added to the policy. This exclusion states, in relevant part, that CGL coverage does not apply to "[d]amages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data."[69] While insureds had almost no success seeking coverage for cyber losses under CGL policies before these amendments, not surprisingly, they have had even less success after these amendments.

Camp's Grocery, Inc. v. State Farm Fire & Casualty Co.[70] illustrates some of the challenges faced by insureds attempting to procure coverage for a data breach under a traditional CGL policy. The plaintiffs in the underlying lawsuit in *Camp's Grocery* were three credit unions that alleged that Camp's' computer network was hacked, exposing customers' confidential data, including their credit card, debit card, and check card information. The credit unions claimed that the breach caused them to suffer monetary losses associated with reissuing compromised cards, reimbursing customers for fraud losses, lost interest and transaction fees, and other expenses.[71] The credit unions claimed that Camp's was liable for the breach because it failed to provide adequate computer systems, employee training, encryption, and intrusion and detection systems.[72]

Camp's tendered its defense to State Farm, which had issued a business liability policy to Camp's with policy language that largely tracked the language of the ISO CGL form and also contained some first-party coverages. The liability coverage part of the policy required State Farm to "pay those sums that [Camp's] becomes legally obligated to pay as damages because of . . . property damage . . ." caused by an "occurrence," but the policy specified that "property damage" does not include damage to "electronic data."[73] This coverage expressly required State Farm to defend claims seeking covered damages.[74] In addition to the preceding coverages, the State Farm policy contained an "Inland Marine Computer Property Form" that covered, among other things, "accidental direct loss to . . . 'electronic data.'"[75] The Inland Marine Computer Property Form did not provide for a defense or indemnity for third-party claims.

State Farm rejected Camp's request for coverage because: (1) the Inland Marine Computer Property Form did not provide liability coverage; and (2) the liability coverages in the State Farm policy expressly stated that "property damage" did not include "electronic data."[76] The court agreed with State Farm, holding that the Inland Marine Computer Property Form only provided first-party coverage and, therefore, did not require it to defend or indemnify Camp's for the underlying suit.[77] In so ruling, the court rejected the insured's argument that provisions in the Inland Marine Computer Property Form giving State Farm the right, but not the duty, "to defend [Camp's], at [State Farm's] expense, against suits arising from claims of owners of property" meant that the Inland Marine Computer Property Form also provided third-party coverage.[78] As the court explained, a provision that permits an insurer to elect to defend does not create a duty to defend.[79]

The *Camp's Grocery* court also rejected the policyholder's argument that the underlying suit sought damages for covered property damage, thereby triggering the policy's liability coverage part, because the credit unions alleged that they suffered "losses for replacement debit and credit cards."[80] The court explained that there were no allegations that Camp's acts or omissions caused physical damage to the cards; rather, Camp's acts or omissions caused damage to electronic data stored on the cards, and damage to electronic data was expressly excluded from the liability coverage part of the policy.[81]

2. Coverage B: Personal and Advertising Injury Coverage

Given the lack of success in finding coverage under Coverage A of a traditionally written CGL policies, insureds often turn to the personal and advertising injury provision of Coverage Part B. The term "personal and advertising injury" is defined as follows:

14. "Personal and advertising injury" means injury, including consequential "bodily injury", arising out of one or more of the following offenses:

a. False arrest, detention or imprisonment;

b. Malicious prosecution;

c. The wrongful eviction from, wrongful entry into, or invasion of the right of private occupancy of a room, dwelling or premises that the person occupies, committed by or on behalf of its owner, landlord or lessor;

d. Oral or written publication, in any manner, of material that slanders or libels a person or organization or disparages a person's or organization's goods, products or services;

e. Oral or written publication, in any manner, of material that violates a person's right of privacy;

f. The use of another's advertising idea in your "advertisement"; or

g. Infringing on another's copyright, trade dress or slogan in your "advertisement".[82]

None of these categories, however, easily encompasses an insured's liability for failure to prevent a data breach, and two courts have agreed that such liability does not fall within the definition of "personal and advertising injury" for coverage under a CGL policy. For example, in *Innovak International, Inc. v. Hanover Insurance Co.*,[83] the insured, Innovak, was named as a defendant in several putative class action suits alleging damages from the release of their personal private information after Innovak was the subject of a data breach.[84] The suits alleged that Innovak was the subject of a data breach when hackers appropriated the plaintiffs' private information Innovak stored on its software database, including social security numbers, addresses, telephone numbers and other identifying information.[85] The plaintiffs claimed that Innovak was negligent, and also sought damages for breach of implied contract, gross negligence,

unjust enrichment and fraudulent suppression.[86] As a result, the plaintiffs claimed that they suffered "psychic injuries" including "stress, nuisance, loss of sleep, worry, and the annoyance of having to deal with issues resulting from the Innovak data breach."[87]

Innovak tendered the defense of these class action suits to Hanover, which denied coverage. Hanover disclaimed coverage under Coverage A because the suits only alleged "psychic injury", and the policy only covered mental anguish, shock or fright if they result from "'bodily injury', sickness or disease."[88] Hanover additionally denied coverage because Coverage A only covers injuries resulting from an "occurrence", which is defined as an accident, and the plaintiffs' claims were based on the intentional acts of third party hackers.[89] Finally, Hanover denied under Coverage A because the information appropriated by the hackers was intangible, so it could not constitute "property damage" as defined in the policy.[90]

Hanover further argued that the plaintiffs' claims did not fall within Coverage B because Coverage B "necessarily requires an act or conduct by the Insured for coverage to be present." However, the suit alleged only that third-party hackers caused the data breach, not the insured.[91]

Notably, Innovak did not contend that the data breach fell within Coverage A. Instead, it argued that it fell within Coverage B because the underlying suits alleged that Innovak negligently prepared, designed and published software that allowed private personal information to be known by third parties.[92] It further maintained that Coverage B provided coverage for claims alleging any publication of material that violates a person's right of privacy, whether the publication is directly or indirectly committed by the insured.[93]

The court rejected Innovak's argument because the underlying complaint did not allege a publication by Innovak.[94] As the court explained, the underlying complaint did not allege that plaintiffs' private information was ever "published" by anyone, either the hackers or Innovak. More importantly, though, even if there was some allegation of a publication, it was not a publication by the insured. Innovak maintained that the complaint alleged that it had published the software, which was hacked, allowing the plaintiffs' information to be obtained. However, the court explained that the publication of the software itself did not violate the plaintiffs' right of privacy as is required for Coverage B.[95]

Innovak then pointed to the language of the definition of "personal and advertising injury" which the policy defined as the oral or written publication "in any manner" of material which violates a person's right to privacy.[96] Innovak contended that the words "in any manner" included both direct publication by Innovak and the negligent failure to prevent third parties from obtaining private information. The court rejected this contention, relying on an unpublished New York decision, *Zurich American Insurance v. Sony Corporation of America*,[97] which determined that the words "in any manner" indicated the medium or the kind of way it is being publicized rather than who actually makes the publication.[98] The court stated that even if it accepted the argument that an indirect publication by Innovak was sufficient, there were no allegations of even an indirect publication. As the court explained, the allegation that Innovak failed to implement sufficient security safeguards was not an allegation of indirect publication or any publication at all.[99]

In another case involving a data breach, *St. Paul Fire & Marine Insurance Co. v. Rosen Millennium, Inc.*,[100] the court came to a similar conclusion. The insured provided data security services to a hotel corporation, which became aware of a potential credit card breach at one of its hotels. The data breach was determined to be the result of malware installed on its payment network, which caused customers' credit cards to be affected. The insured made a claim under its CGL policy, but the insurer denied coverage. The insured contended that the customers' loss of use of their credit cards was covered as "property damage" and that the data breaches fell within the personal injury offense of publication of material which violates a person's right to privacy.

The court did not address whether the loss of use of credit cards would constitute "property damage" under a CGL policy because there was no underlying suit and the demand letter from the claimant to the insured said nothing about the customers' loss of use of their credit cards.[101] With respect to the personal and advertising injury, the court agreed with the decision in *Innovak* and ruled that the personal and advertising injury coverage under a CGL policy covered only the insured's publication of private material, not from the actions of third parties.[102]

B. Policy Provisions and Endorsements Specifically Applicable to Cyber-Related or Data Breach Claims

i. First-Party Coverage

A first-party policy with a "computer fraud" coverage provision does not guarantee coverage for a loss caused by the use of a computer to perpetrate fraud. Rather, as expected and as illustrated by the following cases, the language of the computer endorsement, facts of the case, and applicable standard of causation for coverage can lead to very different results.

1. Interpreting the Causation Standard for Coverage for a Computer Fraud Rider

In *Retail Ventures, Inc. v. National Union Fire Insurance Company of Pittsburgh, PA.*,[103] the Court of Appeals for the Sixth Circuit interpreted the causation standard applicable to a computer fraud rider of a crime policy and affirmed the judgment in favor of plaintiffs, Retail Ventures, Inc., DSW Inc., and DSW Shoe Warehouse, Inc. Specifically, the court found coverage under the computer fraud rider to a "Blanket Crime Policy" for losses resulting from a computer hacking scheme that compromised customer credit card and checking account information for more than 1.4 million customers of 108 DSW Shoe Warehouse stores.[104]

In this case, the hackers used the local wireless network at one DSW store to gain access to DSW's main computer system, subsequently downloading credit card and checking account information.[105] Plaintiffs incurred more than $6.8 million in stipulated losses and prejudgment interest, of which $4 million was for costs associated with charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard in connection with the compromised credit card information.[106]

The coverage provision at issue was entitled "Computer & Funds Transfer Fraud Coverage" found in Endorsement 17 of the policy. It provided in relevant part that National Union agreed to pay the insured for: "Loss which the Insured shall sustain resulting directly from: A. The theft of any Insured property by Computer Fraud; . . . ."[107] "Computer Fraud" was defined as "the 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."[108] Coverage under Endorsement 17 applied "only with respect to . . . Money or Securities or Property located on the premises of the Insured."[109]

National Union did not dispute that the unauthorized access and copying of customer information stored on plaintiffs' computer system involved the "theft of any Insured property by Computer Fraud."[110] The issue in dispute was whether

the district court correctly found that the loss plaintiffs sustained was loss "resulting directly from" the theft of insured property by computer fraud.[111]

The district court predicted, in this case of first impression, that the Ohio Supreme Court would follow those cases that interpret "resulting directly from" as imposing a traditional proximate cause standard in this context.[112] The district court concluded that "there is a sufficient link between the computer hacker's infiltration of [p]laintiffs' computer system and [p]laintiffs' financial loss to require coverage under Endorsement 17."[113] National Union argued it was error to apply the proximate cause standard.[114]

The Sixth Circuit agreed with the district court that the Ohio Supreme Court would apply a proximate cause standard to determine whether plaintiffs sustained a loss "resulting directly from" the "theft of Insured property by Computer Fraud."[115] Although plaintiffs could not cite any Ohio decision where the court applied proximate cause in the context of a fidelity bond or commercial crime policy, the Sixth Circuit noted that plaintiffs identified a few Ohio court decisions in which the court applied a proximate cause standard to determine whether there was a "direct loss" under other kinds of first-party coverage.[116]

The Sixth Circuit rejected National Union's position that the "resulting directly from" language required the theft of property by computer fraud to be the "sole" and "immediate" cause of the insured's loss, *i.e.,* the "direct-means-direct standard," noting that National Union did not identify any Ohio decisions that declined to apply a proximate cause standard in determining "direct" loss.[117]

The Sixth Circuit also found that the meaning of the phrase "resulting directly from" in the context of Endorsement 17 was ambiguous:

> [W]e find that the phrase "resulting directly from" does not unambiguously limit coverage to loss resulting "solely" or "immediately" from the theft itself. In fact, Endorsement 17 provided coverage for loss that the insured sustained "resulting directly from" the "theft of any Insured property by Computer Fraud," which includes the "wrongful conversion of assets under the direct or indirect control of a Computer System by means of . . . fraudulent accessing of such Computer System."[118]

The Sixth Circuit further held that the exclusion in Paragraph 9 of Endorsement 17 did not bar coverage. Paragraph 9 provided the following:

> Coverage does not apply to any loss of proprietary information, Trade Secrets, Confidential Processing Methods, or other confidential information of any kind.[119]
>
> ***
>
> [T]he stolen customer information was not "proprietary information" at all, since the information is owned or held by many, including the customer, the financial institution, and the merchants to whom the information is provided in the ordinary stream of commerce.[120]

The Sixth Circuit also rejected National Union's argument that the customer information came within the broad "catch-all" clause excluding coverage for "loss of . . . confidential information of any kind."[121] Under the principle of *ejusdem generis*, the general term must take its meaning from the specific terms with which it appears. The phrase "loss of . . . confidential information of any kind" should be interpreted as part of the phrase "proprietary information, Trade

Secrets, [and] Confidential Processing Methods", which are "specific terms that all pertain to secret information of *Plaintiffs* which involves the manner in which the business is operated."[122] The Sixth Circuit, therefore, found that the district court did not err in finding that the loss was not excluded by Paragraph 9 of Endorsement 17.[123]

2. Concurrent Causation Doctrine Applied to Prevent Application of Exclusions in Computer Fraud Claim

In *State Bank of Bellingham v. BancInsure, Inc.*,[124] the Court of Appeals for the Eighth Circuit found that the concurrent causation doctrine applied to prevent the application of certain exclusions to a computer fraud claim. The Eighth Circuit affirmed the district court's grant of summary judgment in favor of the State Bank of Bellingham, finding coverage under the financial institution bond[125] issued by BancInsure for a loss resulting from unauthorized wire transfers despite the fact that employees failed to follow policies and procedures.

In this case, Bellingham used the Federal Reserve's FedLine Advantage Plus system to make wire transfers.[126] The wire transfers were made through a desktop computer connected to a Virtual Private Network device provided by the Federal Reserve. To complete a wire transfer via FedLine, two employees had to enter their individual usernames, insert individual physical tokens into the computer, and type in individual passwords and passphrases.[127]

A Bellingham bank employee completed a FedLine wire transfer by using her token, password, and passphrase, as well as the token, password, and passphrase of a second employee.[128] At the end of the workday, the employee left the two tokens in the computer and left the computer running.[129] When the employee arrived at work the next day, she discovered that two unauthorized wire transfers had been made from Bellingham's Federal Reserve account to two different banks in Poland.[130] The employee was unable to reverse the transfers through the FedLine system and immediately contacted the Federal Reserve to request reversal of the transfers.[131] The Federal Reserve refused to reverse the transfers, but did contact intermediary institutions and was able to reverse one of the fraudulent transfers.[132]

Bellingham sought coverage for the fraudulent transfers under the bond issued by BancInsure, which provided coverage for losses caused by employee dishonesty and forgery, as well as computer system fraud.[133] An investigation determined that a "Zeus Trojan horse" virus had infected the computer and permitted access to the computer for the fraudulent transfers.[134] After its investigation, BancInsure concluded the loss was not covered based on two employee-caused loss exclusions, an exclusion for theft of confidential information, and an exclusion for mechanical breakdown or deterioration of a computer system.[135]

The district court granted summary judgment to Bellingham on its breach of contract claim, finding that "the computer systems fraud was the efficient and proximate cause of [Bellingham's] loss."[136] The court further held that "neither the employees' violations of policies and practices (no matter how numerous), the taking of confidential passwords, nor the failure to update the computer's antivirus software was the efficient and proximate cause of [Bellingham's] loss."[137] The Eighth Circuit affirmed the district court's decision, noting that Minnesota has adopted the concurrent-causation doctrine, under which "[a]n insured is entitled to recover from an insurer when [the] cause of the loss is not excluded under the policy, even though an excluded cause may also have contributed to the loss."[138]

BancInsure also argued that even if the district court correctly applied the concurrent-causation doctrine to the bond, it erred in concluding that the criminal activity of a third party was the "overriding, or efficient and proximate cause of the loss."[139] The Eighth Circuit did not agree, finding that the "efficient and proximate cause" of the loss was the illegal transfer of the money and not the employees' violations of policies and procedures.[140] Even if the employees' negligent

actions "played an essential role" in the loss and created a risk of intrusion into Bellingham's computer system by the virus, the "intrusion and the ensuing loss of bank funds" was not "certain" or "inevitable."[141] The Eighth Circuit concluded, therefore, that the district court properly granted summary judgment.[142]

3. Mere Use of an Email to Advance a Fraud Did Not Create a Covered Claim Under Computer Fraud Coverage

In *Apache Corp. v. Great American Insurance Company*,[143] the Court of Appeals for the Fifth Circuit vacated the district court's award of summary judgment in favor of Apache, finding that Apache's loss resulting from fraudulent instructions to change a vendor's payment information was not covered by the "Computer Fraud" provision of Apache's crime-protection insurance policy.[144]

Apache is an oil-production company based in Houston, Texas that operates internationally. An employee of Apache located in Scotland received a telephone call from a person identifying herself as a representative of Petrofac, one of Apache's vendors, instructing Apache to change the bank-account information for its payments to Petrofac.[145] The Fifth Circuit summarized the relevant facts, as follows:

> Here, the "computer use" was an email with instructions to change a vendor's payment information and make "all future payments" to it; the email, with the letter on Petrofac letterhead as an attachment, followed the initial telephone call from the criminals and was sent in response to Apache's directive to send the request on the vendor's letterhead. Once the email was received, an Apache employee called the telephone number provided on the fraudulent letterhead in the attachment to the email, instead of, for example, calling an independently-provided telephone contact for the vendor, such as the pre-existing contact information Apache would have used in past communications. Doubtless, had the confirmation call been properly directed, or had Apache performed a more thorough investigation, it would never have changed the vendor-payment account information. Moreover, Apache changed the account information, and the transfers of money to the fraudulent account were initiated by Apache to pay legitimate invoices.[146]

Within a month, Apache received notification Petrofac had not received approximately $7 million Apache had transferred to the new (fraudulent) account. Apache recouped a substantial portion of the funds, but claimed it lost approximately $2.4 million.[147] Apache submitted a claim to Great American. The "Computer Fraud" portion of Apache's crime-protection insurance policy stated:

> We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: a. to a person (other than a messenger) outside those premises; or b. to a place outside those premises.[148]

Great American denied coverage on the basis that Apache's "loss did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds."[149] Great American also argued that "coverage under this

[Computer Fraud] provision is 'unambiguously limited' to losses from 'hacking and other incidents of unauthorized computer use.'"[150]

Apache filed a coverage action against Great American. The district court denied Great American's motion for summary judgment, ruling that "the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a 'substantial factor.'"[151] The court further reasoned that, "if the policy only covered losses due to computer hacking, such an interpretation would render the policy 'pointless.'"[152]

Great American relied on several non-Texas decisions interpreting similar computer-fraud language to support of its argument against coverage for Apache's claim. The Fifth Circuit acknowledged that the Supreme Court of Texas has "stressed its policy preference for 'uniformity when identical insurance provisions will necessarily be interpreted in various jurisdictions.'"[153] Great American cited *Pestmaster Services, Inc. v. Travelers Casualty & Surety Company of America*,[154] in which the Court of Appeals for the Ninth Circuit affirmed the district court's denial of coverage where the underlying fraud was committed by a payroll contractor who was authorized to initiate transfers of funds from the insured to the contractor's bank account in order to pay invoices approved by the insured. Instead of paying the invoices, the contractor fraudulently used the insured's funds to pay her own expenses, ultimately leaving the insured indebted to the Internal Revenue Service for payroll taxes. The district court found that "there was no loss when funds were initially transferred to [the contractor] because the transfers were authorized by [the insured]."[155]

In affirming the district court's decision that the Computer Fraud provision did not provide coverage, the Ninth Circuit interpreted "the phrase 'fraudulently cause a transfer' to require an unauthorized transfer of funds.'"[156] "Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a 'General Fraud' Policy", essentially covering losses from all forms of fraud rather than a specified risk category."[157]

Great American also noted that similar policy language was at issue in *Vonage Holdings Corp. v. Hartford Fire Insurance Co.*,[158] in which the district court denied the insurer's motion to dismiss and allowed the insured's claim to go forward. In *Vonage*, however, "the insured was unquestionably 'hacked'—hackers gained access to the insured's servers to fraudulently route international telephone calls."[159]

Here, the Fifth Circuit found that the email purportedly from Petrofac was part of a scheme to defraud Apache; "but, the email was merely incidental to the occurrence of the authorized transfer of money. To interpret the computer-fraud provision as reaching any fraudulent scheme in which an email communication was part of the process would, as stated in *Pestmaster II*, convert the computer-fraud provision to one for general fraud."[160]

4. Fraud Committed Through the Use of a Telephone Was Not "Computer Fraud" Despite the Fact that a Computer Was Involved

In *InComm Holdings, Inc. v. Great American Insurance Company*,[161] the District Court for the Northern District of Georgia found there was no coverage under the Computer Fraud Provision in the policy issued to InComm by Great American for a processing vulnerability by which a debit card holder could cause credit to be loaded onto their debit card in multiples of the credit amount purchased.

InComm provided a service enabling debit card purchasers to load funds onto prepaid debit cards by purchasing "chits" from retailers, such as CVS or Walgreens, for the amount of the chit plus a small service fee.[162] InComm's process consisted of an Interactive Voice Response (IVR) system and Application Processing Servers (APS).[163] The IVR used

eight computers that allowed a debit card holder to request transactions on their debit card account by using telephone voice commands or telephone touch-tone codes.

The best way to understand InComm's debit card processing service is to begin with the flow chart that the court used to illustrate how the chit redemption process worked.[164] The prepaid debit cards were issued by Bancorp Bank (Bancorp). InComm was the Program Manager for Bancorp.[165] Bancorp issues a prepaid debit card to a customer. The customer wants to add $100 to his card and purchases a chit for $100, plus a small administrative fee, at a retailer. The retailer wires $100 from that sale to InComm's Wells Fargo account. InComm wires $100 to Bancorp within 15 days of the chit redemption. When the customer is ready to redeem the $100 chit, the customer calls InComm's IVR system and enters the required information; $100 immediately becomes available on the debit card after that redemption. The customer makes a $100 purchase with the debit card, *e.g.*, uses the debit card to buy a nice dinner. Bancorp transmits $100 to the restaurant to cover the purchase.[166]

Debit card holders pay a one-time fee for each chit they purchase, each chit represents the amount purchased, and each chit is to be redeemed only once.[167] From November 2013 to May 2014, there was a "code error" in InComm's IVR system which permitted chits to be redeemed more than once, allowing cardholders to obtain more chit credit than that for which they paid.[168]

In order to obtain multiple redemptions of a single chit, cardholders used more than one telephone simultaneously to access InComm's IVR system to request redemption of the same chit. The simultaneous redemption requests exploited InComm's coding error, causing the IVR system to send to the APS system a "RedeemReload" request to redeem the chit, followed by a "Reverse" request, which returned the chit to its original, unredeemed status.[169] This allowed cardholders to redeem the same chit, multiple times, using the simultaneous phone call scheme.[170] The unauthorized redemptions caused InComm to wire over $10,000,000 to Bancorp.[171]

InComm notified Great American of its claimed losses resulting from the unauthorized chit redemptions and submitted its sworn proof of loss. Great American denied coverage on the basis that InComm's loss did not result from "the use of any computer" to access the IVR system and because no funds were automatically transferred as a result of the chit cards being reloaded.[172] InComm filed its complaint against Great American alleging breach of contract, statutory bad faith, and declaratory judgment. Great American moved for summary judgment on all counts.[173]

The court, applying Georgia law, analyzed the Computer Fraud Provision in Great American's policy. The policy provided coverage for "computer fraud," specifically, a "loss of . . . money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that [money] from inside the premises or banking premises" to a person or place "outside those premises."[174]

The court considered the provision requiring the transfer to be caused by the "use of any computer" to be fundamental and analyzed whether cardholders who made multiple redemptions of a single chit used a computer to do so.[175] The court found it "undisputed that the cardholders used telephones to provide information to InComm's IVR system, which then processed the information incorrectly, resulting in multiple redemptions of a single chit."[176] Citing the dictionary definitions of "computer", "telephone", and "use", the court disagreed with InComm that the IVR system was the "computer" that was "used" when the chits were redeemed.[177] The court found that a "computer" is not a "telephone" and that InComm's 30(b)(6) representative acknowledged at his deposition that debit card holders used "telephones", not "computers" to engage in multiple redemptions of a single chit.[178]

The court also found that although a computer was "somehow involved" in a loss does not establish that the wrongdoer "used" a computer to cause the loss, noting that computers are used in almost every business transaction. "To

hold so would unreasonably expand the scope of the Computer Fraud Provision, which limits coverage to "computer fraud."[179]

Further, the court found that, even if a computer was "used" to cause InComm's loss, InComm was not entitled to coverage under the Computer Fraud Provision because the "loss" did not result "directly" from the alleged computer use.[180] InComm argued its "loss" occurred when the fraudulently reload chit redemptions caused it to transfer money from its own [Wells Fargo] bank account to the cardholder [Bancorp] account.[181] The court did not agree, finding instead that InComm's loss did not occur until the funds held by Bancorp were paid to the merchant to settle the cardholder's transaction, *e.g.*, the nice $100 dinner.[182] The fact that funds wired to Bancorp as a result of the fraudulent chit redemptions were still in the Bancorp account almost three years after the chits were wrongfully redeemed supported the court's conclusion.[183] In addition, the policy covered only those losses caused by the direct transfer of money from "inside the premises or banking premises" to a person or place "outside those premises."[184] The losses, therefore, did not occur when funds were sent to Bancorp's premises; they occurred when Bancorp sent funds "outside the premises" to the accounts of merchants from which cardholders purchased goods or services.[185]

The court further agreed with Great American that, even if the loss occurred earlier in the process, as InComm claimed, the loss still did not result "directly" from the chit redemptions.[186] Great American argued that InComm's transfer of fraudulently-redeemed chit funds to Bancorp "resulted directly from InComm's contractual liability to fund the cardholder account to cover the amount of each redemption, not from the [wrongful chit redemptions]."[187] In other words, Great American claimed that the redemption of the chits did not reduce the available assets in InComm's hands; rather, "it triggered only InComm's contractual obligation to its business partners to fund the redemptions."[188]

Because InComm's loss did not result from "the use of any computer" and, even if it did, the loss did not result "directly" from the computer use, Great American was entitled to summary judgment on InComm's breach of contract and declaratory judgment counts. Further, because InComm did not establish any loss covered by the policy, it was not entitled to statutory penalties or attorney's fees.[189]

ii. Third-Party Liability Cyber Policies

As the risk of data breaches and cyber liability has increased, insurers have responded by issuing stand-alone cyber liability policies or adding cyber liability endorsements to their CGL or professional liability policies. Typically, cyber liability policies provide coverage to insureds for damages and liability resulting from a data breach, so a cyber liability policy could well have provided coverage to the insureds in *Innovak* and *Rosen Millennium*. Unlike CGL policies, though, some cyber liability policies do not provide coverage for the insured's own acts that violate someone's privacy.

In *Doctors Direct Insurance Inc. v. Bochenek*,[190] the insured was a cosmetic surgeon covered under a cyber liability endorsement added to his professional liability coverage. The insured was sued by someone who had received unsolicited text messages advertising the insured's cosmetic surgery services. The complaint alleged that these communications violated the Telephone Consumer Protection Act (TCPA or Act)[191] and section 2 of the Consumer Fraud and Deceptive Business Practices Act (Consumer Fraud Act).[192] The insurer's policy provided coverage for a "Cyber Claim", any "Network Security Wrongful Act" or "Privacy Wrongful Act." The term "Privacy Wrongful Act" was defined as "any breach or violation of . . . statutes or regulations associated with the control and use of personally identifiable financial, credit or medical information, whether actual or alleged, but only if committed or allegedly committed by protected parties."[193]

The insured in *Doctors Direct* maintained that the TCPA claim and consumer fraud claim both fell within the definition of a Privacy Wrongful Act because the conduct complained of involved the use and control of personally identifiable financial, credit and medical information.[194] The court disagreed. First, the court concluded that the plain language of the definition of Privacy Wrongful Act meant that the statute allegedly violated must "be associated with the control and use of personally identifiable financial, credit, or medical information."[195] The court interpreted the word "associate" to mean "'to join or connect in any of various intangible or unspecified ways' . . . and 'to combine or join with another or others as component parts: UNITE.'"[196] The court ruled:

> The Telephone Consumer Protection Act is not joined, combined, united, or connected with the control and use of personally identifiable financial, credit, or medical information . . . .
>
> The plain language of the Telephone Consumer Protection Act illustrates that the statute only prohibits the actual making of certain kinds of calls. The statute does not address how a caller might control or use personally identifiable financial, credit or medical information either before or after the call is made . . . . [W]e note that Congress enacted the Telephone Consumer Protection Act to address telemarketing abuses related to the use of automated telephone calls . . . and that the purposes of this statute are to protect the privacy interests of residential telephone customers by restricting unsolicited automated telephone calls . . . .[197]

The court rejected the argument that the TCPA addressed the manner in which people are selected for marketing, finding that the Act and its supporting regulations were focused on the act of making calls and not connected to the use of personally identifiable financial, credit or medical information in service of the calls.[198]

The court similarly rejected the argument that the Consumer Fraud Act[199] was associated with personally identifiable financial, credit or medical information. Despite the fact that the Consumer Fraud Act could be established by showing a violation of the Personal Information Protection Act,[200] the court concluded that the Consumer Fraud Act was not associated with personally identifiable financial, credit or medical information in this case, since none of the allegations of the underlying complaint alleged violations of the Personal Information Protection Act.[201]

The court also saw no merit in the argument that the amended complaint alleged that the list for the automated texts and calls came from a spa, which established that the claim involved personally identifiable financial, credit or medical information.[202] The court saw no reason to assume that information from a spa meant that it included personally identifiable medical information. Nor did it agree that the fact that the insured was a physician meant that the list compiled for sending the texts involved personally identifiable medical information.[203]

Another variation of cyber policy provides coverage for errors or omissions leading to damages due to cyber events. For example, in *Travelers Property Casualty Co. v. Federal Recovery Services, Inc.*,[204] the insured obtained a cyber policy which provided coverage for damages the insured must pay arising out of the insured's work or product, and caused by an "errors and omissions wrongful act."[205] The term "errors and omissions wrongful act" was defined as "any error, omission or negligent act."[206] The insured provided credit card and bank billing services to a fitness center, which was later sold in an asset purchase agreement. The new owner requested the insured to return the customer account information following the sale, but the insured allegedly refused.[207] As a result, the new owner sued the insured, bringing claims of tortious interference, promissory estoppel, conversion, breach of contract, and breach of the implied covenant of good faith and fair dealing.[208] The insured then tendered the action under its cyber policy.

The insured argued that the allegation that the insured "withheld" data from its computer systems was broad enough to encompass a possible error, omission or negligent act.[209] The court rejected this argument, explaining that the policy covered errors, omissions or negligent acts, but the underlying complaint alleged that the insured had knowingly withheld the data and refused to turn it over until the plaintiff met certain demands. As the court noted, instead "of alleging errors, omissions or negligence, Global alleges knowledge, willfulness, and malice."[210]

Another restriction on cyber coverage was illustrated in *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh, PA*,[211] where an insured sought coverage under its cyber policy for losses it incurred when fraudulent data was entered into its computers by authorized users. The insured was a health insurance company that provides Medicare managed care plans and other insurance products. Under the plans, health care providers submitted claims to the insured, many of which were "auto-adjudicated" through the insured's computer system.[212]

The insured had purchased insurance with a "Computer Systems Fraud" rider that provided coverage for loss resulting 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 . . . ."[213] The insured claimed that it suffered substantial financial losses from fraudulent claims made against it, most of which were submitted directly by healthcare providers directly into the insured's computer system.[214] The insured maintained that such losses were covered because they resulted from the fraudulent entry of data into its computer system that caused money to be paid out.[215] The insurer responded that the policy only provided coverage against computer hackers, *i.e.*, situations in which an unauthorized user accessed the system and caused money to be paid out.[216] Since the providers were authorized users, the policy did not provide coverage.

The court agreed with the insurer. The court found that the phrase, "loss resulting directly from fraudulent . . . entry of Electronic Data . . . into [the insured's] proprietary Computer System" limited coverage to situations in which data was input by an unauthorized user, and there was no coverage when the user was authorized to enter the data, even if that data was fraudulent.[217] The court relied partially on the headings of the policy, which were "Computer Systems" and "Computer Systems Fraud," which the court interpreted to indicate that the coverage was directed at "misuse or manipulation of the system itself rather than at situations where the fraud arose from the content of the claim, and the system was otherwise properly utilized, *e.g.*, a fraudulent claim submitted by an authorized user."[218]

Notably, the forms used for cyber coverage have not become as standard as the forms used for CGL coverage. Therefore, the language of the specific cyber policy or endorsement will be critical for determining the extent to which there is coverage.

IV. Conclusion

The rise of cyber-related and data breach risks poses challenges to both insureds and insurers. The types of losses caused by these risks can be ethereal and difficult to define. They often do not fall within the parties' traditional conception of insurable risks–the risk of a tangible loss of physical property or potential liability for physical property damage or a bodily injury. As a result, as cyber-related and data breach risks become more prevalent in modern economic life–which they surely will, a focus must be made to refine insurance products for these risks so that insurers can appropriately price the risk and insureds can ensure that they obtain the right coverage for these risks.

THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

(Endnotes)

[1] *Cmty. Bank of Trenton v. Schnuck Mkts. Inc.*, 887 F.3d 803 (7th Cir. 2018).

[2] *In re Target Corp. Customer Data Sec. Breach Litig.*, 64 F. Supp. 3d 1304 (D. Minn. 2014); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518 (N.D. Ill. 2011).

[3] *In re Yahoo! Customer Data Sec. Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318 (N.D. Cal. Aug. 30, 2017).

[4] *In re Equifax, Inc.*, 371 F. Supp. 3d 1150 (N.D. Ga. 2019).

[5] *In re Heartland Payment Sys., Customer Data Sec. Breach Litig.*, 834 F. Supp. 2d 566 (S.D. Tex. 2011).

[6] *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 996 F. Supp. 2d 942 (S.D. Cal. 2014).

[7] *See supra* at nn. 1-6.

[8] *See, e.g.*, *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 522 (plaintiffs were consumers of a specialty arts and craft retailer who alleged that their financial data was compromised by the retailer's credit card PIN pads).

[9] *In re Equifax*, 371 F. Supp. 3d at 1157 (plaintiffs included financial institutions who had issued credit cards which were compromised in the breach).

[10] *See supra* at nn. 1-6 for cases discussing the various substantive claims pursued by plaintiffs in cyber-related litigation.

[11] 830 F. Supp. 2d 518.

[12] *In re Michaels Stores Pin Pad Litig*., 830 F. Supp. 2d at 521. PIN pads process a retailers' customers' debit and credit card payments and usually require the customer to swipe his or her card through the PIN pad and, if necessary, input a personal identification number. *Id*. Hackers can use modified PIN pads to capture credit or debit information from cards using modified pads. This inappropriately obtained credit or debit information is then used for illicit purposes, such as the creation of fraudulent duplicate credit or debit cards. *Id*. at 521-22.

[13] *Id.*

[14] *Id.* at 522.

[15] *Id.*

[16] *Id.*

[17] 18 U.S.C. § 2702(a)(1), (2).

[18] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 523-25.

[19] *Id.* at 528.

[20] *Id.*

[21] *Id.* "The rationale underlying this doctrine is that tort law affords the proper remedy for loss arising from personal injury or damages to one's property, whereas contract law and the Uniform Commercial Code provide the appropriate remedy for economic loss stemming from diminished commercial expectations without related injury to person or property." *Id.*

[22] Traditionally, Illinois only recognizes three exceptions to this doctrine: "(1) where plaintiff sustains personal injury or property damage resulting from a sudden or dangerous occurrence; (2) where plaintiff's damages were proximately caused by defendant's intentional, false representation; and (3) where plaintiff's damages were proximately caused by the negligent misrepresentation of a defendant in the business of supplying information for the guidance of others in business transactions." *Id*. at 528. The plaintiff did not contend that any of these traditional exceptions applied in this case.

[23] *Id*. at 530.

[24] *Id*. In another case involving a data breach, the Seventh Circuit affirmed the dismissal of negligence claims against the defendant under the economic loss rule. *Cmty. Bank of Trenton*, 887 F.3d at 812-17. In that case, the Seventh Circuit also questioned whether Illinois would even recognize a common law duty to safeguard personal information. *Id*. at 816.

[25] *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d at 525.

[26] *Id*. at 526 (quoting *In Re TJX Cos. Retail Sec. Breach Litig.*, 564 F.3d 489, 496 (1st Cir. 2009)).

[27] *Id.* at 526.

[28] *Id*. at 526-27. The Illinois Personal Information Protection Act "requires data collectors who own personal information concerning an Illinois resident to notify the resident of a data breach 'in the most expedient time possible and without reasonable delay.'" *Id*. at 527 (quoting 815 ILCS 530/10).

[29] *Id*. at 531.

[30] *Id.*

[31] *Hollingsworth v. Perry*, 570 U.S. 693 (2013).

[32] *Attias v. CAREFIRST*, 365 F. Supp. 3d 1 (D.C. 2019).

[33] *See Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826 (7th Cir. 2018); *Lewert v. P.F. Chang's China Bistro, Inc.*, 963 F.3d 819 (7th Cir. 2016); *Remijas v. Neiman Marcus Grp., LLC*, 794 F.3d 688 (7th Cir. 2015).

[34] *Remijas*, 794 F.3d 688.

[35] *Id.* at 689.

[36] *Id.* at 692.

[37] *Id.*

[38] *Id.* at 689.

[39] *Id*. at 692.

[40] *Id.* at 692 (citing *Clapper v. Amnesty Int'l*, 568 U.S. 398 (2013)).

[41] *Id*. at 693.

[42] *Id.*

[43] *Id.*

[44] *Id.* at 694.

[45] *Id*.

[46] *Lewert*, 819 F.3d 963.

[47] *Id.* at 965.

[48] *Id.*

[49] *Id.*

[50] *Id.* at 967.

[51] *Id.*

[52] *Id.*

[53] *Id.* at 968.

[54] *See*, *e.g.*, *Ward Gen. Ins. Services v. Emp'rs Fire Ins. Co.*, 114 Cal. App. 4th 548 (2003) (holding that the loss of electronically stored data, without loss or damage to the storage media, was not a covered "physical loss", noting that the insured did not lose tangible material but stored information); *Liberty Corp. Capital Ltd. v. Sec. Safe Outlet, Inc.*, 937 F. Supp. 2d 891, 901 (E.D. Ky. 2013) (email addresses stolen from electronic databases did not constitute "tangible property" and were excluded by policy's exclusion of "electronic data"); *Carlon Co. v. Delaget, LLC*, No. 11-CV-477-JPS, 2012 WL 1854146 (W.D. Wis. May 21, 2012) (holding electronic funds were not tangible property).

[55] *See, e.g.*, *NMS Services, Inc. v. Hartford*, 62 F. App'x 511, 515 (4th Cir. 2003) (data erased by a hacker was "direct physical loss"); *American Guar. & Liab. Ins. Co. v. Ingram Micro., Inc.*, No. 99-185 TUC ACM, 2000 WL 726789 (D. Ariz. Apr. 18, 2000) (loss of data constitutes physical damage under first-party business interruption policy); *Southeast Mental Health Ctr., Inc. Pacific Ins. Co., Ltd.*, 439 F. Supp. 831 (W.D. Tenn. 2006) (first-party property policy covered loss of use of a computer as "property damage" after loss of stored programing information and configurations).

[56] *See, e.g.*, *Lambrecht & Assocs., Inc. v. State Farm Lloyds*, 119 S.W.3d 16, 23-24 (Tex. App. 2003).

[57] *Lambrecht & Assocs., Inc.,* 119 S.W.3d at 23-24.

[58] *See, e.g.*, *Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co.*, 691 F.3d 821 (6th Cir. 2012) (affirming district court's grant of summary judgment for the insured and upholding ruling that commercial crime policy, which included a computer and funds transfer fraud endorsement, covered third-party costs resulting from data breach and hacking attack); *State Bank of Bellingham v. BancInsure, Inc.*, 823 F.3d 456, 461 (8th Cir. 2016) (finding coverage under insured's financial institution bond for fraudulent transfer caused by computer virus, reasoning that "the computer systems fraud was the efficient and proximate cause of [the] loss," regardless of whether other non-covered causes contributed); *Ad Advertising Design, Inc. v. Sentinel Ins. Co.*, 344 F. Supp. 3d 1175 (D. Mont. 2018) (emails impersonating CEO that directed employee to wire funds to fraudulent account covered under theft of "money" and forgery provisions, but not under computer fraud provision that required "physical loss"); *Medidata Solutions, Inc. v. Fed. Ins. Co.*, 729 F. App'x 117 (2d Cir. 2018) (*en banc* review denied) (Aug. 23, 2018) (holding that a policyholder was entitled to coverage after an employee wired funds to a criminal's account after receiving a spoofing email from the criminal that appeared to be from a company executive requesting payment finding that the spoofing email from the criminal remained the proximate cause of the loss notwithstanding the fact that a deceived employee initiated the wire transfer); *American Tooling Ctr., Inc. v. Travelers Cas. and Sur. Co. of Am.*, 895 F.3d 455 (6th Cir. 2018) (holding that the policyholder was entitled to coverage after an employee wired funds to a criminal's account after receiving an email from the criminal that appeared to be from a known vendor that provided new banking details for anticipated payments to the vendor finding that if the insurer had wished to limit coverage to situations in which a hacker gains controls over the policyholder's computer system

to steal money from the policyholder, it should have done so expressly); *Principle Sols Group, LLC v. Ironshore Indem., Inc.*, 944 F.3d 886 (11th Cir. 2019) (finding phishing email qualified as a loss covered by a crime policy insuring against fraudulent instructions).

[59] *See Metal Pro Roofing, LLC v. Cincinnati Ins. Co.*, 130 N.E.3d 653 (Ind. Ct. App. 2019).

[60] *See, e.g.*, *InComm Holdings, Inc. v. Great Am. Ins. Co.*, No. 1:15-cv-2671-WSD, 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017), *aff'd* 731 F. App'x 929 (11th Cir. 2018) (finding no coverage for debit card processor's losses under crime protection policy where loss did not result "directly" from computer fraud, since fraudsters used telephone lines to redeem debit cards); *Apache Corp. v. Great Am. Ins. Co.*, 662 F. App'x 252 (5th Cir. 2016) (finding no coverage under the "Computer Fraud" provision of crime protection policy because email sent in the chain of events was "merely incidental to the occurrence of the authorized transfer of money," and the provision did not cover "any fraudulent scheme in which an email communication was part of the process"). *See also Taylor & Lieberman v. Fed. Ins. Co.*, 681 F. App'x 627 (9th Cir. 2017) (finding no coverage because, among other things, the fraudulent wire transfers were not made using a "Financial Instrument" as required by the forgery provisions of the policy).

[61] *See, e.g. Pasco Daewoo Am. Corp. v. Allnex USA, Inc.*, No. 17-483, 2017 WL 4922014 (D.N.J. Oct. 31, 2017) (holding no coverage under a wrap and crime insurance policy because the insured did not own the money transferred to the fraudster (but instead only owned a "receivable"), purportedly in payment of outstanding receivables, and therefore the money transferred did not fall within "Ownership of Property" provision of the policy); *Childrens Place v. Great Am. Ins. Co.*, No. 18-11963 (ES) (JAD), 2019 WL 1857118 (D.N.J. Apr. 25, 2019) (denying insurer's motion to dismiss a claim brought under a "computer fraud" provision in crime protection policy, but granting dismissal without prejudice of claims based on forgery and fraudulently induced transfer provisions); *Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am.*, 719 F. App'x 701 (9th Cir. 2018) (coverage barred by exclusion for "loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System" because the insured's employees and not the fraudster changed bank routing instructions to the account requested by the fraudster).

[62] *See, e.g.*, ISO Form CG 00 01 04 13 at Section I(1).

[63] *See id.* at Section I, Coverage A.

[64] *See id*. at Section V(17).

[65] *See generally* CG 00 01 11 85.

[66] *Compare America Online, Inc. v. St. Paul Mercury Ins. Co*., 347 F.3d 89 (4th Cir. 2003) (webpages, data, and computer software not "tangible property") *with Computer Corner, Inc. v. Fireman's Fund Ins. Co*., 46 P.2d 1264 (N.M. App. Ct. 2002) (computer data stored on hard drive constitutes "tangible property").

[67] *See* CG 00 01 10 01 at Section V(17).

[68] *See, e.g.*, *Eyeblaster, Inc. v. Fed. Ins. Co*., 613 F.3d 797 (8th Cir. 2010) (coverage for physical injury to computer hardware such as freeze-up (loss of use) caused by spyware).

[69] *See* CG 00 01 12 04 at Section I(2)(p).

[70] No. 4:16-CV-0204-JEO, 2016 WL 6217161, at *2 (N.D. Ala. Oct. 25, 2016).

[71] *See Camp's Grocery, Inc.*, 2016 WL6217161, at *1.

[72] *See id*. at *2-3.

[73] *Id*. at *5-6.

[74] *See id*. at *5.

[75] *Id*. at *7-8.

[76] *See id*. at *14-15.

[77] *See id*. at *16-17.

[78] *See id*. at *17-18.

[79] *See id*. at *18.

[80] *Id*. at *20.

[81] *See id*. at *21-22.

[82] *Id.*, Section V, definition 14.

[83] 280 F. Supp. 3d 1340 (M. D. Fla. 2017) (applying South Carolina law).

[84] *Innovak Int'l, Inc*., 280 F. Supp. 3d at 1342.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.* at 1343.

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.* at 1344.

[93] *Id.*

[94] *Id.* at 1347.

[95] *Id.*

[96] *Id.*

[97] No. 651982/2011, 2014 WL 8382554 (N.Y. Sup. Ct. Feb. 21, 2014).

[98] *Innovak*, 280 F. Supp. 3d at 1348 (quoting *Zurich Am. Ins.*, 2014 WL 8382554).

[99] *Id.*

[100] 337 F. Supp. 3d 1176 (M.D. Fla. 2018).

[101] *St. Paul Fire & Marine Ins. Co*., 337 F. Supp. 3d at 1182-83.

[102] *Id.* at 1185-86.

[103] 691 F.3d 821 (6th Cir. 2012).

[104] *Retail Ventures, Inc*., 691 F.3d at 824.

[105] *Id.*

[106] *Id.* at 825.

[107] *Id.* at 826.

[108] *Id.* at 826-27.

[109] *Id.* at 827.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.* at 828.

[114] *Id.*

[115] *Id.* at 831-32.

[116] *Id.* at 831. *See, e.g.*, *Amstutz Hatcheries of Celina, Inc. v. Grain Dealers Mut. Ins. Co.*, No. 4-77-4, 1978 WL 215799, at *1-2 (Ohio App. Mar. 15, 1978) (finding coverage against loss of chickens "directly and immediately resulting from" lightning included suffocation when lightning knocked out power to ventilation system).

[117] *Retail Ventures, Inc*., 691 F.3d at 831.

[118] *Id.*

[119] *Id.* at 832.

[120] *Id.* at 833.

[121] *Id.*

[122] *Id.* at 834.

[123] *Id.*

[124] 823 F.3d 456 (8th Cir. 2016).

[125] Although this case technically dealt with a financial institution bond, financial institution bonds are treated like first party insurance policies from an interpretation perspective. *See State Bank of Bellingham*, 823 F.3d at 460.

[126] *Id.* at 457.

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *Id.* at 457-58.

[134] *Id.* at 458.

[135] *Id.*

[136] *Id.* at 459.

[137] *Id.*

[138] *Id.*

[139] *Id.*

[140] *Id.* at 461.

[141] *Id.*

[142] *Id.*

[143] 662 F. App'x. 252 (5th Cir. 2016).

[144] *Apache Corp.*, 662 F. App'x at 253.

[145] *Id.*

[146] *Id.* at 258.

[147] *Id.* at 253-54.

[148] *Id.* at 254.

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.* at 255.

[154] *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, 656 F. App'x 332, 333 (9th Cir. 2016) (*Pestmaster II*), No. 14-56294, 656 F. App'x. 332, 333 (9th Cir. 2016), *aff'g Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.* (*Pestmaster I*), No. CV 13-5039-JFW, 2014 WL 3844627 (C.D. Cal. 17 July 2014).

[155] *Apache Corp.*, 662 F. App'x at 253 (citing *Pestmaster II*, 656 F. App'x at 333).

[156] *Id.* at 256 (citing *Pestmaster II*, 656 F. App'x at 333).

[157] *Id.* at 256-57 (citing *Pestmaster II*, 656 F. App'x at 333).

[158] No. 11-6187, 2012 WL 1067694, at *4 (D. N.J. Mar. 29, 2012).

[159] *Apache Corp.*, 662 F. App'x at 257.

[160] *Id.* at 258.

[161] No. 1:15-CV-2671-WSD, 2017 WL 1021749 (N.D. Ga. 2017), *aff'd sub nom. Interactive Commc'ns Int'l, Inc. v. Great Am. Ins. Co.*, 731 F. App'x 929 (11th Cir. 2018).

[162] *InComm Holdings, Inc.*, 2017 WL 1021749, at *1.

[163] *Id.*

[164] See *id.* at *7.

[165] *Id.* at *2.

[166] *Id.* at *7.

[167] *Id.* at *2.

[168] *Id.*

[169] *Id.* (citations omitted).

[170] *Id.*

[171] *Id.* at *3.

[172] *Id.* at *4.

[173] *Id.*

[174] *Id.* at *7.

[175] *Id.*

[176] *Id.*

[177] *Id.* at *8.

[178] *Id.*

[179] *Id.*

[180] *Id.* at *9.

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.* at *10.

[187] *Id.*

[188] *Id.* at *11 (citing *Apache Corp.*, 662 F. App'x. at 258, where the court warned that "to find coverage based on the use of a computer, without a specific and immediate connection to a transfer, would effectively convert a computer fraud provision into a general fraud provision.").

[189] *Id.*

[190] 2015 IL App (1st) 142919.

[191] 47 U.S.C. § 227.

[192] 815 ILCS 505/2.

[193] *Doctors Direct Ins., Inc*., 2015 IL App (1st) 142919, ¶ 6.

[194] *Id.* ¶ 12.

[195] *Id.* ¶ 26.

[196] *Id.* ¶ 27.

[197] *Id.* ¶ 28 (internal quotations omitted).

[198] *Id.* ¶ 30.

[199] 815 ILCS 505.

[200] 815 ILCS 530/1 *et seq.*

[201] *Doctors Direct Ins. Inc.*, 2015 IL App (1st) 142919, ¶ 30.

[202] *Id.* ¶ 43.

[203] *Id.*

[204] 103 F. Supp. 3d 1297 (D. Utah 2015).

[205] *Travelers Prop. Cas. Co. of Am*., 103 F. Supp. 3d at 1298.

[206] *Id.*

[207] *Id.* at 1299-1300.

[208] *Id.* at 1300.

[209] *Id.* at 1302.

[210] *Id.* (footnotes omitted).

[211] 38 Misc.3d 859, 959 N.Y.S.2d 849 (N.Y. Sup. 2013).

[212] *Id.*, 38 Misc.3d at 860.

[213] *Id.*

[214] *Id.* at 861.

[215] *Id.* at 862.

[216] *Id.*

[217] *Id.* at 864.

[218] *Id.*

About the Authors

Patrick D. Cloud is an attorney in *Heyl, Royster, Voelker & Allen's* Edwardsville office. Mr. Cloud is the Chair of Heyl Royster's Insurance Services Practice Group and concentrates his practice on insurance coverage litigation, toxic tort matters, complex civil litigation, and products liability defense. He is a graduate of the Washington University School of Law and the University of Notre Dame.

William K. McVisk is a partner at *Tressler LLP* in Chicago where he focuses his practice on complex insurance coverage litigation, and hospital law and medical liability. He has handled all areas of coverage and bad faith litigation, especially third-party bad faith and coverage litigation involving commercial general liability, professional liability coverages, as well as personal lines coverages such as auto and homeowners' coverages. Mr. McVisk is the 2019-2020 President of the Illinois Defense Counsel, the former chair of the IDC Insurance Law Committee, and a member of the DRI Insurance Law Committee. He has tried declaratory judgment actions in several jurisdictions and has briefed and argued appeals concerning coverage matters in several courts. He is a member of the bars in Illinois and Indiana and is admitted to practice before several federal district and appellate courts. He graduated with honors from Northwestern University Law School in 1977.

Seth D. Lamden is a litigation partner at *Neal, Gerber & Eisenberg LLP* in Chicago. He concentrates his practice on representing corporate and individual policyholders in coverage disputes with their insurers. In addition to dispute resolution, Mr. Lamden counsels clients on matters relating to insurance and risk management, including maximizing insurance recovery for lawsuits and property damage, policy audits and procurement, and drafting contractual insurance specifications and indemnity agreements. He obtained his B.A. from Brandeis University and his J.D., *magna cum laude*, from The John Marshall Law School.

Georgia L. Joyce is an attorney with *Bodell Bove LLC* in Chicago where she concentrates her practice in insurance coverage litigation. Her work includes the preparation of coverage opinions and the handling of all phases of litigation of coverage suits in state and federal courts. She represents insurance carriers in a broad range of coverage matters involving commercial general liability policies and their application to personal injury and property damage lawsuits, as well as to claims involving environmental contamination. Ms. Joyce is a graduate of Chicago-Kent College of Law (J.D.), De Paul University (M.B.A. Finance), and University of Illinois at Urbana-Champaign (B.S. Finance).

Jamie L. Hull focuses her practice on complex, high exposure insurance coverage and commercial litigation matters, including broker/agent professional liability, business litigation and appellate. She represents insurance companies, corporations and individuals in a wide range of insurance and business matters in multiple jurisdictions. Ms. Hull has extensive experience working with risk retention groups, self-insured retentions and insurance policies including commercial general liability, professional liability, D&O liability, employer's liability, builder's risk, cyber liability, excess/umbrella liability and disability. In addition, she serves as outside general counsel for a variety of companies. She

counsels on all business-related matters, coordinates and manages all commercial litigation, dispute and transactional work, national, regional, and state distribution agreements, contracts with industry suppliers, employment, operating, services, licensing agreements, and other commercial agreements.

C. William Busse, Jr. is the President of the law firm of *Busse, Busse, P.C.* He has more than 33 years of legal experience handling civil jury trials and appeals. Mr. Busse has concentrated his practice in the defense of tort and insurance coverage litigation. He has handled hundreds of personal injury and wrongful death cases in various Illinois venues, including automobile, trucking, premises liability, product liability, aviation and construction injury claims, as well as fire and explosion and property damage claims. Mr. Busse served on the Board of Directors of the Illinois Defense Counsel from 2002 to 2014 and returned in 2018 to serve again and is a co-author of, *The 50 Year History of the IDC*.

Henry W. Goldman of *Busse & Busse, P.C.* in Chicago concentrates his practice primarily in civil litigation with an emphasis on insurance defense, breach of contract, and workers' compensation claims. Mr. Goldman is a seasoned litigator and has extensive courtroom experience having tried twelve jury trials. Outside the Courtroom, Mr. Goldman has prosecuted matters in alternative dispute resolution forums that include arbitration and mediation. In 2012, Mr. Goldman earned his J. D. from Western Michigan University Thomas M. Cooley Law School where he was repeatedly on the Dean's List and served as President of the Tax Law Society. In 2006, Mr. Goldman earned a B. A. in Political Science from Framingham State University. Mr. Goldman is admitted to practice before the Supreme Court of Illinois and the United States District Court for the Northern District of Illinois.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at www.idc.law or contact us at PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, idc@iadtc.org.