GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions in 2022

Vincent J. Vitkowsky

Connecticut Massachusetts New York New Jersey Pennsylvania

TABLE OF CONTENTS

GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions in 2022

Introduction

We are pleased to present this Compendium of decisions rendered by U.S. courts in 2022 on the law of insurance coverage for cyber risks.

In 2022, for the first time, there were several decisions construing standard provisions in affirmative cyber coverages. Perhaps not surprisingly, the courts misconstrued some key provisions – or at least interpreted them far outside the industry understanding. ***Fishbowl Sol., Inc v. Hanover Ins. Co.*** (*see* p. 3) applied data breach and business impairment provisions to a business e-mail compromise. ***New England Sys. Inc. v. Citizens Ins. Co. of Am.*** (*see* p. 5) suggested the possibility that business interruption may include lost opportunities because of the diversion of business resources when correcting the effects of a virus transmitted to clients. And ***Yoshida Foods Int'l, LLC v. Fed. Ins. Co.*** (*see* p.6) found coverage for a ransomware attack under the Computer Fraud Coverage provisions of a Crime Coverage Part. Similar misinterpretations are inevitable. This suggests Insurers need to tighten and refine their language, especially in the areas identified in these three cases.

Other 2022 cases addressed claims under various lines of business for the costs of issuing replacement payment cards, the interaction between indemnification and self-insured retentions, the costs of migrating data, cryptocurrency, and the ongoing stream of business e-mail compromises and social engineering losses.

On related privacy issues, there were important decisions on coverage for claims concerning the Illinois Biometric Privacy Act, the Telephone Consumer Protection Act, and the Driver's Privacy Protection Act.

Many more decisions from recent years are addressed in our earlier Compendia entitled, respectively, ***Cyber Risks and Insurance Coverage Decisions in 2021, Cyber Risks and Insurance Coverage Decisions 2020*** and ***Cyber Risks and Insurance Coverage Decisions 2015-2019***. Those addressed decisions involving a broad range of risks, including ransomware, cyber extortion, network interruption, data breaches, lost data, lost

software, disabled hardware, cryptomining losses, liability from websites and social media, deceptive funds transfers, social engineering, and cryptocurrency theft. Like the decisions in this Compendium, the earlier decisions arose under various types of policies, including CGL, Businessowners, Computer Fraud, Crime, Financial Institution, Cyber, D&O, and Homeowners. Thus, the prior Compendia present a survey of the most important recent decisions involving "silent cyber" or "non-affirmative cyber" coverage. If you would like to receive copies of these earlier Compendia, please contact me at the email address below.

The body of relevant law continues to emerge, and many novel, complex and challenging issues lie ahead.

Vince Vitkowsky
New York, NY
January 9, 2023

vvitkowsky@gllawgroup.com
www.gllawgroup.com

Cyber Risks and Insurance Coverage Decisions in 2022

Vincent J. Vitkowsky
Gfeller Laurie LLP

State-Sponsored Cyber Attacks

New Jersey State Court Holds that State-Sponsored Cyber Attacks Did Not Fall Within the Hostile/Warlike Acts Exclusion in All-Risk Property Policies

Merck & Co., Inc. v. Ace Am. Ins. Co., No. UNN-L-002682-18, 2022 WL 951154 (N.J. Super. L. Jan. 13, 2022) In a 2017 cyber attack known as NotPetya, Russia sent malware to several dozen Ukrainian companies. It was disguised as ransomware, similar at first view to an earlier ransomware attack called Petya. But the new strain was really "wiperware." That is, it automatically encrypted the victim's data, permanently and inalterably. Essentially, it obliterated the data in the victim's systems. It was designed to spread to other networks automatically, rapidly, and indiscriminately, and it spread throughout the world. It was *so* indiscriminate that it infected the network of the Russian state oil company, Rosneft. It is estimated that NotPetya caused approximately $10 billion in losses, including more than $1 billion in losses to three separate organizations in the United States.

The pharmaceutical giant Merck suffered a widespread systemic failure caused by NotPetya. Operations were halted for two weeks, and Merck asserts it suffered more than $1.4 billion in damages. It had nearly three dozen insurers on all-risk property policies providing coverage for loss or damage resulting from the destruction or corruption of computer data and software. The insurers rejected Merck's claims based on the standard Hostile/Warlike Action Exclusion found in many traditional policies, which excludes the following:

1) Loss or damage caused by hostile or warlike action in time of peace or war, including action in hindering, combatting, or defending against an actual, impending, or expected attack:
    a) by any government or sovereign power (de jure or de facto) or by any authority maintaining or using military, naval or air forces;
    b) or by military, naval, or air forces;
    c) or by an agent of such government, power, authority or forces.

    This policy does not insure against loss or damage caused by or resulting from [the perils in the Exclusion above] regardless of any other cause or event contributing concurrently or in any other sequence to the loss.

On January 13, 2022, the lowest-level state court in New Jersey rendered its decision. It said it was interpreting the words of the Hostile/Warlike Actions Exclusion by their "ordinary meaning." It said that the term "warlike" could only be interpreted as "like war." This is consistent with the definition in the Oxford English Dictionary, which also defines "hostile" as "of, pertaining to, or characteristic of an enemy, pertaining to or engaged in actual hostilities." Merck argued this meant that the Exclusion only applied when armed forces engaged in traditional warfare. The Court agreed. It cited to a few old cases, and said that "no court has applied a war (or hostile acts) exclusion to anything remotely close to the facts herein." Based on this logic, it held "Merck had every right to anticipate that the exclusion only applied to traditional forms of warfare." Thus, it held the Exclusion did not apply.

Other Key Developments Concerning State-Sponsored Cyber Attacks

For many years, insurers, especially cyber insurers, have been concerned about the aggregation risk of state-sponsored cyber attacks. The losses from the NotPetya attack discussed in the previous case put a fine point on it. But even before then, the risk of possible widespread correlated losses, across business sectors or nations, posed an unacceptable accumulation risk.

In late 2021, the Lloyd's Market Association released four "War, Cyber War and Cyber Operation Exclusions" that would address some of the concerns. And then on August 16, 2022, Lloyd's issued Market Bulletin Y5381 entitled "State backed cyber-attack exclusions." It mandates that as of March 31, 2023, all standalone "cyber-attack policies" issued at Lloyd's, unless Lloyd's permits a deviation, must include a suitable clause excluding liability for losses arising from any state backed cyber-attack. The clause must:

- exclude losses arising from a war (whether declared or not), unless the policy has a separate war exclusion;
- exclude losses arising from state-backed cyber attacks that (a) significantly impair the ability of a state to function or (b) that significantly impair the security capabilities of a state (subject to the next requirement);
- be clear as to whether cover excludes computer systems that are located outside any state affected in that way;
- set out a robust basis by which the parties agree on how any state backed cyber-attack will be attributed to one or more states; and
- ensure all key terms are clearly defined.

The Bulletin requires that these exclusions be reviewed by counsel. It also states that Lloyd's is satisfied that any of the LMA Exclusions released in 2021 would meet the requirements of the Bulletin.

Thus, it seems highly likely there will be changes in London market forms. It is not clear what the what the United States response will be. It remains to be seen what the major Insurers will do and what new language, if any, becomes widely accepted.

Data Breaches

Minnesota Federal Court Holds Costs of Issuing Replacement Payment Cards Are Covered by General Liability Policies

Target Corp. v. ACE Am. Ins. Co., No. 19-CV-2916 (WMW/DTS), 2022 WL 848095 (D. Minn. Mar. 22, 2022), *motion to certify appeal denied*, No. 19-CV-2916 (WMW/DTS), 2022 WL 4592094 (D. Minn. Sept. 30, 2022) held that the costs of reissuing payment cards cancelled after a data breach were covered by general liability policies. The Court reversed itself by granting a motion to alter or amend its earlier judgment on this point.

The Court first found that the cancellation and inoperability of the payment cards was an "occurrence." The Policies defined "Occurrence" an "accident . . .." They did not define "accident." Minnesota law defines an accident as "a happening that is unexpected and unintended." An accident "encompasses both the acts of the insured and the consequences of the insured's act." The Court found that the "cancellation and resulting inoperability of the payment cards were the consequences of Target's discovery of the accident, the Data Breach." The Court found that because this constituted an "accident," it was also an "occurrence."

The Policies define property damage to include "loss of use" of "tangible property that is not physically injured." The Court found that there was a "loss of use," and the replacement costs were incurred due to the loss of use the payment cards.

Using this reasoning, the Court concluded that the cost of replacing the payment cards was covered, and ACE was obligated to indemnify Target for Target's settlement with the Banks that issued the payment cards for the costs of their replacement.

Minnesota Federal Court Extends Data Breach and Business "Impairment" Coverage to a Business E-Mail Compromise

Fishbowl Sols., Inc. v. Hanover Ins. Co., No. 21-CV-00794 (SRNDJF), 2022 WL 16699749 (D. Minn. Nov. 3, 2022) was a highly unusual decision. It applied the Data Breach Coverage Form of a Technology Professional Liability Policy issued to a technical consulting and software development company to provide coverage for a Business E-Mail Compromise.

An unknown bad actor gained unauthorized access to the email account of a staff accountant, created multiple "rules" within the account that interfered with the proper receipt of incoming emails, and allowed the bad actor to impersonate the staff accountant. This resulted in two misdirected payments and the loss of $148,000. The decision does not quote the applicable definition of "data breach" and the parties did not dispute that the insured suffered a data breach within the meaning of the Policy. Thus, the Court proceeded to analyze the case within the framework of a Business Interruption claim. It construed the key policy terms in favor of coverage. These include "business operations,"

which were defined as "usual and regular business activities," which the Court construed to include communications with, and invoicing of, clients. The insured's property claims director, in a deposition, admitted that the insured sustained an "actual loss of business income." Having found a loss of business income, the Court found that it was outside the 24-hour "Period of Restoration," because the breach occurred in November and the erroneous payments were made in December. It also found that the loss "directly" resulted from the data breach.

The insurer argued and the Court addressed the position that "a finding of coverage here contradicts the overall purpose of the . . . Policy and of business interruption insurance." The Court found that the Policy's use of the term "impairment" of business operations, rather than "interruption," was significant, under the theory that it demonstrates the Policy "specifically grants coverage when a business suffers something less than a total suspension of operations."

Under the analysis above, the Court found coverage for the loss.

[**Note**: This case is so unusual that it warrants analytical commentary. First, the term "impairment" appears in many cyber policies, with no radical differences in interpretation intended. Yet the result here was clearly an unintended result of liberal and incomplete policy wording. The Policy neither addressed nor excluded coverage for cybercrime, social engineering, or other business email compromises. It did not define "business income" and "business operations" narrowly to address the lack of coverage for financial fraud or invoice manipulation. So, the largest lesson from the decision is the danger of casually adding a non-comprehensive cyber endorsement to a policy in some other line of business.]

Washington Appellate Court Holds that Indemnification from Vendor Responsible for the Data Breach Does Not Reduce the Loss Incurred by the Insured under the Self-Insured Retention

***T-Mobile USA, Inc. v. Steadfast Ins. Co.*, No. 82704-9-I,** 2022 WL 17246715 (Wash. Ct. App. Nov. 28, 2022) presented an unusual set of facts. T-Mobile suffered a data breach. Steadfast issued cyber coverage for $15 million, over a $10 million Self-Insured Retention (SIR). T-Mobile incurred $17.3 million in loss, which it paid. The Breach was caused by a breach of one of its vendors, Experian. T-Mobile recovered $10.75 million from Experian as indemnification. This brought the total amount of the loss paid by T-Mobile to an amount within the SIR. Steadfast refused to provide coverage on the grounds that the SIR had not been satisfied. The Court disagreed, holding that coverage existed, because "T-Mobile incurred $17.3 million in loss as defined by the policy, a loss exceeding the SIR obligation."

The policy defined "loss" as "the total amount which the Insureds become legally obligated to pay on account of each Claim and for all Claims in each Policy Period," and then enumerated various categories. All amounts incurred by T-Mobile fell within the

categories in the definition of "loss." The Court said that "because those are all costs T-Mobile had to pay on account of the data breach, they are a covered loss under the policy."

Steadfast argued that the indemnification from Experian fell within the exclusion from its definition of "loss" for "any amount for which the Insureds are absolved from payment." The Court held that the Experian recovery did not fall within the dictionary definition of "absolve" because it did not release T-Mobile from its obligation to pay the costs and expenses incurred from the data breach. The Court characterized Steadfast's position as an attempt to obtain a "setoff" for the Experian payment, and found nothing in the policy authorizing such a setoff.

On this reasoning, the court granted partial summary judgment for T-Mobile, holding that coverage existed under the Steadfast policy, and remanding to the trial court for further proceedings.

Business Interruption

Federal Court in Connecticut Finds that Diversion of Resources from Usual Operations May Constitute Business Interruption, Denying Summary Judgment

New England Sys., Inc. v. Citizens Ins. Co. of Am., No. 3:20-CV-01743 (SVN), 2022 WL 17585966 (D. Conn. Dec. 12, 2022) is a claim for business interruption losses following a data breach. The insurer moved unsuccessfully to have the claim dismissed on summary judgment. The insured is itself a managed service provider of partially or fully outsourced information technology ("IT") support, IT strategy, consulting, and cybersecurity services. A data breach impacted the insured and several of its clients. The insurance policy included a Data Breach Coverage Form, providing coverage for Cyber Business Interruption and Extra Expense which covered "actual loss of 'business income' . . . directly resulting from a 'data breach' . . . which results in an actual impairment or denial of service of business operations . . .." The insured's own systems were not impacted by the breach, except for one server used by the accounting department, which was quickly restored.

However, as a result of the data breach, the bad actor or actors were able to access some of the insured's client's systems and send a virus and malware that encrypted the clients' data. The Insured then undertook remedy the clients' issues. It asserts it was unable to perform work for six of its clients following the data breach, and suffered losses including lost monthly service agreements, cancelled or lost projects, or lost subscriptions. Its theory of coverage was that it was forced to divert resources from its normal business operations, and thereby suffered losses. According to the Court, "the operative question is whether the data breach result[ed] in an actual impairment . . . of business operations." Specifically, it said that the need for the insured "to expend significant efforts to remediate the impacts of a covered data breach on its clients – and, in doing so, take time away from other client services – presents an 'actual impairment' of . . . regular and usual

business activities." The Court said it could not conclude that the term "actual impairment" categorically excludes the losses suffered from remediation. It cited two other cases, *Fishbowl Sols., Inc. v. Hanover Ins. Co.*, No. 21-cv-00794, 2022 WL 16699749 (D. Minn. Nov. 3, 2022) (discussed *supra*) and *P.F. Chang's China Bistro, Inc. v. Fed. Ins. Co.*, No.CV-15-01322, 2016 WL 3055111 (D. Ariz. May 31, 2016), which had interpreted the term "impairment" broadly, beyond the meaning insurers typically ascribe to it or business interruption claims. The Court also emphasized that "nothing in the Policy expressly limits the definition of 'impairment' to the remediation of impacts on Plaintiff's *own* systems." (emphasis added).

The Court went on to address the specific activities undertaken or forgone, the terminations of client relations, and the Insured's profits and losses (under various measures) in the period. It found there was sufficient evidence to create genuine issues of material fact and defeat summary judgment. The Court also found the Insured had provided sufficient evidence to calculate damages.

The Court did, however, grant summary judgment dismissing the claim of breach of the Implied Covenant of Good Faith and Fair Dealing. It found that no evidence had been presented showing the Insurer acted with a dishonest purpose, and applied the well-settled rule in Connecticut that a Plaintiff cannot recover for bad faith in the Insurer denies a claim that is fairly debatable.

Ransomware

Oregon Federal Court Finds Coverage for Ransomware Attack under the Computer Fraud Coverage of a Crime Coverage Part

Yoshida Foods Int'l, LLC v. Fed. Ins. Co., No. 3:21-CV-01455-HZ, 2022 WL 17480070 (D. Or. Dec. 6, 2022) found coverage for a ransomware attack under the Computer Fraud Coverage in the Crime Coverage Part of a broader policy. An anonymous hacker gained unauthorized entry into the insured's computer system, isolating and encrypting the entire network and its data, rendering the system unusable. The insured had to purchase four decryption keys with cryptocurrency valued at $107,074.20. The Insured's IT consultant was unable was unable to make the payments in cryptocurrency, so the payments were made from the personal cryptocurrency funds of the Insured's President. The Insured also paid its consultant $7,075.96 to diagnose the source of the attack, acquire the decryption keys, recover data, and restore the computer system. One year later, the Insured's manager officially approved the ransom payment by the President and authorized his reimbursement.

The Computer Fraud Coverage insured against loss from a Computer Violation, broadly defined as unauthorized entry into a computer system. The Insurer did not contest whether a ransomware attack fit into this term. Instead, the Coverage required that there be a "direct loss," and the Insurer argued that there was no loss because the President, not the Insured, made the ransom payment, and the reimbursement by the Insured was

an indirect or consequential loss. The Policy did not define "direct loss." Oregon courts have defined the term as requiring "a proximate, rather than remote relationship" between the covered act and the resulting loss or damage. The Court held that both the original payment and the reimbursement "were proximately caused by the hacker's violation directed against the [insured's] computer system." There was no intervening occurrence in the unbroken sequence of events between the attack and the reimbursement.

The Insurer then argued that because the Insured made a conscious decision to pay a cyber-criminal, the Payment was not a direct result of the Computer Violation. The Court rejected this, saying that a payment induced by fraud is, by definition, not volitional, but made under duress. It cited and quoted with approval the court in ***G&G Oil Co. Ind. v. Cont'l W. Ins. Co.***, 165 N.E.3d 82 (Ind. 2021) on this point.

The Insurer also relied on the Fraudulent Instructions Exclusion, which provides that there is no coverage for a transfer or payment of money "approved" by an "employee" of the Insured and made several attempts to apply it. The Court rejected them all. First, it rejected the argument that processing the reimbursement by a clerical employee was not an official "approval." It held the President's decision to personally pay the ransom could not have been made by an ordinary employee in the usual course of their duties, and that the President did not "approve" of the payment because it was made under duress.

The Insurer also objected to reimbursement of the IT provider's expenses, arguing they did not result from a "direct loss." The Court rejected that based on its earlier analysis. The Court also analyzed the requirement of prior written consent in the Computer Violation Expenses provision. The first sentence of the provision permitted reimbursement of expenses to reproduce or duplicate damaged or destroyed data or programs, only "with the company's prior written consent." The next sentence allowed for reimbursement of additional expenses if the programs cannot be duplicated, but did not expressly require written consent. The Court held that at a minimum, the Policy was ambiguous as to whether prior written consent was required for all expenses, and construed the ambiguity against the insurer.

However, the Court dismissed the claim for beach of the duty of good faith and fair dealing. It reasoned that Computer Fraud Coverage did not include the words "ransomware" or "encryption," and that the language in the Policy was not specifically tailored to a ransomware attack. Thus, whether coverage existed was subject to interpretation and disagreement. There was a reasonable basis for denying the claim.

Ohio Supreme Court Finds No Coverage for Ransomware Losses under a Businessowners Policy for Lack of Direct Physical Loss or Damage

EMOI Servs., L.L.C. v. Owners Ins. Co., No. 2021-1590, 2022 WL 17905839 (Ohio Dec. 27, 2022) found there was no coverage under a Businessowner's Policy for the payment of ransom and the costs associated with investigating and remediating an attack, as well as the upgrading of security systems. The insured was a computer software company

that provides services and support to medical offices. It suffered a ransomware attack that encrypted files needed for the insured's software and database systems. The insured paid Bitcoin worth approximately $35,000. The ransomware attack caused no hardware or equipment damage.

The Policy had two potentially applicable provisions. The Data Compromise endorsement expressly excluded coverage for "any threat, extortion, or blackmail," including but not limited to "ransom payments." The Electronic Equipment, Media endorsement provided the policy would pay for direct physical loss or damage to "media," and also pay for costs to research, replace or restore information on "media" which has "incurred direct physical loss or damage by a Covered Cause of Loss." "Media" was defined to include, among other things, "computer software . . . contained on covered media."

The Ohio Supreme Court reasoned that "software is an intangible item that cannot experience physical loss or direct physical damage," so the Electronic Equipment endorsement did not apply. It held that "covered media" means media that has a physical existence. It held that for computer software to be covered, there must be direct physical loss or physical damage of the covered media (*i.e.*, hardware) containing the computer software. It elaborated, saying that "software is essentially nothing more than a set of instructions that a computer follows to perform specific tasks," and "while a computer or other electronic medium has physical electronic components that are tangible in nature, the information stored there has no physical presence." Thus, the Supreme Court reversed an intermediate appellate court decision that the case was not suitable for summary judgment, and reinstated a trial court's grant of summary judgment in favor of the insurer.

Costs of Migrating Data

Ohio Federal Court Holds that Costs of Migrating Data Are Not Covered under a Property Policy because there is No Direct Physical Loss or Damage

Computer Programming Unlimited, Inc. v. Hartford Cas. Ins. Co., Case No. 3:21 CV 02350 (U.S.D.C., N.D. Oh., Oct. 26, 2022) (unpublished) involved a claim under a property policy for expenses incurred in migrating customer data from one cloud provider to another. The Court found no coverage.

The Insured provides information technology (SVN) services to small businesses, securing sufficient server space from third-party providers of cloud services. Its original provider, Nuvolat, filed for bankruptcy, and the insured migrated its customer data to other servers without any disruption in service. The insured then sought over $218,000 from its property insurer, allegedly relating to Nuvolat's default in providing services. Its position was that its claim was not about the servers, but instead about the "*loss of use* of the servers."

The Insurer's Special Property Coverage Form covers "direct physical loss of or damage to" property. It had a Computers and Media endorsement which covered "direct physical loss or damage to 'computer equipment' and the cost to research, replace or restore physically lost or physically damaged 'electronic data' and 'software.'"

The Court held that "because the servers suffered no 'tangible, material, physical alteration,' this loss of use theory is insufficient to demonstrate a 'direct physical loss or damage,'" and hence there was no coverage.

Cryptocurrency

California Court Holds Theft of Cryptocurrency Is Not Physical Loss under a Homeowners Policy

Burt v. Travelers Com. Ins. Co., No. 22-CV-03157-JSC, 2022 WL 3445941 (N.D. Cal. Aug. 16, 2022) involved the theft of various cryptocurrencies worth $339,000 from a Coinbase account owned by a decedent. Hackers took control of the deceased's email address and transferred the cryptocurrencies to their own electronic wallet. The heirs brought a claim under a homeowners policy covering theft, defined as "loss of property from a known place when it is likely the property has been stolen."

The policy covered "direct physical loss to property," including personal property "while it is anywhere in the world." The Court cited to California case law interpreting "direct physical loss" to require physical alteration of or to the property, and holding that the loss of a database does not qualify as direct physical loss "unless the database has a material existence, formed out of tangible matter, and is perceptible to the sense of touch." The Court applied these rules to hold that loss of cryptocurrency is not, as a matter of law, direct physical loss, and hence there was no coverage.

Business E-Mail Compromises and Social Engineering

According to many reports, the most common claims in 2022 shifted from Ransomware to Business E-Mail Compromises. There have been numerous reported decisions on such cases over the years, addressed in detail in our prior annual reviews. There is a tedious similarity in many of these cases, so this year's review will only present summary descriptions with the distilled essence of the individual 2022 cases.

Decisions Finding Coverage

***Fishbowl Sols.*, Inc.,** *supra at 3,* applied the Data Breach Coverage Form of a Technology Professional Liability Policy issued to a technical consulting and software development company to provide coverage for a Business E-Mail Compromise. See the full discussion above.

Ernst & Haas Mgmt. Co., Inc. v. Hiscox, Inc., 23 F.4th 1195 (9th Cir. 2022) is a Ninth Circuit decision construing a Commercial Crime Insurance Policy to provide coverage under Computer Fraud and Funds Transfer provisions. The accounts payable clerk misdirected payments. The loss was the direct result of the original fraudulent email, not the clerk's directions to the bank.

City Unalaska v. Nat'l Union Fire Ins. Co., 591 F. Supp. 3d 440 (D. Alaska 2022) construed the Computer Fraud provisions of a Crime Policy, finding coverage when a fraudster purporting to be a vendor sent a city employee an email requesting a change to its payment instructions for invoices, and the employee paid several invoices. The insurer paid the sublimit of the Impersonation Fraud Coverage endorsement, but declined to find coverage under the Computer Fraud provisions. It argued that the insured's loss did not "result[] directly from the Fraudster's emails," because that phrase requires that the Fraudster's use of a computer, in itself, brings about the funds transfer, with no intervening actions by others. The Court disagreed, holding that the phrase "resulting directly from" only requires proximate causation, and the Fraudster's emails were the proximate cause of the loss.

Decisions Finding No Coverage

Star Title Partners Palm Harbor, LLC v. Ill. Union Ins. Co., No. 21-13343, 2022 WL 4075048 (11th Cir. Sept. 6, 2022) found that the Cybercrime Endorsement of a Cyber Protection Policy does not provide coverage under the following facts. A title company sent a wire transfer of $180,000 to a scam account upon receipt of a fraudulent email from what appeared to be a representative of a Texas-based lender, Capital Mortgage. The Deceptive Transfer Fraud Provision provided coverage for loss from misleading communications from employees, customers, clients, or vendor. Capital Mortgage was none of these because it was not technically doing business with the insured.

Constr. Fin. Admin. Servs., LLC v. Fed. Ins. Co., No. 19-0020, 2022 U.S. Dist. LEXIS 103042 (E.D. Pa. June 9, 2022) involved a claim under a Professional Errors and Omissions Policy (E&O policy) which defined "insured services" as consulting services performed for others for a fee, including those performed electronically via the internet or a Computer Network. The insured was a third-party fund administrator for construction contractors. It received email requests by a Fraudster pretending to be one of its clients, directing payments to a foreign company, and made the payments. It sought recovery under the E&O policy, but the insurer denied, and the Court agreed, because of the policy's exclusion for loss "based upon, arising from or in consequence of any unauthorized or exceeded authorized access to" any computer system or network.

Decisions with Mixed Results

SJ Computers, LLC v. Travelers Cas. & Sur. Co. of Am., No. 21-CV-2482 (PJS/JFD), 2022 WL 3348330 (D. Minn. Aug. 12, 2022) found that a $600,000 social engineering loss was not covered under the Computer Fraud provision of a Crime Policy, but was covered under the policy's Social Engineering Fraud Provisions, which had a sublimit of

$100,000. The insured's purchasing managers received spoofed emails from a bad actor pretending to be a vendor, fraudulently requesting a change in wire transfer information. The bad actor then hacked into the purchasing manager's email and sent fake invoices. The insured's CEO tried to verify the new wire information, failed to reach the vendor, and nonetheless completed the wire transfers.

The Computer Fraud provisions specifically excluded entries or changes made by employees or authorized personnel in reliance on fraudulent instructions. However, the facts fell squarely into the provisions of the Social Engineering Fraud provisions. In fact, that is how the insured originally submitted the claims, only later trying to invoke the Computer Fraud provisions. Yet the Policy expressly provided that the Social Engineering Fraud coverage will not apply to loss or damage due to Computer Fraud. This the two coverages were mutually exclusive.

Landings Yacht, Golf & Tennis Club, Inc. v. Travelers Cas. & Sur. Co. of Am., No. 2:22-CV-464-SPC-NPM, 2022 WL 3227279 (M.D. Fla. Aug. 10, 2022), the Court construed a Crime Policy, finding no coverage for $575,000 in wire transfers because the policy expressly applied only if an instruction to transfer purports to have been transmitted *by the insured* itself. The non-covered transfers were made based on the instructions of a payroll services company, Paychex, Inc., purporting to be acting *on behalf of* the Insured. The court stressed that the Policy's definition of "Insured" did not include an entity allegedly acting *on behalf of* the insured. The Court noted that such language was "notably absent." However, other transfers of $7,000 were allegedly made by individuals who purported *to be* the insured. These allegations were sufficient to allow the coverage dispute to continue as to those transfers.

Illinois Biometric Information Privacy Act (BIPA) Decisions

Overview of Pending Litigation

There is extensive ongoing litigation concerning whether coverage for alleged BIPA violations exists under CGL and Businessowners policies. In 2022, a clear split of authority emerged within the Illinois federal courts with respect to the effect on BIPA claims of the Access or Disclosure exclusion commonly found in these policies. It appears this issue is destined for the Seventh Circuit Court of Appeals.

This issue takes added importance because on September 26, 2022, in the first BIPA class action to be tried to verdict, an Illinois jury found in favor of a class of Illinois truck drivers. ***Rogers v. BNSF Ry. Co.***, No. 19 C 3083, 2022 WL 4465737 (N.D. Ill. Sept. 26, 2022).

Decisions Finding Coverage

Am. Fam. Mut. Ins Co., S.I. v, Caremel, Inc., et al., Case No. 20-c-637, 2022 WL 79868 (N.D. Ill. Jan 7, 2022) found there was coverage notwithstanding the presence of an

Access or Disclosure Exclusion, an Employment Related Practices Exclusion, and a Violation of Statutes Exclusion.

Citizens Ins. Co. Am. v. Thermoflex Waukegan, LLC, Case No. 20-cv-05980, 2022 WL 602534 (N.D. Ill. March 1, 2022) found coverage under a Businessowners Policy notwithstanding the presence of an Access or Disclosure of Confidential or Personal Information Exclusion, an Employment Related Practices Exclusion, and a Recording and Distribution of Material or Information Exclusion.

State Auto. Mut. Ins. Co. v. Tony's Finer Foods Enters., Inc., 589 F. Supp. 3d 919 (N.D. Ill. 2022) found coverage notwithstanding the presence of an Employment Related Practices Exclusion.

Citizens Ins. Co. of Am. v. Highland Baking Co., Inc., No. 20-CV-04997, 2022 WL 1210709 (N.D. Ill. Mar. 29, 2022) found coverage notwithstanding the presence of an Access or Disclosure Exclusion and a Violation of Statutes Exclusion.

Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC, 595 F. Supp. 3d 668 (N.D. Ill. 2022), *appeal dismissed*, No. 22-1713, 2022 WL 15570710 (7th Cir. June 10, 2022) found coverage under a Businessowners policy notwithstanding the presence of a Distribution of Material in Violation of Statutes Exclusion.

Decisions Finding No Coverage

Am. Fam. Mut., Ins. Co., S.I. v. Carnagio Enters., Inc., No. 20 C 3665, 2022 WL 952533 (N.D. Ill. Mar. 30, 2022) and ***Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc.***, 595 F. Supp. 3d 677 (N.D. Ill. 2022) were released the same day by Federal District Judge John Z. Lee. Each found that the Access or Disclosure Exclusion unambiguously barred coverage for BIPA claims.

Church Mut. Ins. Co. v. Prairie Vill. Supportive Living, LLC, No. 21 C 3752, 2022 WL 3290686 (N.D. Ill. Aug. 11, 2022) found that coverage under an Employment Practices Policy was barred by the Violation of Laws Applicable to Employers Exclusion.

Miscellaneous Privacy Decisions

California Supreme Court Opens the Possibility of TCPA Coverage under CGL Policies, where that Meets the Objectively Reasonable Expectations of the Insured

Yahoo Inc. v. Nat'l Union Fire Ins. Co. Pittsburgh, PA, 14 Cal. 5th 58, 519 P.3d 992 (2022) addressed a question certified to the California Supreme Court by the United States Ninth Circuit Court of Appeals. It arose from a coverage dispute concerning the Insurer's duty to defend a series of putative class action lawsuits alleging that Yahoo!'s unsolicited text messaging had violated the federal Telephone Consumers Protection Act

("TCPA"). The opinion examined the meaning and interaction of the "personal and advertising injury" provisions in a standard CGL policy (which generally excludes injuries resulting from violation of the TCPA), as modified by an endorsement which generally removed the exclusion for injuries arising from violations of the TCPA. There are nuances in the language, and the Ninth Circuit performed an extensive linguistic analysis applying concepts such as (1) the proper interpretation of a restrictive relative clause with the word "that" as its relative pronoun, and (2) the rule of the last antecedent (which the lower court applied). Despite the careful analysis, the Court concluded that the coverage was ambiguous, and the standard rules of contract interpretation did not resolve the ambiguity. But instead of interpreting the ambiguity in the insured's favor at this juncture, it concluded that the language must be interpreted in a way that fulfills the Insured's objectively reasonable expectations. It concluded that this must be determined through further litigation. Only if the ambiguity remains unresolved should the Court resort to the rule of construing it against the insurer.

The California Supreme Court emphasized that although the Policy also contained an advertising injury exclusion, the insured had not litigated the case based on that exclusion thus far, so it expressed no view on its application.

In response to this decision, the Ninth Circuit remanded the case to the District Court to develop a record and hear argument on the insured's objectively reasonable expectations, "as well as any other issues that arise in the first instance."

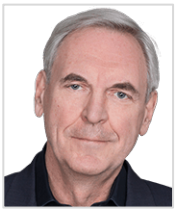
Federal Court in North Carolina Finds No Duty to Defend Alleged Violations of Driver's Privacy Protection Act under CGL Policies

AMCO Ins. Co. v. Van Laningham & Assocs., PLLC, No. 5:20-CV-553-D, 2022 WL 2813041 (E.D.N.C. July 18, 2022) held there was no Duty to Defend lawsuits alleging violations of the federal Driver's Protection Privacy Act ("DPPA"). In North Carolina, information on traffic accidents is recorded in reports which include personal information on the drivers involved, including the driver's names, dates of birth, addresses, and driver's license numbers. The insureds were a lawyer and law firm who allegedly obtained the reports and used the information to mail marketing materials for legal services to the drivers. Several cases were brought by plaintiffs who alleged violations of the DPPA. Those cases were dismissed on summary judgment, on the grounds that the conduct did not violate the DPPA. The insurers defended those lawsuits under CGL policies pursuant to a reservation of rights.

The Court applied the comparison test of North Carolina law, comparing the insurance policy with the allegations of the complaints. Claims under Coverage A were summarily dismissed on the grounds that there were no bodily injuries involved when the plaintiffs retrieved the mailings addressed to them and "had their privacy invaded."

The analysis focused on Coverage B, "personal and advertising injury," specifically the enumerated tort of "oral or written publication, in any manner, of material that violates a

person's right to privacy." The Court held that because the alleged injuries focused on obtaining information for a purpose not authorized by the DPPA, the injuries did not involve "publication" of material. And even if there had been a "publication," coverage was barred by several exclusions, including the exclusions for criminal acts, recording and distribution of material in violation of law, and violation of consumer protection statutes.



Vince Vitkowsky is a partner in Gfeller Laurie LLP, resident in New York. He focuses on cyber risks, liabilities, insurance, and litigation. Vince assists insurers in all aspects of coverage evaluation and dispute resolution in many lines of business, including cyber, CGL, property, and professional liability. He also assists in complex claim evaluations, and at times, the defense of insureds in complex matters. He also assists in product development and in drafting policies and endorsements. *vvitkowsky@gllawgroup.com*

.