GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions in 2021

Vincent J. Vitkowsky

Connecticut Massachusetts New York New Jersey Pennsylvania

TABLE OF CONTENTS

Cyber Risks and Insurance Coverage Decisions in 2021

Introduction

We are pleased to present this White Paper addressing decisions rendered by U.S. Courts in 2021 on the law of insurance coverage for cyber risks.

Many more decisions from recent years are addressed in our earlier White Papers entitled, respectively, ***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 bitcoin theft. Like the decisions in this White Paper, 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 White Papers 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 White Papers, 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 10, 2022

vvitkowsky@gllawgroup.com
www.gllawgroup.com

Cyber Risks and Insurance Coverage Decisions in 2021

Vincent J. Vitkowsky
Gfeller Laurie LLP

Ransomware

Connecticut Federal Court Declines to Dismiss a Claim for Breach of the Implied Covenant of Good Faith and Fair Dealing under Data Breach Coverage brought by an IT Provider Suffering a Ransomware Attack

New England Sys., Inc. v. Citizens Ins. Co. of Am., Case No. 3:20-cv-01743 (JAM), 2021 WL 1978691 (D. Conn. May 17, 2021) involved the denial of business interruption coverage for a ransomware breach under the Data Breach Coverage Part of a Businessowners Policy. In an unusual factual setting, the Court denied a motion to dismiss a claim for breach of the implied covenant of good faith and fair dealing.

New England Systems, Inc. ("NES") is an information technology services provider which itself suffered a ransomware attack. Citizens consented to an arrangement in which NES would repair its own computer systems, given its technical ability and knowledge of the impacted systems. The efforts took more than sixty days and were compensated as a Breach Restoration Expense. During the sixty-day period, NES could not perform contract work for its clients, both because of the damage to its systems and because it was occupied with the repairs. Citizens denied NES's claim for Cyber Business Interruption and Extra Expense coverage.

NES asserted claims for breach of contract, violation of the Connecticut Unfair Insurance Practices Act ("CUIPA") as made actionable under the Connecticut Unfair Trade Practices Act ("CUTPA"), and for breach of the implied covenant of good faith and fair dealing. The Court dismissed the CUIPA/CUPTA claim, which was partially based on a statement on the Citizens' website that coverage included "Cyber Business interruption and extra expense incurred due to a breach," as well as losses to "finances, reputation and operational capabilities." However, a disclaimer at the bottom of the website stated that coverage was subject to the issued policy, and that the website "material is provided for informational purposes only and does not provide any coverage." The Court found the disclaimer fatal to the false advertising claim under CUIPA. NES also alleged unfair claim settlement practices, but the Court found the mere allegations that any of the acts complained of constituted a general practice by Citizens were insufficient.

On the final claim, NES alleged that "Citizens falsely represented that NES had waived its right to claim business interruption insurance," that "Citizens intentionally misrepresented pertinent policy provisions when it allowed NES to undertake self-repair

work without disclosing that Citizens knew it would consider NES ineligible for business-interruption coverage if it performed such work," and that "Citizens engaged in no investigation of its claims whatsoever." The Court ruled that "taken together, these allegations are enough for initial pleading purposes to support a claim that Citizens acted in bad faith to impede NES's rights to the benefits of its insurance policy." Thus, the Court denied a motion to dismiss the claim for breach of the implied covenant of good faith and fair dealing.

Construing the Computer Fraud Provision of a Commercial Crime Coverage Part, the Indiana Supreme Court Holds Payment of Bitcoin in a Ransomware Attack Was a Direct Result of the Attack, but Remands for a Determination of Whether a Computer Was Accessed Fraudulently

G&G Oil Co. of Indiana, Inc. v. Cont'l W. Ins. Co., 165 N.E.3d 82 (Ind. 2021) involved an oil company seeking to recover the amount of Bitcoin paid in a ransomware attack under the Computer Fraud provision of a Commercial Crime Coverage Part. The provision covered loss "resulting directly from the use of a computer to fraudulently cause a transfer of money." The Court first construed the phrase "fraudulently cause a transfer of money." It concluded that the trial court's interpretation -- finding the loss was not fraudulently caused, but resulted from theft—was too narrow. The Court found the phrase to be unambiguous but broad. Noting there are many kinds of fraud, and that computer hacking can take multiple forms, it concluded that the phrase "'fraudulently cause a transfer' can be reasonably understood as simply 'to obtain by trick.'" Using that definition, it found that at this point, neither party had presented sufficient evidence to warrant summary judgment.

The Court next considered whether the payment of ransom was a loss that "resulted directly from the use of a computer." Continental argued that the voluntary transfer of Bitcoin was an intervening cause that severed the causal chain of events, so the loss did not result "directly." The Court rejected this argument, holding that the payment resulted either "immediately or proximately without significant deviation from the use of a computer." It held "the 'voluntary' payment was not so remote that it broke the causal chain." The end result of these rulings was to remand the case to the trial court for further development of the circumstances of the ransomware attack, to determine whether entry into the insured's computer system was "fraudulent."

Ohio Appellate Court Finds Genuine Issues of Material Fact as to Whether an Insured's Claim for Damaged Software Following a Ransomware Attack Was Covered by an Electronic Equipment Endorsement to a Businessowners Policy

EMOI Services, LLC v. Owners Ins. Co., Case No. 29128 2021 WL 5144828 (Ohio Ct. App 2d Dist. Montgomery, Nov. 5, 2021) reversed a grant of summary judgment against an insured following a ransomware attack. EMOI, the insured, provides medical billing services and application services and support to medical providers. Its system was hacked and files encrypted. The hacker made a ransom demand of three bitcoins (at the

time, worth approximately $35,000). EMOI paid the hacker and received the decryption key. Even after multiple decryptions, there were still residual problems with the system.

EMOI had a Businessowners Insurance Policy ("Policy") issued by Owners. The Policy had a Data Compromise Endorsement addressing the compromise of "personal data," and expressly excluding "threat, extortion, or blackmail", including "ransom payments and private security assistance." The Policy also had an Electronic Equipment Endorsement addressing "direct physical loss or damage to 'media.'" "Media" was defined as "materials on which information is recorded, and the provision listed non-exclusive examples of "film, magnetic tape, paper tape, discs, drums, and cards." It further stated that "Media" includes "computer software and reproduction of data contained on covered media." Owners denied coverage and EMOI commenced a breach of contract action. EMOI argued it was seeking coverage for "the damage to the media, not the information or data contained on the media," and asserted the computer software was damaged because it was not accessible or usable, and that there were ongoing problems with the software. Owners argued that because the software was intangible, there was no "direct physical loss or damage."

The Court referred to the provision that "computer software and reproduction of data contained on covered media" fall within the definition of "media," and construed it to mean that the "computer software must be contained in another medium for the provision to apply." The Court applied the principle of *ejusdem generis* to the definition of "media," and concluded that "viewing the evidence in the light most favorable to EMOI, the company's servers constituted materials on which EMOI's information was recorded and thus arguably met the policy's definition of 'media'." The software and reproduction of data was contained within the servers, so those items were also within the definition of "media."

The Court then addressed whether the software was damaged. EMOI's IT manager had testified that portions of the software remained inaccessible and non-functional. The automated phone system could not be decrypted. After the initial decryption, the software became encrypted again, and once again had to be decrypted. Viewing the evidence in EMOI's favor, the Court concluded that there were genuine issues of material fact as to whether the software was damaged.

The Court then addressed whether the damage to software constitutes "direct physical loss or damage" to covered property. It noted with significance that this policy did not include the term "tangible" before the term "property." The Court noted that neither party offered a technical description of how encryption and decryption occur, and the effects on the item encrypted. So again, construing the evidence in EMOI's favor, the Court found it "supports a conclusion that the encryption damaged EMOI's software and data, and that damage was not merely aesthetic or amounted to loss of access or use." Owners relied on California case authority holding that there can be no direct physical loss or damage to property that is not tangible. But the Court noted EMOI's argument that software "is tangible enough for [Owners] to insure and expressly define within 'media' and thus, must be tangible enough to be damaged or suffer direct physical damage." And

EMOI's IT manager testified that the software and reproduction of data was damaged, so once again construing the evidence in EMOI's favor, the Court concluded that the policy contemplated that software and reproduction of data was capable of being physically damaged.

Owners also relied on Exclusions for media failure, a malfunction or breakdown of equipment while the media was being run, a loss of market or improper operation of the media. The Court rejected each of these.

Finally, the Court allowed a claim for bad faith against Owners to continue to trial. The claims handler received and denied the claim on the same day, possessed little if any meaningful experience with computer matters, and did not consult with an IT or computer expert while evaluating the claim.

Damage to Software

Federal Court in North Carolina Holds that CGL Coverage A Does Not Apply To Claims Concerning Software Because There Was an Electronic Data Exclusion, No Allegations of Damage to Hardware, and No Occurrence

Nautilus Ins. Co. v. Philips Med'l Sys. Nederland B.V., et al., No. 3:20-CV-0057-GCM, 2021 WL 29415571 (W.D.N.C. Jul. 13, 2021) applied North Carolina law to a coverage dispute concerning an underlying lawsuit brought against insureds of Nautilus by Philips Medical Systems Nederland B.V. ("Philips'). Philips develops, sells, and maintains medical imaging systems and related proprietary software. Nautilus issued CGL policies to Transtate Equipment Company and others, which provided maintenance and support services to Philips. Philips alleged that the insureds, among other things, gained access to and made unauthorized copies of Philip's software, which it then used to compete unfairly. In turn, Nautilus brought a declaratory judgment action, asserting it had no duty to defend or indemnify any insureds in the underlying lawsuit.

The insureds invoked Coverage A, which provided that the insurer "will pay those sums that the insured becomes legally obligated to pay as damages because of … 'property damage' caused by an 'occurrence.'" "Property Damage" was defined as "physical injury to tangible property, including all resulting use of that property." The policies specifically provided that "electronic data is not tangible property." Electronic data was defined to include computer software.

The complaint in the underlying lawsuit alleged that the insureds "damaged Philips' Systems and the proprietary software on the Systems." The insureds asserted that this was sufficient to allege "property damage" because damage to the Systems, *i.e.,* the machines, is damage to tangible property. But the Court noted that nothing in the underlying complaint alleged damage to the Systems' hardware, such as the monitor, keyboard, mouse or wiring, which it considered the "tangible property elements of the machines." Thus, it concluded that there were no allegations of "property damage" as

defined in the policies. Further, the Court concluded there was no "occurrence," which the policies define as an "accident." The underlying complaint only alleged the insureds' knowing, intentional, and/or deliberate actions, so there was no "occurrence." The Court also found that the Expected or Intended Injury Exclusion precluded coverage. It granted summary judgment in favor of Nautilus.

Payment Card Breaches

Fifth Circuit Holds that Insurer Must Defend a Data Breach Under Personal and Advertising Injury Coverage

Landry's, Inc. v. Ins. Co. of the State of Pa., 4 F. 4th 388 (5th Cir. 2021) involved a retailer who operated restaurants, hotels and casinos. Its payment card transactions were processed by Paymentech, LLC, a branch of JP Morgan Chase Bank. Paymentech suffered a data breach. Cardholders' names, numbers, expiration dates and internal verification numbers were stolen from the cards' magnetic strips from millions of credit cards. At least some of the information was used to make unauthorized charges. Paymentech participated in Visa's Global Compromised Account Recovery Program, incurring over $12.6 million in liability, and MasterCard's Account Data Compromise Program, incurring over $7.3 million in liability. Paymentech and Landry's had a Select Merchant Payment Card Processing Agreement, requiring Landry's to comply with all Payment Brand rules and security guidelines, and indemnify Paymentech for any assessments against it by Visa and Mastercard. Landry's refused to pay, and Paymentech commenced suit against it.

Landry's sought coverage and a defense under the personal and advertising injury section of its insurance with Insurance Company of the State of Pennsylvania ("ICSOP"). The Court applied the "eight-corners" rule of Texas, comparing the four corners of the policy to the four corners of the Paymentech complaint. The Court determined that the parties intended for the phrase "oral or written publication, in any manner" in the policy to be defined in the broadest manner possible. It applied dictionary definitions of publish, including a Webster's definition "to make known . . . as by exposing or presenting it to view". The Court applied the rule that any ambiguity must be resolved in favor of the insured. The Court found two publications – Landry's to the hackers, and the hackers in making fraudulent purchases. The Court noted that at the stage of determining a duty to defend, it is irrelevant whether Landry's did in fact cause the publication. It was sufficient that Paymentech *alleged* publication.

The Court went on to determine that the alleged publication involved an injury "arising out of … the violation [of] a person's right of privacy." It found it to be "undisputed that a person has a right of privacy in his or her credit-card data." ICSOP argued that the policy only covers damages in tort, not breach of contract, but the Court followed Texas Supreme Court authority which makes no distinction between tort and contract damages in this context. It said that the focus should be on facts alleged, not the legal theories

invoked. Finally, the Court found that it made no difference that the suit was brought by Paymentech, as opposed to the individual consumers whose credit card data was stolen.

Minnesota Federal Court Holds There is No Coverage Under CGL Policies for Replacement of Compromised Cards

Target Corp. v. ACE American Ins. Co., et al., 517 F.Supp.3d 798 (D. Minn. 2021) grew out of the massive credit and debit card breach of Target in 2013. As always in these such cases, the banks cancelled the cards and reissued new cards, incurring substantial expenses. The banks sued Target for these expenses, and the case was settled. Target sought indemnity for the settlement under two Commercial General Liability ("CGL") policies. It relied upon the Policy language providing coverage "for the 'ultimate net loss' … because of 'bodily injury' or 'property damage.'" Property damage was defined as the "loss of use of tangible property that is not physically injured" and the Policy provided that "all such loss of use shall be deemed to occur at the time of the 'occurrence' that caused it." Minnesota law applied to the cross-motions for summary judgment.

The Court stressed that the case involved the duty to indemnify, not the duty to defend. The Court assumed without deciding that a data breach was an occurrence but found that Target could not prevail for other reasons. Specifically, if found there was no "loss of use." It stated that Minnesota courts have held loss-of-use damages must be "based on" the alleged loss of use … It interpreted these cases as suggesting that Minnesota law requires loss-of-use damages to have some connection to the value of the use of the now-damaged property when it previously was unimpaired. It found "the record is devoid of allegations or evidence as to what the value of the *use* of the payment cards is, either to Target's customers or to the payment card companies." (Emphasis by the Court.) So "damages cannot be 'based on' the loss of use because there is no nexus between the damages and the loss of use … Target has not established a connection between the damages incurred for settling claims related to replacing the payment cards and the value of those cards, either to the payment-card holders or issuers." It thus found the connection "insufficiently direct" and concluded that Target's settlement liability did not constitute loss-of-use damages. It granted ACE's motion for summary judgment.

Social Engineering and Business Email Compromises

Fifth Circuit Finds No Coverage Under Commercial Crime Policies for Funds the Insured Did Not Hold that Were Lost in a Phishing Exploit

RealPage, Inc. v. National Union Fire Ins. Co. of Pittsburgh, Pa. and Beazley Ins. Co., Inc., 2021 WL 6060972 (5th Cir. Dec. 22, 2021) involved transfers through a service provider to property managers. A fraudster used a targeted phishing scheme to obtain the account credentials of a RealPage employee, and diverted over $10,000,000 in rent payments owed to the property managers. Some payments were recovered, but over $6,000,000 were not. RealPage reimbursed its clients for the lost funds. Applying Texas

law, the Court found the loss was not covered by commercial crime policies issued by National Union and Beazley.

The structure of the transactions was as follows. Tenants and property managers would provide RealPage with bank account, credit card, and routing information. RealPage would transmit the information to a processing service provider named Stripe. Stripe would then direct its bank, Wells Fargo, to process a transfer of funds from the tenants' bank accounts to Stripe's bank account at Wells Fargo. Thereafter Stripe would direct another transfer to pay the funds to the property managers' accounts.

The policy provided that "[T]he property covered under this policy is limited to property: (1) That you own or lease; or (2) that you hold for others …." Giving effect to all the words in the policy, the Court reasoned that "hold" must have a meaning distinct from "own" or "lease." It relied on the Black's Law Dictionary definitions of "hold," and concluded the only definitions applicable in this context are "[t]o keep in custody or under an obligation," and "[t]o possess or occupy[.]" The Court concluded that RealPage never possessed (or kept in its custody) the funds at issue. RealPage merely provided routing instructions to Stripe, and never "held" the funds intended for the property managers. Although the Court did not accept the Insured's argument that "hold" could also mean "control," it found that even if it did, the Insured did not control the funds designated for the property managers.

The Court rejected the argument that the Insured held the funds in bailment. The Insured never had possession of any funds, nor did it ever accept delivery of any property, so no bailment could exist. Finally, the Court also rejected an agency theory because the services agreement between the Insured and the processor explicitly disclaimed any agency relationship. And after providing routing instructions, the Insured had no power to control the payment processes.

The Court affirmed summary judgment in favor of National Union and Beazley.

Fifth Circuit Holds There Is No Coverage Under a Computer Transfer Fraud Provision that Required the Transfer Be Made Without the Insured's Knowledge or Consent

Miss. Silicon Holdings, LLC v. Axis Ins. Co., 843 **Fed.Appx.** ***581*** (5th Cir. 2021) involved a silicon metal manufacturer, Mississippi Silicon Holdings, LLC ("MSH"), who fell victim to a social engineering cybercrime. It received an email from a regular vendor, directing that future payments should be sent to a new bank account, attaching a letter on the vendor's letterhead and apparently signed by one of the vendor's executives. The scheme involved the creation of a "fraudulent channel" in MSH's email system, through which the fraudsters could monitor and alter emails sent between MSH and its vendor. MSH paid approximately $1.025 million, pursuant to a verification process that involved three of its employees to authorize the transfer. MSH sought recovery from Axis Insurance Co. ("Axis") under a commercial crime policy that covered (1) Social Engineering Fraud, (2) Computer Transfer Fraud and (3) Funds Transfer Fraud. Axis

paid under the Social Engineering Fraud provision, which had sub-limits of $100,000, but denied coverage under the other provisions.

The case addressed the Computer Transfer Fraud provision, which covered loss "resulting directly" from a fraudulently induced transfer made "without the Insured Entity's knowledge or consent." The lower court had focused on the "resulting directly" language, but the Fifth Circuit did not reach that issue. Instead, applying Texas law, it held that there was no coverage because of the requirement that the transfer must be made without the Insured Entity's consent. Three employees had affirmatively authorized the transfer, so even though they had no knowledge of the fraud, the denial of coverage was proper. The Fifth Circuit noted that the situation in which an employee relies in good faith on a fraudulent instruction was covered under the Social Engineering Fraud provision, not the Computer Transfer Fraud provision. It affirmed summary judgment for Axis.

Pennsylvania Federal Court Holds That Losses from Fraudulent Emails and Wire Transfer Authorization Forms Are Not Covered under a Commercial Crime Policy's Forgery or Alteration Provisions

Ryeco, LLC v. Selective Ins. Co., No. 20-3182, 2021 WL 1923028 (E.D. Pa. May 13, 2021) involved a claim by a fruit and vegetable receiver and distributor. A hacker gained access to the email account of the company's Vice President of Operations and sent emails to a bank directing it to execute wire transfers consistent with Wire Transfer Authorization Forms attached to the emails. The forms purportedly bore the signature of two employees authorized to sign them. There were 15 transactions totaling approximately $1,462,000.

The commercial crime policy insurer offered three different potentially applicable coverages – Forgery or Alteration, Funds Transfer, and Computer Fraud. Ryeco only purchased the Forgery or Alteration Coverage. The Court construed the Forgery or Alteration provision as requiring that written promises, orders or directions to pay a sum certainly must result in a negotiable instrument. It referred to federal courts around the country reaching this conclusion. A Wire Transfer Authorization Form is a direction to a bank to do something. It is not negotiable. Finding no coverage under the Forgery or Alteration provision, the Court granted Selective's motion for summary judgment.

The Court emphasized that Ryeco chose not to purchase the other two coverages. In dicta, it stated that the coverages do not overlap. "The Computer Fraud provision does not cover Funds Transfer Fraud and the Funds Transfer provision does not cover Computer Fraud. The term 'fraudulent instruction' in the Funds Transfer provision covers a written instruction "other than those described in the [Forgery or Alteration] provision."

Biometric Information

Illinois Supreme Court Finds a Duty to Defend under Businessowners Policies where the Plaintiff Alleged Emotional Upset, Mental Anguish and Mental Injury from Sharing of Her Fingerprints with a Single Third Party, and Declines to Apply Violation of Statutes Exclusion

West Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc., 2021 IL 125978 (2021) is a landmark coverage case under the Illinois Biometric Information Privacy Act ("BIPA"). It found the insurer had a Duty to Defend under the Privacy coverage of Businessowners Policies based on the allegation that an insured had suffer injury consisting of emotional upset, mental anguish and mental injury because of sharing her fingerprints to a single third party.

Plaintiff filed a class action alleging that a tanning salon and franchise of L.A. Tan violated the written release provisions of BIPA by scanning customers' fingerprints without first obtaining the required written release, and violated the disclosure prohibitions by systematically disclosing those biometric identifiers and information to a single out-of-state vendor. The Court analyzed the components necessary for coverage: personal injury; publication; and the right to privacy.

The Court found the allegations that plaintiff suffered personal injury, consisting of emotional upset, mental anguish, and mental injury, were sufficient to trigger coverage if the other elements were met. The term "publication" was not defined in the policies, so the Court looked to definitions in dictionaries, insurance law and law of privacy treatises, and the Restatement (Second) of Torts. It concluded that all three sources included publications not only to the public at large, but also to a single third party. The policies also did not define "Privacy," so the Court again turned to dictionaries and insurance cases. It found that Privacy includes the right to secrecy. It ruled that BIPA "protects a secrecy interest – here, the right of an individual to keep his or her personal identifying information like fingerprints secret." Thus, it found the allegation of shared biometric information "alleges a potential violation of [the] right to privacy within the purview of the policies."

In finding coverage, the Court declined to apply the Exclusion for Violation of Statutes. That Exclusion applied to (1) the TCPA, (2) the CAN-SPAM Act, and (3) statutes "other than" those two that prohibit or limit the communication of information. The Court applied the interpretive principle of *ejusdem generis* to conclude that the "other than" language only extended the Exclusion to the same general kind or class of things as those specifically mentioned. The Exclusion related only to the methods of communication, namely telephone calls, faxes and e-mails. It found that BIPA's regulation of the collection, use, storage, and retention of biometric identifiers and information was fundamentally different from the methods of communication, so the Exclusion did not apply.

For all these reasons, the Court found the insurer had a Duty to Defend.

Federal Court In North Carolina Finds No Duty to Defend BIPA Claims, Enforcing the Recording and Distribution of Material or Information Exclusion of General Liability and Umbrella Policies

Massachusetts Bay Ins. Co., et al. v. Impact Fulfillment Services, LLC, et al., No. 1:20CV926, 2021 WL 4392061 (M.D.N.C. Sept. 24, 2021), also involved BIPA claims. But unlike *West Bend Mut., supra,* it enforced an exclusion and found no duty to defend. The insureds are North Carolina Companies who sought a defense and coverage for class actions brought by their employees. They contended that the personal and advertising injury provisions of their general liability and umbrella policies provided coverage.

A class action alleging BIPA violations was brought in state court in Illinois. The insureds allegedly used employees' fingerprints as part of their payroll time-keeping procedures at one of their facilities in Illinois, but did not make the required disclosures or obtain the required consents. The insurers denied coverage based on the Recording and Distribution of Material or Information Exclusion (the "Exclusion.") The Exclusion applies to the alleged violation of statutes which limit the "printing, dissemination, disposal, collecting, recording, sending, transmitting, communicating or distribution of material or information." The Court referred to another federal court, in another district in North Carolina, which applied North Carolina law, and which interpreted a similar exclusion to deny coverage for an alleged violation of a federal privacy law, the Driver's Privacy Protection Act. *Hartford Cas. Ins. Co. v. Greve*, No. 3:17CV183-GCM, 2017 WL 5557669 (W.D.N.C. Nov. 17, 2017). It also referred to another court which, in construing an identical provision to the one in this case, found it excluded coverage alleging violations of the Song-Beverly Credit Card Act. *One Beacon Am. Ins. Co. v. Urb. Outfitters, Inc.,* 21 F. Supp 3d 426 (E.D .Pa. 2014). The Exclusion here contains catch-all language – "any federal, state, or local statute" – following a list of specifically enumerated statutes: the TCPA, the CAN-Spam, and the FCRA/FACTA statutes. This Court, too, applied the interpretive principle of *ejusdem generis,* which it described as providing that general catch-all language, directly following a list of specific items, is construed to include "only things of the same kind, character and nature as those specifically enumerated." However, the Court found that the Exclusion here, which bars the collection and dissemination of information, is consistent with BIPA's prohibition against collection and disclosure of biometric identifiers and biometric information. It also found that BIPA is of the same kind, character and nature as the enumerated statutes in the Exclusion.

The Court acknowledged the decision in *West Bend Mut. Ins. Co., supra*, but distinguished it on the ground that the exclusion in that case was similar to the exclusion in *Greve, supra,* but different from the one here, because the *West Bend Mut/Greve* exclusion specifically listed only the TCPA and CAN-SPAM statutes. The Court also stated that if there were any contradictions between *Greve* and *West Bend,* it would resolve those contradictions in favor of *Greve,* which applied North Carolina law, not Illinois law. Thus, the Court found that the insurers had no duty to defend the BIPA claims.

Federal Court in Illinois Finds a Duty to Defend BIPA Claims under an Employment Practices Liability Part, but not under a D&O Liability Part

Twin City Fire Ins. Co. v. Vonachen Services, Inc. et al., 2021 WL 4876943 (C.D. IL Oct. 19, 2021) involved two putative class actions alleging BIPA violations. The insureds required their employees to use their fingerprints "as a means of authentication" via a biometric tracking system. It did not make the required disclosures or obtain the required consents. The insurer issued a Private Choice Premier Policy with two coverages: (a) a Directors, Officers and Entity Liability Coverage Part; and (b) an Employment Practices Liability Coverage Part. The issue was the duty to defend.

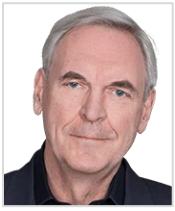
As a preliminary matter, the Court concluded it would consider the Insured's Employee Handbook in determining whether there was a duty to defend. Although the Employee Handbook was not referenced specifically in the class action complaints, the timekeeping requirements were memorialized in it. Also, the Policy specifically mentioned "obligations arising from the handbooks."

As to the D&O coverage, both parties agreed in the first instance that the underlying BIPA claims fell within the D&O coverage. However, Twin City asserted that two exclusions applied. First, it relied on the Insured v. Insured Exclusion. That contained an exception for Whistleblowing, and the Court found that this exception would apply. However, the Court also found that the Invasion of Privacy Exclusion would apply. The parties did not address how these provisions are to be read together, and the Court declined to do so, in view of its determination that the Exclusion for invasion of privacy applied. It stated that several cases have held that a BIPA violation is an invasion of privacy. It also noted that the Exclusion referred to claims, "based upon, arising from, or in any way related to any actual or alleged invasion of privacy." It found this language to be "incredibly broad," and that BIPA violations are actual invasions of privacy. It concluded that "the exclusion for invasions of privacy is clearly broad enough to exclude the BIPA violations expressed here."

As to the EPL coverage, the Court stated that it was a "close call," but any doubts must be construed in favor of the insured. It reasoned that in the Policy, the Insurer agreed to provide coverage based on any obligations arising from "the handbooks." The Court made no finding as to whether the actual Employee Handbook is a contract, but said it "arguably creates obligations on both parties," and "could be construed as such by a state court." As a result, the allegations in the underlying complaints potentially fell within the EPL coverage."

Further, the Insured argued that the claims alleged constituted a covered "Employee Data Privacy Wrongful Act." That term was defined to include, among other things, an "employment-related invasion of privacy," which is covered when it is "alleged in addition to or as part of any Employment Practices Wrongful Act." Thus, the alleged breach of the Employee Handbook constituted the Employment Practices Wrongful Act, which together with the invasion of privacy, established an Employee Data Privacy Wrongful Act. The

Court found that based on its prior discussion on BIPA and invasions of privacy regarding D&O Coverage, the complaints clearly alleged an "employment related invasion of privacy." Thus, the Insurer had a duty to defend under the EPL Part. The Court declined to reach the duty to indemnify, finding it was not ripe or determination.



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 and reinsurers in product development, and 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 if necessary, the defense of insureds in complex matters.
vvitkowsky@gllawgroup.com

.