GFELLER LAURIE LLP
ATTORNEYS AT LAW

Cyber Risks and Insurance Coverage Decisions 2020

Vincent J. Vitkowsky

Connecticut New York New Jersey Massachusetts

TABLE OF CONTENTS

Introduction 1

Businessowners Policy 2

Maryland Federal Court Finds Coverage for Lost Data and Software, and Loss of Functionality, following a Ransomware Attack, as "Direct Physical Loss of or Damage to" Covered Property and a Computer System under a Businessowners Policy 2

National Ink and Stitch, LLC v. State Auto Prop. and Cas. Ins. Co. 2

Professional Services Liability Policies 3

California Federal Court Finds Coverage under a Professional Services Liability Policy for Receipts which Unmasked Extra Credit Card Digits 3

FedEx Office and Print Services, Inc. v. Continental Cas. Co. 3

New Jersey Court Finds No Coverage for a Social Engineering Loss under a Professional Liability Policy 3

Authentic Title Services, Inc. v. Greenwich Ins. Co. 3

Crime Policies 4

Various Deceptive Funds Transfer Cases under Crime Policies 4

Midlothian Enterprises, Inc. v. Owners Insurance Co. 4

Mississippi Silicon Holdings, LLC v. AXIS Ins. Co. 4

RealPage, Inc. v. National Union Fire Ins. Co. et al. 4

Authentic Title Services, Inc. v. Greenwich Ins. Co. 5

Ransomware Payments under Crime Policy 5

G&G Oil Co. of Indiana v. Continental Western Ins. Co. 5

Significant Non-Coverage Case 5

Pennsylvania Federal Court Finds No Duty to Prevent Transmission of NotPetya Virus under Contract, and No "Broader Social Duty" 5

Heritage Valley Health System, Inc. v. Nuance Communications, Inc. 5

Introduction

We are pleased to present this Resource addressing decisions rendered in 2020 on the law of insurance coverage for cyber risks. We also include a case not involving coverage, but which is significant because it addresses liability for transmission of the NotPetya virus under a given set of facts.

Many more decisions from recent years are addressed in our earlier Compendium entitled ***Cyber Risks and Insurance Coverage Decisions 2015-2019***. That Compendium addressed decisions involving a broader 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. These arose under various types of policies, including CGL, Businessowners, Computer Fraud, Crime, Financial Institution, Cyber, D&O, and Homeowners. A convenience copy of that Compendium accompanies this Resource.

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

Vince Vitkowsky
New York, NY
January 11, 2021

vvitkowsky@gllawgroup.com
www.gllawgroup.com

Please note that this Resource is for informational purposes only, and is not comprehensive. It does not constitute the rendering of legal advice or opinions on specific facts or matters. The distribution of this Resource to any person does not constitute the establishment of an attorney-client relationship.

Businessowners Policy

Maryland Federal Court Finds Coverage for Lost Data and Software, and Loss of Functionality, following a Ransomware Attack, as "Direct Physical Loss of or Damage to" Covered Property and a Computer System under a Businessowners Policy

National Ink and Stitch, LLC v. State Auto Prop. and Cas. Ins. Co., 435 F. Sopp 3d 679 (D. Md. Jan. 23, 2020). National Ink is an embroidery and screen printing business which suffered a ransomware attack. Its server stored art, logos, designs, graphic art software, shop management software, embroidery software, and webstore management software. The ransomware prevented access to everything except the embroidery software. National Ink made the ransom payment, but the attacker refused to release the software and data. In response, National Ink replaced and reinstalled its software, and installed protective software. After that, the computers functioned, but were impaired. The protective software slowed the system. The art files stored in the server could not be accessed. There is a possibility that dormant ransomware could re-infect the system.

The Businessowners Policy covered "direct physical loss of or damage to" Covered Property. The Policy included a Special Form Computer Coverage endorsement which defined "Covered Property" to include "Electronic Media and Records (Including Software)," defined to include "(a) Electronic data processing, recording, or storage media such a films, tapes, discs, drums or cells; (b) Data stored on such media." The Insured sought coverage for the cost of replacing its computer system. State Auto denied coverage on the grounds that there was no direct physical loss of or damage to the computer system that would justify replacement of the entire system.

On a motion for summary judgment, the Court applied Maryland law and found coverage for both the loss of data and software, and the loss of functionality. The Court found that the plain language of the policy endorsement contemplates that data and software are categories of "Covered Property" which can experience direct physical loss or damage.

The Court also found damage to the computer system itself, even though there was only partial, not total, loss of functionality. National Ink was left with a slower system, which appears to be harboring a dormant virus, and unable to access a significant portion of software and stored data. State Auto argued there was no coverage because that would require an utter inability to function. The Court found no such requirement. It held that a "loss of use, loss of reliability, or impaired functionality" constitute physical loss or damage sufficient for coverage.

Professional Services Liability Policies

California Federal Court Finds Coverage under a Professional Services Liability Policy for Receipts which Unmasked Extra Credit Card Digits

FedEx Office and Print Services, Inc. v. Continental Cas. Co., 2020 WL 6804455 (C.D. Cal. Oct. 20, 2020). FedEx provides services through various types of kiosks at its retail stores. These perform functions such as copying, printing, and scanning, as well as other functions. Each kiosk requires the customer to scan a credit card to enable the kiosk to function, and at the end of the use, prints a physical receipt. As a result of a software update, the kiosks "unmasked" extra credit card digits which were then printed on receipts. This resulted in violation of the Fair and Accurate Credit Transactions Act, and class actions followed. The Policy defined a "Professional Services Claim" as "any Claim arising out of a Wrongful Act in the Performance of Professional Services." Continental denied coverage, arguing that the event of "printing a receipt" is not part of "the performance of Professional Services."

Applying California law, the Court held for FedEx, ruling that printing a receipt "is one part of an integrated process unique to FedEx's business model in the performance of providing professional services through a self-service, multi-function kiosk . . . the user's credit card data is inextricably intertwined with the service itself." The Court granted summary judgment in favor of FedEx. It denied Continental's motion for judgment on the pleadings on FedEx's claim for breach of the implied covenant of good faith and fair dealing. Here, under Fed.R.Civ.P. 12(c) standards, it took the allegations of the complaint as true.

New Jersey Court Finds No Coverage for a Social Engineering Loss under a Professional Liability Policy

Authentic Title Services, Inc. v. Greenwich Ins. Co., **2020 WL 6739880** (D.N.J. Nov. 17, 2020) (marked "Not for Publication)". Authentic is an agent for title insurance companies. It received a series of fraudulent emails directing the transfer of loan proceeds to a fraudulent account, and made the transfer. Greenwich had issued a Title Professional Liability Errors and Omissions insurance policy, and Authentic sought coverage. Applying New Jersey law, the Court ruled in favor of Greenwich, enforcing an exclusion for damages arising out of "a commingling, improper use, theft, stealing, embezzlement or misappropriation of funds or accounts[.]" It found that the plain and ordinary meaning of the exclusion supported denial of coverage. The Court stressed that under the provision, the exclusion does not depend on whether the insured or another party committed the theft or other prohibited act. It rejected Authentic's attempt to import language from another exclusion, for alleged criminal, intentionally wrongful, fraudulent, or malicious acts or omissions, which exempts insureds who did not acquiesce or participate in such act, error, or omission.

Crime Policies

Various Deceptive Funds Transfer Cases under Crime Policies

Midlothian Enterprises, Inc. v. Owners Insurance Co., 439 F.Supp. 3d 737 (E.D. Va. Feb. 20, 2020). A fraudster claiming to be the president of Midlothian sent an email directing an employee to transfer funds to one of the fraudster's accounts. Owners issued a Crime Policy that had a Money and Securities Endorsement, which contained a Voluntary Parting Exclusion. Under the Exclusion, the policy does not cover "[l]oss resulting from [Midlothian's], or anyone acting on [Midlothian's] express or implied authority, being induced by any dishonest act to voluntarily part with title to or possession of any property." Applying Virginia law, the Court found that the plain language of the Voluntary Loss Exclusion unambiguously encompassed the loss. The policy also had a Forgery or Alteration endorsement. Midlothian argued that the fraudulent email constitutes a "covered instrument," defined to include "[c]hecks, drafts, promissory notes or similar written promises, orders or directions to pay a sum certain in 'money.'" The Court rejected this, finding that an email does not have the same form or effect as a check, draft, or promissory note.

Mississippi Silicon Holdings, LLC v. AXIS Ins. Co., 440 F. Supp. 3d 575 (N.D. Miss. Feb. 21, 2020), *appeal docketed*. Mississippi Silicon Holdings (hereafter "MSH") is a manufacturer who purchases electrodes from a Russian supplier. It received emails from someone purporting to be an employee of the supplier directing that bank transfers for payment should be sent to a new bank account. MSH made the transfers, using triple authorization procedures. However, all the authorizations were within MSH. It lost over $1 million. AXIS had issued a Privatus Platinum Insurance Policy which provided, among other grants, coverage for Social Engineering Fraud (sub-limited at $100,000), Computer Transfer Fraud (with a $1 million limit), and Funds Transfer Fraud (also with a $1 million limit). MSH sought coverage under the Computer Transfer Fraud and the Funds Transfer Fraud provisions. AXIS only agreed to coverage under the Social Engineering Fraud provision. Applying Mississippi law, the Court ruled in favor of AXIS. The loss did not result directly from the fraud, as specifically required by the Computer Transfer Fraud provision. Rather, it was MSH's employees, not the fraudulent emails, that initiated the transfer. Also, the provision required that the transfer be made without the knowledge or consent of MSH, circumstances which were obviously not present. Further, the knowledge of MSH's employees of the transfer also rendered the Funds Transfer provision inapplicable. That provision, too, required that the electronic transfer instructions be issued without the insured's knowledge or consent.

RealPage, Inc. v. National Union Fire Ins. Co. et al., 2020 WL 1550798 (N.D. Tex. Apr. 1, 2020). RealPage is a property management software company. An outsider to the company obtained an employee's credentials and accessed third-party software, diverting $10 million in collected payments. National Union issued a Commercial Crime Policy with three relevant insuring agreements: Computer Fraud; Funds Transfer Fraud; and Employee Theft. RealPage brought various claims, including one under the Texas Prompt Payment Claims Act ("TPPCA"). That Act does not apply to fidelity

bonds. National Union argued that its policy fell within the fidelity bond exemption, and moved to dismiss the TPPCA claim only. The Court accepted the traditional definition of fidelity bonds, which apply only to loss "due to embezzlement, larceny, or gross negligence by an employee or other person holding a position of trust." The Court found no such limitations in the Computer Fraud or Funds Transfer Fraud insuring agreements. Rather, the claim arose from the acts of an outsider. Thus, the Court declined to dismiss the TPPA claim.

Authentic Title Services, Inc. v. Greenwich Ins. Co., 2020 WL 6739880 (D.N.J. Nov. 17, 2020) (marked "Not for Publication"). Authentic is an agent for title insurance companies. It received a series of fraudulent emails directing the transfer of loan proceeds to a fraudulent account, and made the transfer. Greenwich had issued a Title Professional Liability Errors and Omissions insurance policy, and Authentic sought coverage. Applying New Jersey law, the Court ruled in favor of Greenwich, enforcing an exclusion for damages arising out of "a commingling, improper use, theft, stealing, embezzlement or misappropriation of funds or accounts[.]" It found that the plain and ordinary meaning of the exclusion supported denial of coverage. The Court stressed that the exclusion does not depend on whether the insured or another party committed the theft or other prohibited act. It rejected Authentic's attempt to import an exception from the language of another exclusion, for alleged criminal, intentionally wrongful, fraudulent, or malicious acts or omissions, which excepts insureds who did not acquiesce or participate in such act, error, or omission.

Ransomware Payments under Crime Policy

G&G Oil Co. of Indiana v. Continental Western Ins. Co., 145 N.E. 3d 842 (Ind. Ct. App. Mar. 31, 2020), *transfer granted, opinion vacated* 157 N.E. 3d 527 (Ind. 2020). An intermediate appellate court in Indiana ruled that there is no coverage under a Crime Policy for bitcoin ransom payments made to a hacker to restore access to computer systems. This case is under active appeal to the Indiana Supreme Court, was argued in December 2020, and the parties are awaiting a decision. That decision will be analyzed in next year's survey.

Significant Non-Coverage Case

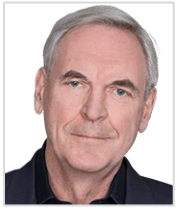
Pennsylvania Federal Court Finds No Duty to Prevent Transmission of NotPetya Virus under Contract, and No "Broader Social Duty"

Heritage Valley Health System, Inc. v. Nuance Communications, Inc., 2020 WL 4700842 (W.D. Pa. Aug. 13, 2020), *appeal docketed*. Heritage Valley is a comprehensive health care provider in Pennsylvania which was infected by the NotPetya virus. NotPetya entered Heritage Valley's computer network systems through a trusted virtual private network connection with Nuance. Nuance provides numerous technologies to the healthcare and other industries. These include medical

documentation transcription services and Dragon Medical, a dictation software used by physicians. (In 2017, Nuance's fact sheet stated that its healthcare solutions were deployed in 86 percent of all US hospitals and more than 500,000 clinicians and 10,000 healthcare facilities worldwide.) Nuance has subsidiaries in many places in the world, including Ukraine (the original target of the NotPetya attacks). Nuance's connection with Heritage Valley comes from Nuance's acquisition of Dictaphone Corporation, which had entered into a 2003 Agreement with Heritage Valley. Although Heritage Valley brought no claim for breach of the Agreement, the Court still considered that the 2003 Agreement's legal impact was central to the pending action. The 2003 Agreement only warrants against viruses from Dictaphone programs for 90 days, places the burden of protecting the network from viruses on Heritage Valley, and Dictaphone was not to provide any maintenance, support, or other assistance for problems necessitated by damage to Dictaphone software from any external source including computer hacks and acts of war. It also had force majeure and limitation of liability clauses.

Heritage Valley sued Nuance, as Dictaphone's parent, for negligence, breach of implied contract, and unjust enrichment. Applying Pennsylvania law, the Court dismissed all claims. First, it applied the "gist of the action doctrine," which precludes plaintiffs from recasting ordinary breach of contract claims into tort claims. The Court found that any duty Nuance owed to Heritage Valley exists only by way of the 2003 Agreement. The Court explicitly rejected the argument that a "broader social duty" existed for Nuance to provide a secure private network connection for the transmission of software. Heritage Valley "has not presented adequate factual averments demonstrating that Nuance breached any social duty beyond the obligations of the [2003 Agreement]." The Court next dismissed the claim for breach of implied contract because Heritage Valley failed to allege any conduct by the parties that would establish an implied contract. Rather, the allegations tend to establish that the parties acted as though the 2003 Agreement had *not* been terminated. Thus, the Court concluded that any duty arises from the 2003 Agreement. Finally, it denied the claim for unjust enrichment because such a claim is inapplicable when the relationship is founded upon a written or express contract. Here, "written contracts govern the disputed issues and frame the duty of care owed and obligations incurred." The Court dismissed the complaint with prejudice, finding that any amendment would be futile.

January 11, 2021



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, including manuscript policies and endorsements. He also assists in all aspects of coverage evaluation and dispute resolution across many lines of business, including cyber, CGL, property, and professional liability. He assists in complex claim evaluations, and if necessary, the defense of insureds in selected matters.