Georgia State University Law Review

Volume 36
Issue 2 *Winter 2019-2020*

Article 5

1-1-2020

Phishing for Computer Fraud Insurance Coverage

Stephen Swanson
Georgia State University College of Law, sswanson12@student.gsu.edu

PHISHING FOR COMPUTER FRAUD INSURANCE COVERAGE

Stephen Swanson*

INTRODUCTION

"Insurance is the only product that both the seller and buyer hope is never actually used."[1] This quotation certainly has merit, but the proliferation of technology in recent decades and the associated risks to sensitive business data are making insurance coverage claims a necessity as cyber threats continue to rise.[2] Cyber threats involve "persons who attempt unauthorized access to a [computer] system device and/or network using a data communications pathway[, and] [t]his access can be directed from within an organization by trusted users or from remote locations by unknown persons using the [i]nternet."[3] Cyber threats originate from many sources,[4] but in the insurance litigation arena, courts across the country are struggling to interpret the proper coverage for monetary business losses pursuant to phishing attacks.[5]

---

* J.D. Candidate, 2020, Georgia State University College of Law. Thank you to my family and friends for your continued support over the past four years. Thank you to Professors Diamond and Bracker for your guidance and feedback during the process of writing this Note. Finally, thank you to my Law Review colleagues for your invaluable diligence in editing and publishing this note.

1. *Life Insurance*, SUMMIT FIN. CONSULTING, http://summitfc.net/services/insurance/life-insurance [https://perma.cc/2JWP-FBYL] (last visited Aug. 15, 2019) (quoting unknown author).

2. J. Clement, *Annual Number of Data Breaches and Exposed Records in the United States from 2005 to 2018 (in Millions)*, STATISTA, https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/W398-CJC5] (last updated Aug. 5, 2019) ("The number of data breaches and the number of exposed records in the U.S. have reached the highest figures to date in 2017 [with] [n]early 179 million records . . . exposed in the U.S. in 2017, whereas the number of data breaches in the country added up to 1,579 that year.").

3. *Cyber Threat Source Descriptions*, U.S. DEP'T OF HOMELAND CISA CYBER + INFRASTRUCTURE, https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions [https://perma.cc/4NMX-S3EH] (last visited Aug. 15, 2019).

4. *Id.* Various threats to computer systems include bot-network operators, criminal groups, foreign intelligence services, hackers, insiders, phishers, spammers, spyware/malware authors, and terrorists. *Id.*

5. J. Robert MacAneney et al., *2 Circuit Court Rulings Rock Phishing Loss Coverage Field*, LAW 360 (July 26, 2018, 3:10 PM), https://www.law360.com/articles/1067338/2-circuit-court-rulings-rock-phishing-loss-coverage-field [https://perma.cc/NP4D-C5R3] ("[Recent] decisions create a bona fide circuit split on the issue of whether a 'phishing' . . . scheme comes within the computer fraud coverage part of a crime/fidelity policy.").

Generally, phishing entails "attempt[s] by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques [that] are crafted to appear as if they have been sent from a legitimate organization or known individual."[6] Phishing attacks proceed quickly with minimal exposure to the cybercriminal.[7] For example, France-based Etna Industrie was targeted when the company president contacted its accountant regarding a "very confidential" acquisition of a company in Cyprus.[8] The president instructed that a lawyer supporting the transaction would make contact with details of where to wire the funds for the purchase.[9] Within one hour, and after about ten urgent emails and several phone calls, the accountant had wired €500,000 to foreign bank accounts.[10] While the accountant seemingly acted in accordance with the business's needs, the president's communication, the external lawyer, and the confidential transaction were actually all a fraudulent phishing attack aimed at rapidly excising funds from Etna Industrie with little or no paper trail.[11]

Following a successful phishing attack, businesses seek to recoup these losses and turn to their cyber insurance policy or the computer fraud provision of their crime insurance policy.[12] Oftentimes,

---

6. *Report Phishing Sites*, U.S. DEP'T OF HOMELAND SECURITY CISA CYBER + INFRASTRUCTURE, https://www.us-cert.gov/report-phishing [https://perma.cc/CGL2-8J8P] (last visited Aug. 15, 2019). Usually in the form of emails, phishing "often attempt[s] to entice users to click on a link that will take the user to a fraudulent website that appears legitimate [or] to provide personal information, such as account usernames and passwords, that can further expose them to future compromises." *Id. Accord* Thomas J. Smedinghoff, *Phishing: The Legal Challenges for Business*, 24 BANKING & FIN. SERVICES POL'Y REP. 2, 2 (2005) ("Phishing attacks take advantage of customer trust in a company's identity and brand names . . . [and] they do serious damage to the company's reputation, as well as undermine confidence in online commerce generally.").

7. Marie Keyworth & Matthew Wall, *The 'Bogus Boss' Email Scam Costing Firms Millions*, BBC NEWS (Jan. 8, 2016), https://www.bbc.com/news/business-35250678 [https://perma.cc/ZKA4-MMX9].

8. *Id.*

9. *Id.*

10. *Id.*

11. *Id.*

12. *Social Engineering Fraud*, ARTHUR J. GALLAGHER & CO., https://www.wasb.org/wp-content/uploads/2017/04/20161219_ajgallagher_social_engineering_fraud.pdf [https://perma.cc/NR23-99XX] (last visited Aug. 15, 2019) [hereinafter *Social Engineering Fraud*] ("Many insureds assume that theft of funds through social engineering fraud would be covered under a cyber liability policy or a crime insurance policy's computer/funds transfer fraud extension; however, insurers have generally denied coverage under both policies.").

however, the insurer denies coverage under latter provisions, and litigation ensues.[13] Courts faced with this insurance coverage issue are split on whether phishing attacks result in a direct loss of money that should be covered under a computer fraud provision of a crime insurance policy.[14] The Fifth and Ninth Circuits side with the insurers in denying coverage under similar computer fraud provisions.[15] The Second and Sixth Circuits have found direct losses and sustain coverage in favor of the insureds, whereas the Eleventh Circuit is divided.[16]

Accordingly, the following note discusses the disparity between the federal circuit courts regarding the proper insurance coverage for phishing-type attacks. Part I examines the cyber threats companies face when handling sensitive transactions and customer data, as well as the coverage gap between traditional crime insurance policies and the targeted cyber insurance policies that help prevent, detect, and ultimately mitigate the damages resulting from a cybersecurity breach.[17] Part II analyzes the current circuit split and the various

---

13. Id.

14. MacAneney, *supra* note 5.

15. Id.

16. *Id.*; Interactive Commc'ns Int'l v. Great Am. Ins., 731 F. App'x 929, 935–36 (11th Cir. 2018); Principle Sols. Grp. v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *5 (N.D. Ga. Aug. 30, 2016); Success Healthcare v. Zurich Am. Ins., No. 9:14-81423-CIV, 2015 WL 11439019, at *6 (S.D. Fla. Mar. 20, 2015), *report and recommendation adopted*, No. 9:14-CV-81423, 2015 WL 11438207 (S.D. Fla. Apr. 9, 2015).

17. Daniel Garrie & Michael Mann, *Cyber-Security Insurance: Navigating the Landscape of a Growing Field*, 31 J. MARSHALL J. INFO. TECH. & PRIVACY L. 379, 390–91 (2014) ("The various types of coverage offered under cyber-security insurance policies include coverage for:

- Data breach/privacy crisis management: expenses related to the management of a cyber-security incident, including the investigation, remediation, data subject notification, call management, credit checking for data subjects, legal costs, court attendance and regulatory fines;
- Business/Network Interruption: loss of net profit that was caused by a material interruption to the insured's network, due to a cyber-attack or a network security breach;
- Multimedia/Media liability: third-party damages which can include defacement of a website, infringement of intellectual property rights or negligence relating to electronic content;
- Extortion liability: losses due to a threat of extortion and professional fees related to terminating an external threat;
- Network security liability: third-party damages resulting from denial of access to a system, costs related to data stored with third-party suppliers and costs related to the theft of data on third-party systems;

contract interpretation strategies, policy considerations, and tests employed in reaching a coverage decision. Part III proposes a resolution to the overarching circuit split that will provide more clarity and predictability to victims of phishing attacks and the insurance companies they employ.

I. Background

Scams and schemes are not new phenomena in human history.[18] They have traditionally varied in sophistication,[19] but the rise of cyber threats in recent years is so pervasive that the public likely has already "been hacked" or they just "don't [yet] know [that] they've been hacked."[20] The insurance market responded to these threats in 1997 with its first iteration of cyber insurance policies.[21] Initially covering only third-party liability, insurers soon realized that a significant amount of data breaches originated from within companies, so the policies expanded in kind to include first-party liability coverage to the affected company.[22] Further developments in

- Reputational Injury: third-party damages from disparagement or privacy violations caused by breach of the insured's system;
- Conduit Injury: damages to customers' systems affected by breach of the insured's system;
- Disclosure Injury: damages to individuals caused by the unauthorized access of their private information held on the insured's system.");

Jason Tashea, *Are You Covered*, 104 A.B.A. J. 30, 31 (2018) (discussing the insurance coverage gap between law firm's computer fraud coverage policy and general cyber insurance policies).

18. Linton Weeks, *How Scams Worked in the 1800s*, NAT'L PUB. RADIO (Feb. 12, 2015, 7:03 AM), https://www.npr.org/sections/npr-history-dept/2015/02/12/385310877/how-scams-worked-in-the-1800s [https://perma.cc/ES9W-KQHT] (detailing "the Golden Age of schemes" and the rise of the so-called "confidence man" or "con man").

19. Jean Braucher & Barak Orbach, *Scamming: The Misunderstood Confidence Man*, 27 YALE J.L. & HUMAN. 249, 250 (2015) ("Familiar [con] examples include telemarketing frauds, fraudulent charities, pyramid and Ponzi schemes, work-from-home schemes, quack medicines, home repair scams, and Nigerian scams.").

20. *Barbarians at the Digital Gate*, WALL STREET J. (Feb. 5, 2013, 12:01 AM), https://www.wsj.com/articles/SB10001424127887323701904578275920521747756 [https://perma.cc/5U47-PQB5].

21. Brian D. Brown, *The Ever-Evolving Nature of Cyber Coverage*, INS. J. (Sept. 22, 2014), https://www.insurancejournal.com/magazines/mag-features/2014/09/22/340633.htm [https://perma.cc/6ABU-N7QS].

22. *Id.*

> [T]he original policies covered only third party suits arising from breaches originating from outside the company. However, studies at the time showed that over half of all data breaches originated from inside the company from rogue and disgruntled

the cyber insurance arena seemingly came about in response to evolving cyber threats and businesses looking to be made whole for revenue interruption, digital investigations, and public relations expenses.[23] Still, businesses struggle "to stay ahead of criminals and stop old cat and mouse games" in an age when information security is increasingly vulnerable.[24] Targeted cyber threats, coupled with limited options for business recovery, have created a gap that courts nationwide are grappling to fill.

A. Cyber Threats

The social engineering attack is prominent among the cyber threats facing businesses.[25] This involves "manipulat[ing] . . . a victim's understanding of a transaction . . . so that they unwittingly . . . provide the thief with funds or information."[26] Under the social engineering umbrella, group and spear phishing attacks target businesses with demonstrated success.[27]

> employees. The markets offering coverage at that time responded by broadening coverage to cover loss to the entity, but coverage for loss from the malicious employee was excluded.

Id.

23. Id.

24. COMBATING UNAUTHORIZED REMOTE NETWORK ACCESS AND EMBEDDED MALICIOUS CODE, WARREN GORHAM & LAMONT, 2010 WL 865796.

25. PETER TRIM & DAVID UPTON, COUNTERACTING CYBER THREATS THROUGH ORGANIZATIONAL LEARNING AND TRAINING § 2.2 (2013) (ebook) ("Social Engineering has been defined in numerous ways. The best definition is an enemy who manipulates or uses psychological tricks to gain the confidence of an authorized network employee relying on the natural human tendency to trust and help others. While there may be internal, disgruntled enemies within your organizational system, the external enemy will, more than likely, use social engineering to terrorize your organization. These hackers will rely on the fact that people within your organization are either willing to share private information or are unaware of the value of information they possess and therefore are careless about protecting it.").

26. Scott L. Schmookler & Christopher M. Kahler, *Social Engineering: Is the Manipulation of Humans a Computer Fraud?*, 22 FIDELITY L.J. 1, 7 (2016).

27. CAROLE BASRI & MARY MACK, EDISCOVERY FOR CORPORATE COUNSEL § 30:10, § 30:11 (2018) ("Criminals often send . . . phishing emails by the thousands, which is referred to as group phishing. A phishing email will generally claim that it is a well-known individual or organization (a bank, a credit card company), which the target may or may not have a relationship with, that needs certain access information, such as usernames, passwords, or anything else a criminal may need to gain access to the system they are targeting. If an individual opens a file in the email or clicks on a link, malware may be delivered to the system or the individual may be tricked into divulging system credentials or other important information Unlike group phishing, spear phishing, like its name suggests, is a targeted, individually designed, phishing attempt to gain access, or spread malware, to a specific individual or entity. The goal of a spear phishing attack is frequently to steal intellectual

1. Business Email Compromise

Business Email Compromise (BEC) is a type of spear phishing attack where scammers target businesses that routinely send large sums of money via wire transfer.[28] Between October 2013 and December 2016, the Federal Bureau of Investigation reported BEC losses nearing $1.6 billion.[29] The scam proceeds when a company employee, usually in the accounting or finance department, is contacted by a third-party posing as a high-ranking company executive or trusted external vendor who requests a monetary wire transfer to a new or slightly-different-than-normal bank account.[30] The employee completes the transfer, and the company later discovers that the internal executive or external vendor never requested the transaction.[31] All, or part, of the transferred funds are typically unrecoverable from the third-party scammer, and the company immediately looks to recover those losses.[32]

property, financial data, trade or military secrets, and other confidential data.").

28. Lee Matthews, *Phishing Scams Cost American Businesses Half a Billion Dollars a Year*, FORBES (May 5, 2017, 2:00 PM), https://www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#7b7879703fa1 [https://perma.cc/T28S-9E56].

29. Id.

30. Jan Larson & Raymond Simmons, *Favoring Coverage for Business Email Compromise Losses*, LAW 360 (Aug. 9, 2018, 4:18 PM), https://www.law360.com/articles/1071615/favoring-coverage-for-business-email-compromise-losses [https://perma.cc/V7XK-K52K]. *Accord* Smedinghoff, *supra* note 6, at 2 ("A phishing attack typically involves sending individuals an email request for information that appears to come from a legitimate company, such as a bank, retailer, or other e-commerce Web site (the spoofed company). Through the use of a false 'from' address, copies of company logos, Web links, and graphics, these emails have the look and feel of a message that recipients might expect to receive from a company with whom they do business. Often the message makes reference to new security measures allegedly being undertaken by the spoofed company and asks recipients to verify or reconfirm confidential personal information, such as account numbers, Social Security numbers, passwords, and other sensitive information. To provide a sense of urgency, the message may indicate that the recipient's account will be suspended or cancelled if the information is not verified by a certain date.").

31. Larson & Simmons, *supra* note 30. *See also* Thomas H. Bentz, Jr., *Cyber Insurance and Social Engineering Fraud, Why Voluntary Transfers May Not be Covered by Your Insurance Policies*, 21 CYBERSPACE LAW., no. 2, Feb. 2016, at 1, 1, https://www.hklaw.com/files/Uploads/Documents/Articles/0216_Bentz_CyberSpaceLawyer.pdf [https://perma.cc/JFS5-5GVA].

32. Larson & Simmons, *supra* note 30.

B. Coverage Options

Apart from absorbing the loss, phished companies have limited avenues to recover the fraudulently transferred funds.[33] They may look to the involved parties or even to the bank that facilitated the transfer. If this fails, a claim may be tendered under a relevant business insurance policy.

1. Between Parties

The involved parties may seek to recover the losses as between themselves. In *Bile v. RREMC, LLC*, a $63,000 employment discrimination settlement agreement was erroneously transmitted to a third party posing as the plaintiff's counsel.[34] Unable to retrieve the wire transfer, the payee refused to dismiss the employment discrimination action until the payor initiated a second $63,000 payment.[35] The payor refused as well, and both parties sought resolution in the United States District Court for the Eastern District of Virginia as per the settlement agreement's venue stipulation.[36] Though the court ultimately held that no duplicate payment was due because the plaintiff's counsel failed to warn the opposing parties of a known fraudulent email issue,[37] the court interpreted common law contract principles and Uniform Commercial Code Article 3 provisions to form the rule that "if a person has an obligation to deliver a check, and does not deliver that check due to that person's own error, then that person remains liable on the underlying obligation."[38] Consequently, the risk of loss remains with the payor

33. Larson & Simmons, *supra* note 30 ("The money from the transaction, of course, disappears and is often unrecoverable from the third party that fraudulently induced the transfer.").

34. Bile v. RREMC, LLC, No. 3:15CV051, 2016 WL 4487864, at *1–2 (E.D. Va. Aug. 24, 2016).

35. *Id.* at *2.

36. Id.

37. *Id.* at *5, *11 ("Two days before the fraud was perpetrated on LeClairRyan, both Ubom and Bile were aware that an unidentified third party had targeted the settlement funds for diversion to a Barclay's bank account that had nothing to do with Bile. Additionally, Bile and Ubom knew that ubomlawgroup@yahoo.com was being used in an effort to perpetrate the fraud. Ubom failed to pass this information along to Defendants, defense counsel, or the Court. This failure substantially contributed to the loss of $63,000.00 within the meaning of U.C.C. § 3-406.").

38. *Id.* at *10.

in the context of hacked settlement agreements. The payor is also unable to recover lost funds from the bank involved in a fraudulent transfer.

2. Financial Institutions

The Uniform Commercial Code generally allocates the risk of loss to banks that honored requests for fraudulent wire transfers.[39] Yet, banks oftentimes are not bound to reinstate lost funds when the "bank and its customer agree to implement a security procedure designed to protect themselves against fraud."[40] The risk of loss will shift to the customer, that is, the party whose funds were fraudulently transferred, when "the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and the bank proves that it accepted the payment order in good faith and in compliance with the security procedure."[41] With yet another recovery mechanism closed, companies look to their individual insurance policies for repayment of the lost funds.

3. Cyber Insurance and Crime Insurance Policies

One source of insurance coverage may be a cyber risk policy, though many U.S. businesses have not yet subscribed.[42] For those that have, a typical cyber insurance policy may not cover "losses . . . where companies have funds, data, or intellectual property stolen by computer hackers."[43] Instead, cyber policies tend

39. Banco Del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302, 304 (S.D.N.Y. 2016).

40. Choice Escrow & Land Title, LLC v. BancorpSouth Bank, 754 F.3d 611, 617 (8th Cir. 2014).

41. U.C.C. § 4A-202(b) (AM. LAW INST. & UNIF. LAW COMM'N 2018); s*ee also Choice*, 754 F.3d at 617, 622–23 (noting that BancorpSouth Bank was not required to replenish $440,000 in lost funds because it maintained commercially reasonable "security procedures . . . [such as] password protection, daily transfer limits, device authentication, and dual control" and "accepted and executed the . . . payment order in a way that comported with [the customer's] reasonable expectations, as established by reasonable commercial standards of fair dealing.").

42. *Why 27% of U.S. Firms Have No Plans to Buy Cyber Insurance*, INS. J. (May 31, 2017), https://www.insurancejournal.com/news/national/2017/05/31/452647.htm [https://perma.cc/DE86-LJ5B] (detailing that, despite an expected increase of cyber breaches in the next year, 50-55% of U.S. firms do not have cyber risk insurance due in part to lack of clarity regarding cost and coverage).

43. Joseph S. Harrington, *Cyber Losses Testing Insurance Policy Boundaries*, INS. J. (Apr. 13, 2017), https://www.insurancejournal.com/news/national/2017/04/13/447758.htm

to focus on "provid[ing] . . . [consulting] resources to mitigate cyber-fraud [sic]."[44] Without a cyber policy specifically covering losses from computer or funds transfer fraud, phished companies must tender a claim under a more traditional insurance policy.[45] Though a crime insurance policy may seem like a logical source of coverage after a phishing attack, the prevailing case law demonstrates that courts differ on the interpretation of such provisions.[46]

II. Analysis

Federal circuit courts nationwide interpret crime insurance policies differently.[47] The Fifth and Ninth Circuits align with traditional contract interpretation strategies or policy considerations to deny the insured's claim for coverage.[48] The Second and Sixth Circuits focus on the technical accomplishment of a phishing attack and apply that process to the policy language in question, and ultimately in favor of the insured.[49] The Eleventh Circuit bases its rulings on the principles

---

[https://perma.cc/38SM-BAK5].

44. *Id.*; s*ee also* Garrie & Mann, *supra* note 17.

45. *CyberRisk*, TRAVELERS INDEMNITY CO. (2014), https://www.travelers.com/energy-practice/iw-documents/CyberRiskBond-59784.pdf [https://perma.cc/3Y3Z-TWNB]; *see also* Harrington, *supra* note 43.

46. *See Social Engineering Fraud*, *supra* note 12. Though it varies depending on the insurer, a typical computer fraud provision of a crime insurance policy will pay the insured for the following:

> the [i]nsured's direct loss of, or direct loss from damage to, [m]oney, [s]ecurities, and [o]ther [p]roperty directly caused by . . . [t]he use of any computer to fraudulently cause a transfer of [m]oney, [s]ecurities, or [o]ther [p]roperty from . . . inside the [p]remises . . . to a person . . . outside the [p]remises . . . or to a place outside the [p]remises.

Posco Daewoo Am. Corp. v. Allnex USA, Inc., No. CV 17-483, 2017 WL 4922014, at *2 (D.N.J. Oct. 31, 2017); *see also* BEAZLEY, *Crime Insurance Policy* 3, https://www.beazley.com/documents/Management%20Liability/Crime/Crime%20Policy.pdf [https://perma.cc/LKD5-XXZE] ("'Computer Fraud' means the Theft of Money, Securities or Merchandise by a Third Party, through the use of any Computer System."); *Social Engineering Fraud*, *supra* note 12 ("Under [a crime policy], the insurer pays the insured for a direct loss of money sustained by the insured resulting from computer fraud committed by a third party.").

47. MacAneney, *supra* note 5.

48. Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 259 (5th Cir. 2016); *see also* Taylor & Lieberman v. Fed. Ins. Co., No. CV 14-3608 RSWL (SHx), 2015 WL 3824130, at *4 (C.D. Cal. June 18, 2015), *aff'd*, 681 F. App'x 627 (9th Cir. 2017).

49. Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 119 (2d Cir. 2018).

of direct causation, but even these decisions are inconsistent.[50] A review of the federal circuit split is illustrative.

A. Phishing Attacks Are Not Covered

The Ninth and Fifth Circuits do not find coverage for phishing attacks under a computer fraud provision of a crime insurance policy.[51] Both employ varying interpretative techniques to reach this result.[52] The Ninth Circuit clings to traditional insurance policy guidelines, whereas the Fifth Circuit views insured responsibility as a principle policy consideration.[53] Despite their diverse analysis, the insurer prevails in either circuit.[54]

1. Canons of Construction

In the Ninth Circuit, regardless of the claimed coverage provision, fraudulent wire transfers do not constitute a direct loss by the insured.[55] In *Taylor & Lieberman v. Federal Insurance Co.*, the plaintiff, an accounting firm, held power of attorney to make monetary wire transfers out of their client's bank account.[56] The client sent three seemingly legitimate emails to the plaintiff requesting over $320,000 in wire payments to bank accounts in

---

50. Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465 (6th Cir. 2018); Interactive Commc'ns Int'l v. Great Am. Ins., 731 F. App'x 929, 935–36 (11th Cir. 2018); Success Healthcare v. Zurich Am. Ins., No. 9:14-81423-CIV, 2015 WL 11439019, at *6 (S.D. Fla. Mar. 20, 2015).

51. *Apache*, 662 F. App'x at 259; *Taylor & Lieberman*, 2015 WL 3824130, at *4.

52. *Apache*, 662 F. App'x at 255; *Taylor & Lieberman*, 2015 WL 3824130, at *3.

53. *Apache*, 662 F. App'x at 259; *Taylor & Lieberman*, 2015 WL 3824130, at *4.

54. *Apache*, 662 F. App'x at 259; *Taylor & Lieberman*, 2015 WL 3824130, at *4.

55. *Taylor & Lieberman*, 2015 WL 3824130, at *3. The court bullet pointed the three provisions under which plaintiff Taylor & Lieberman, an accounting firm, sought coverage:

- Forgery Coverage: "The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Forgery or alteration of a Financial Instrument committed by a Third Party."
- Computer Fraud Coverage: "The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Computer Fraud committed by a Third Party."
- Funds Transfer Fraud Coverage: "The Company shall pay the Parent Corporation for direct loss sustained by an Insured resulting from Funds Transfer Fraud committed by a Third Party."

Id. (citations omitted).

56. *Id.* at *1.

Malaysia and Singapore.[57] Following the discovery of the scam, the client's bank recovered roughly only $93,000, leaving around $100,000 of the client's funds lost to the BEC phishing scheme.[58] The client requested and received repayment of the lost funds, and Taylor & Lieberman sought indemnification of this loss under its crime insurance policy.[59]

Both the district court and court of appeals employed various canons of construction to deny plaintiff's claim of coverage.[60] The district court relied on existing strategies of coverage interpretation and classified Taylor & Lieberman's policy as an "indemnity polic[y] that [does] not provide third-party coverage . . . [so] [p]laintiff ha[d] not suffered a 'direct loss.'" [61] Because the third-party liability sections were "expressly delineated" and "separated in an entirely different document," plaintiff's claimed coverage provisions, which made no mention of liability coverage, were construed as indemnity provisions that did not provide for third-party coverage under the canon of *expressio unius est exclusio alterius*.[62]

Further, the court applied the whole-text canon to find that the policy as a whole "more likely contemplate[d] fraudulent violations against [p]laintiff that result[ed] in a 'direct loss' of [p]laintiff's own money—not fraudulent violations upon which [p]laintiff relie[d] that result[ed] in a loss of a [third-party] client's money."[63] This coverage

---

57. *Id.* The fraudster took hold of the client's email account for use in the first two email requests but used a different email address in the third request. *Id.* This final, different request tipped off plaintiff as to the fraud, and the third wire transfer was not completed. *Id.*

58. *Id.* at *2.

59. *Id.* at *2, *4.

60. *See generally* Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017); *Taylor & Lieberman*, 2015 WL 3824130.

61. *Taylor & Lieberman*, 2015 WL 3824130, at *3 ("[M]ost courts . . . have indicated that *liability policies* may require an insurer to discharge an obligation of the insured to a third party for some act of the insured or its employee, while *indemnity policies* may not.").

62. United States v. Vonn, 535 U.S. 55, 65 (2002) (noting the "canon that expressing one item of a commonly associated group or series excludes another left unmentioned"); *Taylor & Lieberman*, 2015 WL 3824130, at *4; *Expressio unius est exclusio alterius*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("A canon of construction . . . express[ing] or includ[ing] one thing implies the exclusion of the other, or of the alternative.").

63. *Taylor & Lieberman*, 2015 WL 3824130, at *4.

> For example, the section of the [p]olicy in question also contains coverage for employee theft, which is similar in nature to the 'employee fidelity' policies that . . . [do not] require an insurer to discharge an obligation of the insured to a third

denial left Taylor & Lieberman unreimbursed under the policy even though it had in good faith repaid the client for the lost funds.[64] Such a result could not only damage the accounting firm's reputation for monetary responsibility but also discourage said firm from distributing repayments to clients ahead of any claim tendered under its insurance policy. This too could damage the accounting firm's relationship with clients; consequently, Taylor & Lieberman appealed in the hopes of a different outcome.[65]

On appeal, the Ninth Circuit found no coverage for Taylor & Lieberman via different canons of construction.[66] The plaintiff contended forgery coverage could apply to non-financial instruments, like emails, based on application of the rule of the last antecedent.[67] Under a "natural reading of the policy," however, coverage logically extended also to forgery of "financial instruments, like checks, drafts, or the like," but not to emails with wire instructions.[68] Likewise, the fraudulent emails neither constituted an unauthorized "entry into" nor "introduction of instructions" to the plaintiff's computer system.[69] Instead, the ordinary-meaning canon was applied to find that such computer fraud language is generally understood to cover only hacking-type attacks, "like the introduction of malicious computer code" to a computer system, as opposed to just "the text of three emails."[70] Whereas the Ninth Circuit favors canons of construction to interpret crime insurance coverage, the Firth Circuit looks to policy considerations in its decisions.

---

party for some act of the insured or its employee.

Id. at *3–4; *Whole-Text Canon*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("The doctrine that a legal text . . . must be construed as a whole.").

64. *Taylor & Lieberman*, 2015 WL 3824130, at *4.

65. *Taylor & Lieberman*, 681 F. App'x at 628.

66. *Id.* at 628–29.

67. *Id.* ("The policy provides coverage for an insured's direct loss 'resulting from [f]orgery or alteration of a [f]inancial [i]nstrument by a [t]hird [p]arty."); *Rule of the Last Antecedent*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("An interpretive principle by which a court determines that qualifying words or phrases modify the words or phrases immediately preceding them and not words or phrases more remote, unless the extension is necessary from the context or the spirit of the entire writing.").

68. *Taylor & Lieberman*, 681 F. App'x at 628.

69. *Id.* at 629.

70. *Id.*; *Ordinary-Meaning Canon*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("The doctrine that words in a legal instrument are to be understood in their ordinary, everyday meanings unless the context indicates that they bear a technical sense or are otherwise defined in the text.").

2. Policy Considerations

The Fifth Circuit interprets computer fraud coverage provisions narrowly.[71] In *Apache Corp. v. Great American Insurance Co.*, a petroleum company's employee received a telephone call from a purported vendor requesting a change to the bank account details for invoice payment.[72] After the vendor's follow-up email with attached instructions on letterhead, as well as the petroleum company's internal approval of the change and verification call to the vendor, millions of dollars were transferred into the new bank account before the petroleum company discovered this was a fraudulent request.[73] In considering Apache's claim for coverage under the computer fraud provision,[74] the court viewed Apache's change-request protocols as "flawed" and stated that the company could have avoided the fraud but for a "fail[ure] to investigate accurately the new, but fraudulent, information provided to it."[75] In this vein, the court declined to find coverage where the insured's due diligence investigation could have uncovered the fraud.[76] To find otherwise would be too far-reaching in "convert[ing] the computer fraud provision to one for general fraud" since "few—if any—fraudulent schemes would not involve some form of computer-facilitated communication," like emails.[77] Despite

71. *See generally* Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252 (5th Cir. 2016).

72. *Id.* at 253.

73. *Id.* at 253–54 ("Apache[, the petroleum company,] received notification [that the vendor] had not received the £4.3 million (approximately $7 million) Apache had transferred to the new (fraudulent) account. After an investigation determined the criminals were likely based in Latvia, Apache recouped a substantial portion of the funds. It contends, however, it suffered a loss, before the $1 million policy deductible, of approximately £1.5 million (approximately $2.4 million).").

74. *Id.* at 254 ("[Great American Insurance Company] will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises . . . to a person (other than a messenger) outside those premises . . . [or] to a place outside those premises.").

75. *Id.* at 258–59 ("Arguably, Apache invited the computer-use at issue . . . [since] [t]he email was sent only after Apache's advising, in reply to the criminals' change-request telephone call, that the request had to be made on Petrofac letterhead. The criminals complied: by attaching to the email (sent using a slightly different domain name) a letter on altered letterhead; and, as stated in the email, by allegedly mailing that letter to Apache. Accordingly, the computer-use was in response to Apache's refusing, during the telephone call, to, for example, transcribe the change-request, which it could have then investigated with its records.").

76. *Id.* at 269.

77. *Apache*, 662 F. App'x at 258; *see also* Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332, 333 (9th Cir. 2016) ("[N]o coverage was afforded under the [c]omputer [f]raud

these policy considerations that are construed against the insured, the Second and Sixth Circuits find coverage in favor of the insured on different grounds.[78]

B. Phishing Attacks Are Covered

The Second and Sixth Circuit Courts break from their sister circuits in finding coverage for the policy holder.[79] In the Second Circuit, traditional interpretive tools are disfavored over a modern examination of the steps to accomplish a phishing attack.[80] Similarly, the Sixth Circuit forgoes a conventional understanding of insurance contract causation in favor of an expansive interpretation.[81] Both views, however, capture the insured's conduct and find coverage under the computer fraud policy.[82]

1. Technical Interpretations

The Second Circuit reads a computer fraud provision quite literally to find coverage for the insured.[83] *Medidata Solutions, Inc. v. Federal Insurance Co.* involved a familiar phishing scheme whereby a Medidata accounts payable employee was contacted by the company president with instructions to wire $4.7 million to an external attorney who was handling a confidential business acquisition.[84] After completing this transfer, a second, suspicious wire request

provision for any transfers to [its payroll provider] that were authorized by Pestmaster . . . [since the policy] require[s] an unauthorized transfer of funds. When [the payroll provider] transferred funds pursuant to authorization from Pestmaster, the transfer was not fraudulently caused. Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this [c]rime [p]olicy into a '[g]eneral [f]raud' [p]olicy. While [the insurer] could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.").

78. *See generally* Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455 (6th Cir. 2018); Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018).

79. *Am. Tooling Ctr.*, 895 F.3d at 465; *Medidata*, 268 F. Supp. 3d at 479.

80. *Medidata*, 268 F. Supp. 3d at 477.

81. *Am. Tooling Ctr.*, 895 F.3d at 463.

82. *Am. Tooling Ctr.*, 895 F.3d at 465; *Medidata*, 268 F. Supp. 3d at 479.

83. *Medidata*, 268 F. Supp. 3d at 477.

84. *Id.* at 473.

came through, and Medidata discovered the fraud scheme.[85] Medidata sought coverage under the computer fraud provision of their crime coverage policy.[86] The district court, and the Second Circuit on appeal, found that Medidata's losses were covered under the policy since the "fraudsters . . . crafted a computer-based attack that manipulated [its] email system," and this constituted an "'entry of data into' [and] 'change to data elements or program logic of' a computer system."[87] Moreover, Medidata also suffered a direct loss within the meaning of the policy since "the [phishing] attack was the proximate cause of [the] losses" and the employees' involvement was not "sufficient to sever the causal relationship between the [phishing] attack and the losses incurred."[88]

Instead of citing to external policy or maxims of interpretation, the court focused on the actual, technical method of intrusion to find coverage.[89] The fraudster manipulated the "true origin of the spoofed emails" by "embedd[ing] a computer code" that caused the electronic computer system components to display different email address senders in the "From" field.[90] Upon receipt, Medidata's email system

85. *Id.* at 473–74.

86. *Id.* at 474. The policy's crime coverage section protected an organization from a direct loss of money resulting from a computer fraud committed by a third party. *Id.* Computer fraud included the "unlawful taking or the fraudulently induced transfer of money" as a result of a computer violation. *Id.* The policy defined a computer violation as both a fraudulent entry of data into a computer system and a "change to data elements or program logic of a computer system." *Medidata*, 268 F. Supp. 3d at 474.

87. Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118 (2d Cir. 2018) ("We agree with the district court that the plain and unambiguous language of the policy covers the losses incurred by Medidata here. While Medidata concedes that no hacking occurred, the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's email system, which the parties do not dispute constitutes a 'computer system' within the meaning of the policy. The spoofing code enabled the fraudsters to send messages that inaccurately appeared, in all respects, to come from a high-ranking member of Medidata's organization. Thus the attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system. The attack also made a change to a data element, as the email system's appearance was altered by the spoofing code to misleadingly indicate the sender. Accordingly, Medidata's losses were covered by the terms of the computer fraud provision.").

88. *Id.* at 119.

89. *Medidata*, 268 F. Supp. 3d at 477.

90. *Id.* ("[T]he thief constructed messages in Internet Message Format ('IMF') which the parties compare to a physical letter containing a return address. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ('SMTP'). Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. To mask the true origin of the spoofed emails, the thief embedded a computer code. The computer code caused the SMTP Envelope

interpreted the spoofed message as from the company president rather than the hacker.[91] In this way, the court saw the fraudulent scheme as a change to a data element, since the email system displayed the incorrect sender because of the computer code, and as an entry of data element in a computer system because the malicious computer code was embedded therein.[92] According to the Second Circuit, both phases of the phishing scheme fit squarely within the policy's provisions of coverage for the insured.[93] The Sixth Circuit similarly comes down in favor of the insured.[94]

2. Principles of Causation

The Sixth Circuit employs a causation analysis when interpreting computer fraud coverage.[95] In *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America*, a tool and die manufacturer that outsourced some of its orders to a Chinese company mistakenly sent an imposter approximately $834,000 in vendor payments via wire transfer.[96] American Tooling claimed the losses under its computer fraud policy, but Travelers (their insurance agency) denied the claim.[97] The Sixth Circuit Court of Appeals

---

and the IMF Letter to display different email addresses in the 'From' field. The spoofed emails showed the thief's true email address in the SMTP 'From' field, and Medidata's president's email address in the IMF 'From' field. When Gmail received the spoof emails, the system compared the address in the IMF 'From' field with a list of contacts and populated Medidata's president's name and picture. The recipients of the Gmail messages only saw the information in the IMF 'From' field.") (citations omitted).

91. *Id.*

92. *Medidata*, 729 F. App'x at 118.

93. *Id.*

94. Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 465 (6th Cir. 2018).

95. *Id.* at 460.

96. *Id.* at 457–58. ("Gizinski[, American Tooling's President and Treasurer,] emailed YiFeng employee Jessie Chen requesting that Chen provide ATC all outstanding invoices. An unidentified third party, through means unknown, intercepted this email. This third party, impersonating Chen, then began a correspondence with Gizinski about the outstanding invoices. On March 27, 2015, the impersonator emailed Gizinski and claimed that, due to an audit, ATC should wire its payments to a different account from usual. YiFeng had previously (and legitimately) informed ATC it had changed its banking details, and ATC had no process for verifying the changed information. Consequently, Gizinski wired the money to the new account.") (citations omitted).

97. *Id.* at 458–59 ("The [p]olicy states . . . [that] [t]he [c]ompany will pay the [i]nsured for the [i]nsured's direct loss of, or direct loss from damage to . . . [m]oney . . . directly caused by [c]omputer [f]raud.").

reversed the lower court and found coverage for American Tooling based on principles of causation.[98] The court focused on the timing of the loss, and found "no intervening event" occurred between the transfer to the fraudster and the point at which the funds were lost.[99] Thus, American Tooling suffered a "direct loss" as caused by the fraudster.[100]

Equally, the scheme constituted a "computer fraud" within the meaning of the policy.[101] The policy only required that a computer be used on the one hand, and a fraudulent money transfer be caused on the other.[102] Contrary to Travelers' suggestion, a computer fraud was not limited only to scenarios where the phishing scheme fraudulently caused a computer to make the transfer, such as in a more traditional hack where "a nefarious party somehow gains access to and/or controls the insured's computer."[103] Travelers had not expressly limited computer fraud coverage to such hacking situations in their terms of coverage, so the court was not going to read such a

98. *Id.* at 462–63, 465; *see* 11 CORBIN ON CONTRACTS § 55.7, Westlaw (database updated 2018) ("One of the rules most commonly laid down is that damages are not recoverable for injury that is too remote from the conduct of the defendant constituting his breach of duty. Another form of the rule is that damages are not recoverable for losses suffered or gains prevented unless the requirements of the law as to "proximate" causation are satisfied. The form of this rule is the same whether it is being applied in the field of contracts or in the field of torts, and in both alike, its meaning and its application are equally indefinite and uncertain.").

99. *Am. Tooling Ctr.*, 895 F.3d at 460.

100. *Id.* at 459–61. Notably, the court found unpersuasive the suggestion that the loss was only incurred later in time when the fraud was discovered, not at the moment of payment to the imposter, because American Tooling "had already contracted with YiFeng to pay that amount of money for the product it had received " *Id.* "This interpretation defies common sense" when viewed against a "simplified analogy:"

> Imagine Alex owes Blair five dollars. Alex reaches into her purse and pulls out a five-dollar bill. As she is about to hand Blair the money, Casey runs by and snatches the bill from Alex's fingers. Travelers' theory would have us say that Casey caused no direct loss to Alex because Alex owed that money to Blair and was preparing to hand him the five-dollar bill.

Id.

101. *Id.* at 461 ("The [p]olicy specifically defines the term . . . [c]omputer [f]raud [to mean] [t]he use of any computer to fraudulently cause a transfer of [m]oney . . . from inside the . . . [f]inancial [i]nstitution [p]remises . . . to a person . . . outside the [f]inancial [i]nstitution [p]remises . . . [or] to a place outside the . . . [f]inancial [i]nstitution [p]remises.").

102. Id.

103. *Am. Tooling Ctr.*, 895 F.3d at 461–62.

restriction into the policy; thus, the door was left open concerning coverage of BECs.[104]

It is not enough, however, for there to be a direct loss and a computer fraud. The company must also demonstrate, as per the policy language, that "its 'direct loss' was 'directly caused by' the computer fraud."[105] The Sixth Circuit, borrowing a test from the Eleventh Circuit, deemed the computer fraud to have directly caused the direct loss when the loss was incurred immediately after wiring the funds to the impersonator pursuant to the fraudulent email.[106] Interestingly, the company's "internal actions" were not found to break the causal chain between the fraudulent emails and the loss, suggesting that, in the Sixth Circuit at least, external steps taken by the company between the fraudulent act and the loss incurred could produce contrary results.[107]

C. The Eleventh Circuit's View

The Eleventh Circuit has also opined on the issue with mixed results. On the one hand, it employs the same causation test as the Sixth Circuit, but comes to a different result that favors the insurer.[108] On the other hand, the Eleventh Circuit also adopts a cause-in-fact

104. *Id.* at 462 ("If Travelers had wished to limit the definition of computer fraud to such criminal behavior it could have done so. *Cf. Citizens Ins. v. Pro-Seal Serv. Grp.*, 730 N.W.2d 682, 686 (2007) (holding that a contract is construed in favor of the insured if there is an ambiguity). Because Travelers did not do so, the third party's fraudulent scheme in this case constitutes 'Computer Fraud' per the Policy's definition.").

105. *Id.* at 462.

106. *Id.* at 463 ("[American Tooling] received the fraudulent email at step one. [Its] employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was 'the point of no return,' because the loss occurred once [American Tooling] transferred the money in response to the fraudulent emails. Thus, the computer fraud 'directly caused' [American Tooling's] 'direct loss.'").

107. *Id.* at 462 ("The chain of events that was precipitated by the fraudulent emails and led to the wire transfers involved multiple *internal* actions at [American Tooling]. After receiving each fraudulent email, [American Tooling] verified that YiFeng had completed the tasks required for the next scheduled payment. Gizinski subsequently determined which outstanding invoices to pay, and chose to pay the YiFeng invoice. He then signed into the banking portal and manually entered the fraudulent banking information emailed by the impersonator. Finally, after Gizinski submitted the wire transfer, [American Tooling's] Assistant Comptroller approved the payment. [American Tooling] thus suffered its loss immediately after the transfer, which marked the end of the 'Computer Fraud' as defined in the policy.") (emphasis added) (citations omitted).

108. Interactive Commc'ns Int'l v. Great Am. Ins., 731 F. App'x 929, 936 (11th Cir. 2018).

approach that aligns with the insured's claim for coverage.[109] This intra-circuit split further highlights the divide amongst the courts.

1. The Point of No Return Test

As in the Sixth Circuit, the Eleventh Circuit decides phishing attack coverage disputes based on principles of causation in light of the link between the fraud and the loss.[110] This link proved too remote in *Interactive Communications International, Inc. v. Great American Insurance Co.* where a chit retailer was defrauded out of $11.4 million after thieves found a way to redeem a single chit multiple times.[111] The insured, Interactive Communications, held a standard computer fraud policy with Great American Insurance,[112] but the court adopted a plain meaning of the word "directly"[113] to find that the loss came only after the "fraudsters . . . set into motion [a] chain of events."[114] Unfortunately for Interactive Communications, the fraudsters' chit manipulation occurred at "Step

109. *Id.* at 933–36; *But-For Cause*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("The cause without which the event could not have occurred.").

110. *Interactive*, 731 F. App'x at 935–36; Principle Sols. Grp. v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *4, *5 (N.D. Ga. Aug. 30, 2016).

111. *Interactive*, 731 F. App'x at 930–32; *see also* Joshua Davey & Kevin Denny, *Federal Court: Computer Fraud Provision Does Not Cover Fraudulent Debit Card Transactions Conducted Over the Telephone*, MCGUIREWOODS INS. RECOVERY BLOG (Apr. 12, 2017), https://www.insurancerecoveryblog.com/2017/04/federal-court-computer-fraud-provision-does-not-cover-fraudulent-debit-card-transactions-conducted-over-the-telephone/ [https://perma.cc/LF5Q-BYQ7] ("The insured, InComm Holdings, processes debit cards that allow consumers to purchase credits, called 'chits,' from retailers, which can then be redeemed for actual dollars that are loaded onto prepaid debit cards to make everyday purchases. InComm's redemption program works as follows: Third-party banks issue prepaid debit cards to consumers. Consumers buy 'chits' from retailers like CVS or Walgreens for the value of the chit plus a service fee. Each chit represents the amount purchased, i.e., a $100 chit represents $100. The retailer then wires the consumer's funds to InComm. To convert chits to actual dollars on the debit cards, a consumer calls InComm and uses voice or touchtone commands to 'redeem' the chits. After a chit is redeemed, InComm wires the amount of the chit to the bank that issued the debit card, and the funds become available for the consumer's use.").

112. *Interactive*, 731 F. App'x at 931 ("[T]he policy provides coverage for 'loss of, and loss from damage to, money, securities and other property *resulting directly* from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises.'") (emphasis added).

113. *Id.* at 934 ("In accordance with the term's ordinary meaning, we hold that . . . one thing results 'directly' from another if it follows straightaway, immediately, and without any intervention or interruption.").

114. Id.

1," but the funds were not lost until "Step 4," and, as such, the "use of . . . computers did not . . . immediately . . . cause [the] loss."[115]

The Eleventh Circuit formulated a "point of no return" test whereby, for computer fraud policy purposes, a loss occurs at the point in time when the insured loses control over the funds.[116] If this dominion is lost immediately following that fraudulent act, such as the use of a computer, the loss will "result [ ] directly" from the fraudulent activity.[117] Otherwise, where there are intervening "steps, acts, [or] actors," the loss is too remote from the fraud to be covered under a standard computer fraud policy.[118] Accordingly, the court uses a strict causation standard where virtually any intervening steps between the fraud and the loss, irrespective of their impetus or who performs the step, will break the causal chain such that the insured may not recover under the policy.[119] Another decision within this circuit, however, relaxes this causation standard.[120]

2. But for Causation Test

The Eleventh Circuit has also interpreted a computer fraud policy using a "'but for' test."[121] *Success Healthcare, LLC v. Zurich American Insurance Co.* involved a payroll director who obtained Success's electronic signature to fraudulently wire more than $10 million away from the company.[122] Zurich American denied coverage under the policy[123] citing, in pertinent part, that the "theft was not 'directly related to' the use of a computer."[124] Success sued

---

115. Id.

116. *Id.* at 935 ("InComm retained at least some control over the funds . . . even after [Step 2] . . . and could prevent their loss by intervening to halt the disbursement of money.....").

117. Id.

118. *Interactive*, 731 F. App'x at 935.

119. Id.

120. *See generally* Success Healthcare v. Zurich Am. Ins., No. 9:14 81423-CIV, 2015 WL 11439019 (S.D. Fla. Mar. 20, 2015), *aff'd in part, rev'd in part*, 2015 WL 11438207 (S.D. Fla. Apr. 9, 2015).

121. *Id.* at *6.

122. *Id.* at *1.

123. *Id.* at *5 ("[T]he [p]olicy provides coverage for.....'[c]omputer [f]raud,' which is defined in relevant part to be 'theft of property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside.....the 'premises' or 'banking premises' to a person..... outside those 'premises' or to a place outside those 'premises.'") (citation omitted).

124. *Id.* at *6.

for breach of contract, and the court resolved this issue by invoking a rudimentary but for test for causation—but for the payroll director's use of a computer, the fraud would not have occurred.[125] This formulation was sufficient to survive a motion to dismiss,[126] but it unfortunately brought no interpretive uniformity to the computer fraud coverage arena. The following proposal suggests a remedy in this regard.

III. Proposal

A common theme among the prevailing case law is the insurer's initial denial of coverage under the computer fraud provision of the crime insurance policy.[127] This clash is seemingly ingrained into the professional relationship as insurance companies seek to keep down their bottom line by limiting claim payments and, in contrast, the insured looks to avoid the risk that the insured believes the policy was meant to protect against in the first place.[128] An ideal proposal to bridge this coverage gap is for insurers, in recognition of BEC prevalence, to uniformly spell out the types of coverages that are and are not envisioned by the policy.[129] This ensures that both parties have a meeting of the minds regarding the contractual coverages of the policy. This solution may avoid coverage disputes for future policy holders, but it does not address the inevitable disagreements between current policy holders and the coverages available under

---

125. Id.

126. *Success Healthcare*, 2015 WL 11439019, at *7.

127. Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 458 (6th Cir. 2018); Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118 (2d Cir. 2018); Interactive Commc'ns Int'l v. Great Am. Ins., 731 F. App'x 929, 932 (11th Cir. 2018); Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627, 627 (9th Cir. 2017); Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 254 (5th Cir. 2016); *Success*, 2015 WL 11439019, at *1.

128. Duncan Minty, *Ethics and Insurance Claims—Part 3—Addressing Conflicts of Interest*, ETHICS AND INS. (June 18, 2013), https://ethicsandinsurance.info/2013/06/18/ethics-claims-3-conflicts-of-interest/ [https://perma.cc/CD5F-JH8G]; *What to Do if Your Business Insurance Claim is Denied*, FINDLAW, https://smallbusiness.findlaw.com/liability-and-insurance/what-to-do-if-your-business-insurance-claim-is-denied.html [https://perma.cc/TA36-EXFW] (last visited Sept. 17, 2019).

129. Bill Wilson, *Resolving Insurance Coverage and Claim Disputes*, PROPERTYCASUALTY360 (Aug. 14, 2018, 12:00 AM), https://www.propertycasualty360.com/2018/08/14/resolving-insurance-coverage-and-claim-disputes/ [https://perma.cc/Z8PQ-5EQR] ("[T]he best way to [avoid a] dispute [is] to have addressed the issue at policy inception.").

existing, standard computer fraud provision language. This resolution will be dependent on uniformity in judicial interpretation so that insureds can predict coverage gaps and acquire additional protection as required. Similarly, insurers can update their policy language and offerings in line with this uniform interpretation so that fewer claims and coverage disputes arise. While the facts of each claim vary, insurance disputes over phishing attacks are best adjudicated using a hybrid scheme that incorporates the Fifth Circuit's theory of accountability with the Sixth and Eleventh Circuit's temporal causation analysis.

A. Accountability

Accountability as a judicial consideration can influence the insurer and insured alike. For the policy holder, the knowledge that the measures taken to detect and mitigate a phishing attack will be considered in a coverage dispute may induce the insured to increase security measures ahead of any potential attack. Indeed, cyber security experts call for this type of preparedness irrespective of any insurance policy language.[130] Partnering sound cyber security

130. Joanna Belbey, *How to Avoid Cyber Attacks: 5 Best Practices From SEC and FINRA*, FORBES (June 30, 2017, 1:20 PM), https://www.forbes.com/sites/joannabelbey/2017/06/30/how-to-avoid-cyberattacks-5-best-practices-from-sec-and-finra/#3bbb09021a16 [https://perma.cc/KD2T-RC9S] (noting that governance, risk assessment, cybersecurity training, access management, and vendor management are among the best ways to educate about and defend against cyber risks); *Business Email Compromise: The 3.1 Billion Dollar Scam*, FED. BUREAU OF INVESTIGATION (June 14, 2016), https://www.ic3.gov/media/2016/160614.aspx [https://perma.cc/922X-5DJE] ("Businesses with an increased awareness and understanding of the BEC scam are more likely to recognize when they have been targeted by BEC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments. Businesses that deploy robust internal prevention techniques at all levels (especially targeting front line employees who may be the recipients of initial phishing attempts), have proven highly successful in recognizing and deflecting BEC attempts. Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time, to verify the legitimacy of the request Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts. Be careful what is posted to social media and company websites, especially job duties/descriptions, hierarchal information, and out of office details. Be suspicious of requests for secrecy or pressure to take action quickly. Consider additional IT and financial security procedures, including the implementation of a 2-step verification process . . . . Significant Changes: Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner . . . . Verify changes in vendor payment location by adding additional

prevention with judicial notice of those procedures can result in fewer successful phishing attacks against the insured and, if a coverage dispute does arise, can ensure that the policy holder is not abusing the computer fraud protection by seeking "shelter" as a "provision . . . for general fraud."[131] Similarly, insurance companies would see benefits when courts favor responsible cyber security protocols.

Risk management is central to the insurance industry.[132] Insurers measure various factors in determining the premium to charge a policy holder or whether to offer any coverage at all.[133] In the cyber policy arena, insurers typically require that potential insureds produce a security assessment of their cyber defenses.[134] With the relevant factors in mind, insurers determine individual or business premiums based on "how much cost will be involved in paying

---

two-factor authentication such as having a secondary sign-off by company personnel. Confirm requests for transfers of funds. When using phone verification as part of the two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request. Know the habits of your customers, including the details of, reasons behind, and amount of payments. Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary."); *Security 101: Business Email Compromise (BEC) Schemes*, TREND MICRO (Jan. 11, 2016), https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/business-email-compromise-bec-schemes [https://perma.cc/X9Y4-BEKS] ("Businesses are advised to stay vigilant and educate employees on how to prevent being victimized by [BEC] scams and . . . here are some tips on how to stay protected and secure: Carefully scrutinize all emails. Be wary of irregular emails that are sent from C-suite executives, as they are used to trick employees into acting with urgency. Review emails that request transfer of funds to determine if the requests are irregular[; e]ducate and train employees. While employees are a company's biggest asset, they're also usually its weakest link when it comes to security. Commit to training employees according to the company's best practices. Remind them that adhering to company policies is one thing, but developing good security habits is another[; v]erify any changes in vendor payment location by using a secondary sign-off by company personnel[; s]tay updated on your customers' habits including the details, and reasons behind payments[; c]onfirm requests for transfer of funds when using phone verification as part of two-factor authentication, use known familiar numbers, not the details provided in the email requests.").

131. *Apache*, 662 F. App'x at 258–59.

132. Paul Kaye, *Risk Measurement in Insurance*, CASUALTY ACTUARIAL SOC'Y (2005), https://www.casact.org/pubs/dpp/dpp05/05dpp1.pdf [https://perma.cc/Q2UP-ATWS].

133. Michelle Boardman, *Risk Data in Insurance Interpretation*, 16 CONN. INS. L.J. 157, 162–63 (2009); Mila Araujo, *What Is an Insurance Premium (and How Does It Work)?*, BALANCE (July 9, 2018), https://www.thebalance.com/understanding-what-is-an-insurance-premium-4155239 [https://perma.cc/Z3R4-L3DS]. The type and amount of coverage sought determines the premium. *Id.* Likewise, personal information "from credit rating to car accident frequency or personal claims history and even occupation" play a role in premium pricing. *Id.*

134. Mark Lanterman, *Managing Cyber Risk: Is Cyber Liability Insurance Important for Law Firms?*, 75 BENCH & B. MINN. 13, 14 (2018).

claims as well as how much money the insurance company should collect in order to make sure that they make enough money to pay potential claims."[135] Judicial emphasis on cyber accountability would then incentivize "cultures of security," resulting in less claims under the policy.[136] Over time, fewer BEC claims would lessen the risk and cost to insure, resulting in a net benefit to all stakeholders.[137] This principle, coupled with a court's temporal causation standard, would yield the best outcome in computer fraud coverage disputes.

B. Temporal Causation

Unsurprisingly, when coverage disputes arise, the insured will seek an expansive definition of "direct loss," where a sequence of events does not break the chain of causation between the claimed loss and the computer fraud, and the insured will insist upon an unbroken link between the loss and fraud.[138] While the Sixth and Eleventh Circuits apply the latter interpretation to computer fraud provisions,[139] a majority of jurisdictions see "direct [as] direct" in similar policy language that provides coverage against employee theft.[140] Regardless of the type of covered loss, insurance policies routinely include language such as "direct loss" or "loss resulting

135. Araujo, *supra* note 133.

136. Lanterman, *supra* note 134.

137. Chubb Launches Online Cyber Risk Index, INS. J. (Apr. 12, 2018), https://www.insurancejournal.com/news/national/2018/04/12/486335.htm [https://perma.cc/NY5E-JATP]. Global insurance provider Chubb subscribes to this culture of cyber threat prevention by "offer[ing] businesses throughout North America [an online index that] provide[s] insight into real threats facing them on a daily basis." *Id.* Chubb understands that "[t]he first step to protecting a business from a cyber attack is staying aware of what threats are most prominent to a company's size and industry [and] . . . help[ing] users to better understand their exposures and manage risk before a cyber incident occurs." *Id.*

138. Principle Sols. Grp. v. Ironshore Indem., Inc., No. 1:15-CV-4130-RWS, 2016 WL 4618761, at *5 (N.D. Ga. Aug. 30, 2016) ("It is reasonable for [the insured] to interpret the language of the policy to provide coverage even if there were intervening events between the fraud and the loss. [The insurer's] interpretation, which would require an immediate link between the injury and its cause, is also reasonable.").

139. Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 463 (6th Cir. 2018); Interactive Commc'ns Int'l v. Great Am. Ins. Co., 731 F. App'x 929, 934 (11th Cir. 2018).

140. Tooling, Mfg. & Techs. Ass'n v. Hartford Fire Ins. Co., 693 F.3d 665, 674 (6th Cir. 2012) ("Other jurisdictions have considered the meaning of the word in the context of similar insurance policies. The weight of the authorities define 'directly' as meaning 'immediate'—known by some as the 'direct is direct' approach—although other jurisdictions espouse a 'proximate cause' approach.").

directly from," and state and federal circuit courts around the country have predominantly adopted a direct, immediate understanding of causation when adjudicating coverage disputes.[141] For purposes of promoting uniformity and predictability, courts should apply the direct causation approach when deciding computer fraud coverage cases. There are, however, additional considerations that make this the best approach.

1. Intent of the Parties

Limiting covered losses to those that immediately follow the fraud not only comports with the plain meaning of the term,[142] but this approach also aligns with the intent of the parties at the time of contract formation.[143] None of the policies in question expressly define the sorts of losses covered when a direct loss of money is caused by a computer fraud. Hence, where the "terms of the [policy] itself" do not clearly indicate the parties' understanding, courts can look to a "body of law or an established custom or usage" to provide a definition.[144] Because a majority of courts, both federal and state, subscribe to the immediate causation standard,[145] the parties' intent may be inferred as aligning with this common understanding.[146]

---

141. David Spielbauer & Shane Mecham, *Post Hoc, Ergo Propter Hoc: A Fifty-State Survey of Causation in Fidelity Bonds*, 22 FIDELITY L.J. 265, 266 (2016) ("Unfortunately, not all courts agree on what the phrase 'loss resulting directly from' means. The majority rule and modern trend is for courts to enforce the plain language of the contract and conclude that the [policy] unambiguously requires the loss to be 'direct' or immediate. Intervening and superseding acts break the causal chain. A minority of courts . . . interpret the [policy's] 'direct loss' language to mean 'proximate cause' or 'but for' causation."); *Id.* at 281 (noting that thirty-three of fifty states and eight of eleven federal circuits follow the direct causation approach).

142. *Direct*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("Free from extraneous influence; immediate.").

143. Beazley Ins. Co. Inc. v. ACE Am. Ins. Co., 880 F.3d 64, 69 (2d Cir. 2018) ("[A]n insurance contract is interpreted to give effect to the intent of the parties as expressed in the clear language of the contract.") (alteration in original) (citation omitted).

144. *Id.* ("In assessing whether there is [ ] a prevailing federal definition, we consider not whether there is complete unanimity among the courts that have addressed the question, but rather whether there is an overwhelming current of judicial opinion, that is, a meaning used by the vast majority of federal courts.") (alteration in original) (citation omitted).

145. *See* discussion *infra* Section III.B.

146. *Beazley*, 880 F.3d at 70 ("Federal case law is simply another way of determining whether the parties shared a common language that would lead them to a mutual, unambiguous understanding of the meaning of an undefined term.").

Certainly, parties could draft policy language more clearly, but absent these specific provisions, the "ordinary and popular sense" is deemed to be its intended definition.[147]

2. Reasonable Expectations

The temporal causation analysis is also superior because of the parties' reasonable coverage expectations. Computer fraud policies typically cover traditional hacking where a person "surreptitiously break[s] into the computer, network, servers, or database of another person or organization."[148] Though insureds "have tried to extend hacking coverage to instances in which criminals give bad information that is then legally entered into the policy holder's computer," policy coverage is generally understood to apply where a third party carries out the computer fraud.[149] Indeed, many insurance companies offer a social engineering fraud coverage extension or endorsement that specifically applies to BEC schemes where an authorized company employee ultimately executes the wire transfer based on fraudulent instructions.[150] Based on the contract

147. Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627, 629 (9th Cir. 2017) ("We interpret words in accordance with their ordinary and popular sense, unless the words are used in a technical sense or a special meaning is given to them by usage.") (quoting Emp'rs Reinsurance Co. v. Superior Court, 161 Cal. App. 4th 906, 919 (Cal. Ct. App. 2008)).

148. *Hack*, BLACK'S LAW DICTIONARY (11th ed. 2019); Alan Rutkin, *Cyber-Crimes: How Have Courts Dealt with the Insurance Implications of This Emerging Risk?*, AM. C. COVERAGE & EXTRACONTRACTUAL COUNS. (2016), https://coverage.memberclicks.net/assets/Documents/accec_2016_annualmeeting_attendeematerials_web.pdf [https://perma.cc/S7H7-DLCA].

149. Rutkin, *supra* note 148.

150. Lynda Bennett, *Beware of Coverage Gaps for Social Engineering Losses*, RISK MGMT. MONITOR (May 23, 2016), https://www.riskmanagementmonitor.com/beware-of-coverage-gaps/ [https://perma.cc/DH9H-3SM2] ("Given the prevalence of social engineering claims and the clear market for companies looking to insure against such risks, some insurers have begun to offer an endorsement that provides coverage for social engineering claims."); *Social Engineering Fraud Coverage for Crime Insurance*, CHUBB, https://www.chubb.com/ca-en/business-insurance/social-engineering-fraud-coverage-for-crime-insurance.aspx [https://perma.cc/SJW2-4QHE] (last visited Sept. 17, 2019) ("The Social Engineering Fraud Endorsement insures a range of social engineering fraud losses when added to a Chubb Crime Insurance policy, including . . . [v]endor or supplier imitation . . . [e]xecutive imitation . . . [and] [c]lient imitation."); *Social Engineering Fraud Endorsement*, TRAVELERS INDEMNITY CO. (2016), https://www.travelers.com/iw-documents/professional-liability-insurance/CP-8697-social-engineering-fraud.pdf [https://perma.cc/33RL-L569] ("That is why Travelers is offering an endorsement with a social engineering fraud insuring agreement for Wrap+ and Executive Choice+ Fidelity and Crime coverages.

interpretation maxim *expressio unius est exclusio alterius*,[151] the lack of specific policy language purporting to cover phishing attacks supports the interpretation that such attacks are not covered, meaning the insurer and insured alike could not "reasonably have expected this provision to cover" BECs at the time of contract formation.[152]

C. Same and Different Results Under This Proposal

Following the "direct is direct" approach tends to narrowly interpret the sequence of events that may transpire and still provide for computer fraud coverage.[153] Yet, when "direct [means] direct" in the policy language, a "temporally remote" loss is necessarily excluded.[154] Employing the Eleventh Circuit's step-by-step analysis to a coverage dispute helps delineate when losses are direct or remote. In *Brightpoint, Inc. v. Zurich American Insurance Co.*, for example, Brightpoint, the plaintiff, received a known purchaser's fax requesting $1.5 million worth of prepaid phone cards.[155] Brightpoint complied but later discovered that the purchase documentation was fraudulent, and the cards were never recovered.[156] Brightpoint then tendered a claim under its crime insurance policy and later brought suit after the insurer denied coverage.[157] The court ultimately found for the insurer because lost property was not inside Brightpoint's premises when the fraud occurred and because the fax did not "'fraudulently cause[] a transfer' of the phone cards."[158] However,

---

Traditional Fidelity and Crime insurance policies often limit losses to fraud schemes that a business is unaware of and is not an active participant in the scheme. This endorsement specifically extends coverage to include instances of social engineering fraud perpetrated by a purported vendor, client, employee or authorized person.").

151. *Expressio unius est exclusio alterius*, *supra* note 62.

152. Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332, 333 (9th Cir. 2016).

153. Tooling, Mfg. & Techs. Ass'n v. Hartford Fire Ins. Co., 693 F.3d 665, 674 (6th Cir. 2012).

154. Interactive Commc'ns Int'l v. Great Am. Ins., 731 F. App'x 929, 935 (11th Cir. 2018); *Tooling, Mfg. & Techs. Ass'n*, 693 F.3d at 674.

155. Brightpoint, Inc. v. Zurich Am. Ins. Co., No. 1:04-CV-2085-SEB-JPG, 2006 WL 693377, at *2–3 (S.D. Ind. Mar. 10, 2006).

156. *Id.* at *3.

157. *Id.* at *1.

158. *Id.* at *6–7.

the temporal causation analysis could have produced similar results as well.

In *Brightpoint*, the plaintiff received the fraudulent fax at step one.[159] At step two, Brightpoint sent an employee to a separate company from which Brightpoint purchased its phone cards.[160] This company employee then turned the phone cards over to the fraudulent buyer at step three.[161] It is at this point that Brightpoint lost control of the property, and thus the loss did not flow directly from the fraudulent fax at step one.[162] Other cases are similarly illustrative.

Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America involved a seafood importer who was defrauded out of $713,890 when a hacker, posing as a vendor, requested new wire instructions via spoofed emails.[163] The court found a voluntary transfer provision controlling, but the temporal causation analysis would have sufficed as well.[164] In this case, Aqua Star received the fraudulent emails at step one.[165] The recipient employee, following company protocol, then "printed out a copy of the spreadsheet [with the fraudulent wiring instructions therein] and included it in a package of documents that was presented to a member of Aqua Star's

159. *Id.* at *2 ("On both January 23 and 24, 2003, by facsimile, Brightpoint received copies of purchase orders, post-dated checks, and bank guaranties believed to be from or authorized by Genato.").

160. *Id.* ("After Brightpoint received these faxed documents on both January 23 and 24, 2003, it sent an employee, Jay-Jay N. Moralde, to the main office of Globe Telecom ('Globe'), the company from which Brightpoint purchased the cards to be distributed to Genato.").

161. *Brightpoint*, 2006 WL 693377, at *2 ("At a location just outside Globe's building, and after receipt of the originals of the post-dated checks and bank guaranties that had earlier been faxed to Brightpoint, Moralde turned over the phone cards he had purchased from Globe. The exchange was made with Reena Aldeguer, a person who had attended other similar exchanges and who was believed to be a representative of Genato.").

162. *Id.* at *7.

163. Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. C14-1368RSL, 2016 WL 3655265, at *1 (W.D. Wash. July 8, 2016), *aff'd*, 719 F. App'x 701 (9th Cir. 2018).

164. *Aqua Star*, 719 F. App'x at 702 ("Exclusion G unambiguously provides that the policy 'will not apply to loss or damages resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System[.]' Aqua Star's losses resulted from employees authorized to enter its computer system changing wiring information and sending four payments to a fraudster's account. These employees 'ha[d] the authority to enter' Aqua Star's system when they 'input' Electronic Data, on Aqua Star computers, to change the wiring information and authorize the four wires. Their conduct fits squarely within the Exclusion. While other contractual exclusions may also bar coverage in this case, we need not go any further.") (citations omitted).

165. *Aqua Star*, 2016 WL 3655265, at *1.

management for approval of the payment."[166] This constituted step two. At step three, presumably following management's approval, the employee completed "four payments to a fraudster's account."[167] Here, again, an intervening step between the fraud and the loss would have provided a sufficient basis to deny coverage under the computer fraud provision, irrespective of any policy exclusions.

Under this proposal, *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America* would come out differently. In *American Tooling Center*, the court noted that the plaintiff "received the fraudulent email at step one."[168] Yet, the "internal actions" of the employees that ultimately authorized the wire transfer were not deemed to be intervening steps between the email at step one and the loss of the funds at the final step.[169] A better approach is to classify the phishing attack from beginning to end and determine the steps involved to get from the fraudster's initial attack to the ultimate loss of control of the property or money. Any steps between these two points in time, whether inside or outside the company, would sever the causal relationship and not be a direct loss under the policy.

This strict policy interpretation appears to favor insurers on its face, but in practice it would promote insured awareness and diligence in identifying coverage gaps. Tying back to accountability, this approach would put insureds on notice regarding their security policies and how the steps between initiation and completion of a phishing attack may preclude computer fraud coverage. However, upon receipt of a suspicious email or other electronic communication, the policy holder will ideally discover and thwart the attack ahead of any loss—as prompted by the courts' uniform application of a computer fraud policy.

166. *Id.* at *3.
167. *Aqua Star*, 719 F. App'x at 702.
168. Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 463 (6th Cir. 2018).
169. *Id.*

CONCLUSION

Insurance companies and policy holders face an uncertain future given the bombardment of new and emerging cyber threats. Sophisticated email phishing attacks in particular have cost businesses hundreds of thousands, even millions, of dollars in fraudulent wire transfers.[170] Coverage decisions under a computer fraud policy have (to this point) been inconsistent in the federal circuit courts. To resolve this circuit split, a uniform interpretation is proposed that fosters the insured's threat detection and prevention and keeps with traditional readings of insurance policies. These factors can work in parallel to keep businesses safe and encourage harmony and—importantly—predictability between insurer and insured.

170. Matthews, *supra* note 28.