Volume 65
Issue 6 *V.65, Tolle Lege*

Article 1

2-3-2021

Go Phish: Circuit Split in Policy Interpretation for Social Engineering Fraud Losses Creates Ambiguity for Insurers and Insureds

Gabriella Scott

Comment

GO PHISH: CIRCUIT SPLIT IN POLICY INTERPRETATION FOR SOCIAL ENGINEERING FRAUD LOSSES CREATES AMBIGUITY FOR INSURERS AND INSUREDS

GABRIELLA SCOTT*

> "The development of technology will leave only one problem: the infirmity of human nature."[1]

I. UNCHARTED WATERS: INSURERS AND COURTS HIT A SNAG IN LINE OF PRECEDENT WITH SOCIAL ENGINEERING FRAUD

"I need your help with a last-minute transaction," the email read, sent to a new employee in a company's large finance department.[2] The employee read on, realizing that the message bore the signature, company logo, and email address of her CEO.[3] Somewhat startled that she would be singled out among her peers for such an important task, the employee's hand lingered over the phone to contact her supervisor as she read the details of the client's financial institution and the large sum of money to be wired.[4]

---

* J.D. Candidate 2021, Villanova University Charles Widger School of Law; B.A. 2018, University of Kentucky. I would like to dedicate this Comment to my family for their constant love and support. I also would like to thank all of the teachers and professors who have helped me grow as a writer over the years; namely, Kristi Spayd, Debbie Hudson, Dr. Bruce Holle, and Professor Diane Pennys Edelman. Finally, I would like to thank my friends, who have brightened even the toughest of law school days, and everyone on *Villanova Law Review* who helped with this Comment.

1. KARL KRAUS, HALF-TRUTHS & ONE-AND-A-HALF TRUTHS: SELECTED APHORISMS OF KARL KRAUS 123 (Harry Zohn ed. & trans., Univ. of Chi. Press 1990) (1976). Kraus, a satirical Austrian writer during World War I, did not live to see the rise of world-altering technology intertwined with modern everyday life; yet, this pansophical statement serves as an ominous prediction of the manner in which computers and contemporary technology have surpassed human intellect and reliability in many ways. *See generally* Wilma Abeles Iggers, KARL KRAUS: A VIENNESE CRITIC OF THE TWENTIETH CENTRY (1967).

2. *See generally* David S. Wilson et al., *Social Engineering Fraud in the Context of Computer and Funds Transfer Fraud Coverages*, FIDELITY & SURETY COMM. NEWSL. (ABA, Chicago, Ill.), Fall 2016, at 13 (describing common social engineering fraud schemes). Although the scenario described here is fictional, it is indicative of a typical social engineering fraud scheme categorized as the "executive impersonation scam," characterized by a spoof or similar domain email sent by a high-ranking individual in the company to a lower ranked employee "relating to a 'top secret' acquisition, merger or emergency situation." *Id.*

3. *See generally* Kunal Pandove et al., *Email Spoofing*, 5 INT. J. OF COMPUT. APPLICATIONS 27, 27–28 (2010) (describing methods used by fraudsters to send phishing emails either from compromised email account or those which are "spoofed" to appear as though they are sent from official account). Because fraudulent emails can bear the exact address and signature of the sender whose credentials are imitated either by compromising the sender's email or by spoofing, it is often difficult for the recipient to spot a phishing email. *See id.* at 27–28.

4. *See generally* Justin Pritchard, *How Wire Transfers Work: Sending and Receiving*, BALANCE https://www.thebalance.com/bank-wire-transfer-basics-315444 [https://perma.cc/AK3S-CB47]

The employee stopped, however, when she reached the last line: "This is extremely time-sensitive, and due to an error on my part this did not go through on the correct date. If you could, please, keep this between us."[5] Although the company had a specific verification protocol to follow prior to a transfer of this sum, the employee felt that the email explained the situation and required her secrecy.[6] Following orders from her superior, the employee input the information and completed the transfer.[7]

Only after the employee irrevocably wired $300,000 to a criminal's bank account did she realize that a fraudster had spoofed the CEO's email account and sent them the message.[8] To make matters worse, she was not the only employee targeted.[9] Four other new employees that received the same email also fell for the scheme, resulting in a combined total loss of $1.2 million.[10]

Unfortunately, fraudulent schemes like the fictional scenario described here are on the rise and are increasingly targeting a wide range of corporations.[11] Ironically,

---

(last updated May 19, 2020) (explaining how wire transfers work). The immutability of wire transfers explains why they are commonly used in fraudulent schemes. *See id.*

5. For further discussion of the various trends and schemes in social engineering fraud, see *supra* note 2.

6. *See generally* Wilson, *supra* note 2, at 13 ("The financial institution's employee is induced by email, phone or fax to wire client funds to a 'new' account. Verification procedures are either absent or not followed, and the funds are typically unrecoverable.").

7. *See* Scott L. Schmookler & Christopher M. Kahler, *Social Engineering: Is the Manipulation of Humans A Computer Fraud?*, 22 FIDELITY L.J. 1, 15 (2016) (explaining why social engineering fraud schemes in which criminals impersonate employee's superior are particularly successful). As in the fictional scenario presented in the text, this article describes why these schemes can successfully target multiple employees in the same company. Impersonation of a superior can "appeal[] to several of the unwitting participant's emotions: credibility; fear of repercussions for failing to act; adherence to the corporate structure; and, sense of importance by fulfilling an important task." *Id.* at 16.

8. *See* Jessica H. Park & John G. O'Neill, *An Evolving Landscape: Insurance Coverage for Social Engineering Wire-Fraud Scams*, 60 DRI FOR THE DEF. 70, 70–72 (2018) (detailing anatomy of social engineering scam). Prior to selecting the means used to contact the target of a social engineering scam, criminals will typically gain information by "infiltrating company networks or other channels." *Id.* at 71. In the fictitious scenario presented in the text, the criminals targeted new employees within the company, which is indicative of the knowledge often gained regarding the company's hierarchy to select a vulnerable target. The cited article also highlights that once a wiring transaction has been completed, it typically cannot be retrieved. *See id.*

9. *See* Katrien Anthonis, *It Can Happen to You: Social Engineering in Finance*, SECURELINK (Oct. 10, 2018), https://securelink.net/en-be/insights/it-can-happen-to-you-social-engineering-in-finance/ [https://perma.cc/HX94-M5B5] (describing test of social engineering fraud scheme). This article describes a security test performed on a large financial institution in Belgium, in which ten of the top managers were targeted through a fake social engineering scheme seeking the managers' credentials. *See id.* The article highlights the ease that those performing the study were able to find information about the managers, their employment duties, and hobbies through "a simple internet search." *Id.* (emphasis omitted). Astoundingly, six of the ten managers fell for the social engineering scheme. *See id.*

10. *See* Schmookler & Kahler, *supra* note 7 (explaining why social engineering fraud schemes in which criminal impersonates employee's superior are particularly successful).

11. *See* Henry Kenyon, *Hackers Increasingly Target Financial Institutions, Carbon Black Says*, CONG. Q., Mar. 12, 2019, 2019 WL 1122058 (noting 79% of financial institutions reported an increase in social engineering fraud); *see also* Schmookler & Kahler, *supra* note 7, at 2–4 (illustrating recent increase in crimes which target humans rather than technology). Although social engineering is not a new concept, "the reported number of social engineering type-schemes targeting employees increased by 55% in 2015 and is the leading threat to organizations." Schmookler & Kahler, *supra*

due to advancements in cybersecurity measures like antivirus software and malware protection, criminals have started to use humans to acquire funds and information from companies.[12] These schemes surpass direct hacking methods whereby the hacker would gain access to information using malicious code and instead trick employees into giving away money or critical information in good faith.[13] Such schemes have been categorized as "social engineering" fraud schemes.[14]

Social engineering fraud schemes have enormous implications upon both the scope of fraudulent losses suffered by companies and the future of crime and fidelity insurance coverage litigation.[15] An example of a social engineering fraud scheme is displayed in the hypothetical scenario presented above: a criminal sends a phishing email—"spoofed" to appear as though it is from a trusted individual—to persons with access to funds or with specific instructions for a transaction. Fraudsters also implement these schemes through telephone calls and fax machines.[16]

Currently, most companies' crime or fidelity insurance policies only contain provisions for "computer fraud," which often rely on language drafted before the prevalence of social engineering fraud.[17] In drafting policy language, underwriters

---

note 7, at 5 (footnote omitted).

12. *See* Jennifer Towne, *Social Engineering: An Old Con is Becoming a New Threat*, ACADIA INS., https://www.acadiainsurance.com/social-engineering-fraud-old-con-becoming-new-threat/ [https://perma.cc/DEY6-H7PU] (last visited Nov. 25, 2019) (noting that because social engineering preys on good-natured employees, this type of fraud is difficult to prevent and especially threating to businesses). As noted by the article, "[t]here is no antivirus for this" type of threat. *Id.* Thus, it is especially important to have insurance to cover these types of risks because they are extremely difficult to avoid. *See id.*

13. *See* Wilson et al., *supra* note 2, at 13 (explaining why fraudsters are increasingly finding it easier to "hack" humans rather than computers). Due to the growing protections on computer systems to protect against hackers, typically the "weakest point in an organization's security system is the employees themselves," thus, explaining the increase in social engineering fraud schemes. *Id.*

14. *See generally* Christie M. Bird & Reina Dorvilier, *Social Engineering Fraud: Current Trend in Coverage for Insureds*, 48 SPG BRIEF 10 (2019) (providing definition for social engineering fraud). In addition to classifying 2018 "as the year of the social engineering fraud claim" in the fidelity industry, this article provides a broad definition of social engineering fraud as "scams used by criminals to trick, deceive and manipulate their victims into giving out confidential information and funds," which "may be carried out online, by telephone, or even in person." *Id.* at 11 (first internal quotation marks omitted) (citation omitted).

15. *See* Park & O'Neill, *supra* note 8, at 10 (detailing how social engineering fraud has evolved in courts and insurance coverage continues to affect businesses of all types and sizes). Additionally, this article addresses the changed landscape of insurance coverage litigation, as "courts generally have not yet grappled with questions of coverage for social engineering losses . . . making it difficult to predict how potential coverage arguments under those policies will be developed and resolved." *Id.*

16. For further explanation of social engineering fraud schemes and the manner in which they are implemented, see *supra* notes 2–14; *see also* Brian Krebs, *Voice Phishing Scams are Getting More Clever*, KREBS ON SECURITY (Oct. 1, 2018, 10:02 AM), https://krebsonsecurity.com/2018/10/voice-phishing-scams-are-getting-more-clever/ [https://perma.cc/HS7Q-AT8U] (describing how voice phishing schemes or "vishing" are growing increasingly common as social engineering fraud techniques). A common voice phishing scheme involves criminals from a financial institution calling and stating that fraudulent transactions have been made on a certain account, prompting the recipient of the call to give their information to confirm their identity. *See id.*

17. *See* Melissa M. D'Alelio, *One Phish, Two Phish: Developments in the World of Computer Fraud Coverage*, 48 SPG BRIEF 18, 19 (2019) (distinguishing "hacking" from "phishing" and explaining insurance policy forms for computer coverage were intended for hacking). Furthermore, this article

anticipated coverage of a cybercriminal's unauthorized and direct taking of information or funds by hacking a computer system.[18] Therefore, the language in most standard policies for computer fraud strictly and plainly necessitates a "direct" loss due to a "fraudulent entry" into the computer system.[19]

In addition to highly specific coverage language, most applicable policies contain exclusions that distinguish "computer fraud" from indirect methods of fraud or theft; for example, some policies have exclusions for losses resulting from data entry by an authorized "natural person," such as an employee.[20] Due to the involvement and necessary manipulation of an employee in social engineering fraud, the waters of coverage for these schemes are murky.[21]

Historically, insurers and courts categorized social engineering fraud as distinct from losses covered under "computer fraud" provisions, leaving companies to bear the impact of these losses without coverage.[22] Prior to 2018, the majority of courts held that social engineering fraud losses were not covered under insurance

---

explains "that the purpose of the Computer Fraud Coverage Form is to cover instances where a perpetrator directly hacks into an insured's computer system and fraudulently causes—by his own actions—a transfer of money." *Id.* For more information regarding the modern phenomenon of social engineering fraud, see *infra* notes 38–66 and accompanying text. To compare this to information regarding when the Computer Fraud Coverage Form was drafted, see *infra* notes 77–81 and accompanying text.

18. *See* John J. McDonald, Jr. et al., *Computer Fraud and Funds Transfer Fraud Coverages*, 14 FIDELITY L.J. 109, 111–13 (2008). This article explains that the insurance industry standard form for computer fraud "coverage is intended to protect against third-party access" to the computer system, rather than losses involving employees of the insured company. *Id.* at 112. This intent is evidenced by multiple exclusions added to the standard policy form since its inception. *See id.* at 113–14.

19. *See, e.g.*, Interactive Commc'ns Int'l Inc. v. Great Am. Ins. Co., 731 F. App'x 929, 930 (11th Cir. 2018) (holding social engineering losses did not "result directly" from computer fraud as required by plain language of insured's policy even though losses were perpetrated through computers); Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78, 82 (N.Y. 2015) (holding "fraudulent entry" in insured's policy refers to unauthorized access into computer system and not to content submitted by authorized users such as employees). *But see, e.g.*, Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 119 (2d Cir. 2018) (holding sending email manipulated to appear as though it was sent from company's official satisfied "fraudulent entry" of data and, thus, social engineering scheme constituted computer fraud).

20. *See, e.g.*, Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., 719 F. App'x 701 (9th Cir. 2018) (holding coverage for social engineering fraud loss was precluded by policy exclusion for data entry "by a natural person"). In this case, the relevant exclusion stated that computer fraud coverage would 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," such as input by an employee. *Id.* at 702.

21. *See generally* Roberta Anderson, *Securing Insurance for Social Engineering Exploits*, 20 TORTSOURCE 12 (2018) (explaining insurers' resistance to concede coverage for social engineering fraud losses due to victim's role in scheme). In this article, written to provide advice to ensure that companies secure adequate coverage, the author warns that "[s]ocial engineering exploits present relatively new exposures that do not tend to fit neatly into traditional forms of coverage." *Id.* at 13. For a further discussion of social engineering fraud schemes and the manner in which they are implemented, see *supra* notes 2–14.

22. *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 258–59 (5th Cir. 2016) (holding company's social engineering losses were not covered under computer fraud provision in crime-protection insurance policy because employee personally authorized fraudulent transfers to criminal's bank account). In this decision, the court reasoned that even though the crime was initially perpetrated through an email, the email and thus use of computer was "merely incidental" to the transfer. *See id.* at 258.

provisions for "computer fraud" due to courts plainly interpreting language in the insurance policies.[23] These initial decisions denied coverage for companies and favored insurers under several rationales—most notably, the opinion that computer fraud provisions have language requiring that losses arose "directly" from the use of a computer.[24]

By contrast, in social engineering fraud, an employee is involved in the chain of events that causes the losses. Courts have historically held that the mere use of a computer in achieving human deception did not trigger coverage.[25] The solution initially appeared to be a simple one: insurance underwriters could add social engineering coverage as either an optional or standard endorsement to the crime or fidelity policies insurers issue, making social engineering coverage completely separate from computer fraud.[26] To protect against this specific type of threat, companies would either select a standard policy with a social engineering endorsement or make sure that they added this coverage to their existing policies.[27]

Recently, however, several circuit courts signaled a break from precedent and created a circuit split over the question of whether losses from social engineering fraud schemes are covered under virtually identical insurance provisions for

---

23. *See* Jonathan L. Schwartz & Colin B. Willmott, *And Then There Was One: The Emerging Split Over Insurance Coverage for Social Engineering Fraud Claims*, FIDELITY & SURETY COMM. NEWSL. (ABA, Chicago, Ill.), Fall 2018, at 17 (contrasting prior majority view with more recent decisions). This analysis explains that prior to 2018, the majority of courts were "reluctа[nt] to find coverage for social engineering fraud." *Id.* The authors state: "[a] maxim undergirding [the majority] approach is that since the use of computers is ubiquitous, virtually all fraudulent conduct merely involving the use of email could potentially be covered. In other words, the majority approach is wary to transform a computer fraud/crime policy into a general fraud policy." *Id.*

24. For a discussion of early cases that denied coverage and favored the insurers, see cases cited *supra* notes 19–20.

25. *See Apache*, 662 F. App'x at 258 (explaining that, although email was part of scheme, Apache employee changing account information and transferring funds leading to large financial loss did not trigger coverage); *see also* Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332 (9th Cir. 2016) (holding general intent of computer fraud coverage is to be limited to hacking incidents through unauthorized entry into computer systems). Although *Pestmaster* did not involve an instance of social engineering fraud, a company executed an authorization to a payroll company for invoices. *See Pestmaster*, 656 F. App'x at 333. However, the payroll company kept the funds instead of paying the authorized invoices, and the lower court found and appellate court affirmed that the company was not covered under their policy provision for computer fraud because that provision would be triggered only "when someone 'hacks' or obtains unauthorized access or entry to a computer to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds." Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., No. 13-5039-JFW, 2014 WL 3844627, at *6 (C.D. Cal. July 17, 2014), *aff'd in part*, *vacated in part*, 656 F. App'x 332 (9th Cir. 2016).

26. *See* Bird & Dorvilier, *supra* note 14, at 16 (discussing insurers making social engineering fraud coverage available to insureds). The authors assert that, despite this attempted solution, they do not believe the introduction of this coverage will deter insureds from seeking social engineering coverage under computer fraud provisions. *See id.*

27. *See* Ken Kronstadt, *Insurance Coverage for Social Engineering Fraud*, 33 WEST. J. CORP. OFFICERS & DIRS. LIAB. 2 (2018) (surveying recent court rulings for social engineering fraud under computer fraud provisions and providing insights for companies looking to secure coverage). As the article notes, due to the prevalence of social engineering fraud schemes, there is demand for companies to secure coverage against these schemes. *See id.* Due to increasing demand, "some insurers have begun to offer policy endorsements specifically providing coverage for these claims." *Id.* However, insurers have added additional sublimits and exclusions to these policy provisions. *See id.*

"computer fraud."[28] In 2018, the Second and Sixth Circuit Courts of Appeals issued monumental decisions when they held that social engineering fraud attacks were covered under "computer fraud" provisions using a proximate cause standard; both courts found that a sufficient causal relationship existed between the use of a computer and the losses suffered.[29] Additionally, these decisions shifted interpretation of various policy exclusions, such as those involving "the input of Electronic Data by a natural person."[30]

While the current trend favoring insureds may be appealing to some, courts should return to a strict interpretation of plain policy language because the loosened causal analyses applied in recent cases depart from the standard method of insurance policy interpretation.[31] By restricting coverage to a plain interpretation of policy language, courts will promote cross-jurisdictional uniformity for the interpretation of the same policy language across state lines.[32] Furthermore, interpretation of computer fraud provisions to exclude social engineering schemes will induce underwriters to add social engineering fraud to crime and fidelity policies, thus, ensuring that all companies are adequately covered for these losses, regardless of where their claim arises jurisdictionally.[33] Finally, disentangling computers from the crime or activity involved will prepare the insurance litigation field for a future in

---

28. *See generally* Schwartz & Willmott, *supra* note 23 (detailing emerging circuit split regarding social engineering fraud coverage and discussing impact of the rulings).

29. *See* Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 119 (2d Cir. 2018) (holding spoofed emails proximately, and thus directly, caused social engineering fraud losses despite employee involvement in unfolding of scheme). Explaining its rationale for affirming the district court's holding that the company's losses were covered under "computer fraud" provision in company's insurance policy, the court stated:

> While it is true that the Medidata employees themselves had to take action to effectuate the transfer, *we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred*. The employees were acting, they believed, at the behest of a high-ranking member of Medidata. And New York law does not have so strict a rule about intervening actors as [the insurer] argues.

Id. at 119 (emphasis added); *see also* Am. Tooling Ctr., Inc. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 462 (6th Cir. 2018) (holding company suffered "direct loss" that was "directly caused by computer fraud" when employee signed into his company's "banking portal and manually entered the fraudulent banking information" sent by criminal via spoofed email).

30. *See Am. Tooling*, 895 F.3d at 463–65 (explaining why none of policy exclusions asserted by insurer precluded coverage for stated claim). In analyzing the asserted exclusions, the court found that several exclusions in the insured's policy with similar provisions found applicable in other jurisdictions did not preclude coverage for social engineering losses: Exclusion R, which stated that the subject crime policy would "not apply to loss resulting directly or indirectly from the giving or surrendering of [m]oney . . . whether or not fraudulent"; Exclusion G, which stated that coverage would "not apply to loss or damages resulting directly or indirectly from the input of [e]lectronic [d]ata by a natural person"; and Exclusion H, which stated that the policy does not cover any "loss resulting directly or indirectly from forged, altered or fraudulent . . . written instruments." *Id.* (emphasis omitted) (quoting Transcript of Record at 21-2, *Am. Tooling*, 895 F.3d at 463–65).

31. For a further discussion of the circuit cases favoring the insured, see *infra* notes 108–24 and accompanying text. For a discussion of the standard method of insurance policy interpretation, see *infra* notes 67–84 and accompanying text.

32. For a further discussion of how a plain interpretation of policy promotes cross-jurisdictional uniformity, see *infra* notes 83–84 and accompanying text.

33. For a further analysis of the impact of interpreting computer fraud to exclude social engineering, see *infra* notes 138–39 and accompanying text.

which technology is ubiquitous in all aspects of corporate and daily life.[34]

Part II of this Comment describes common schemes used in social engineering fraud, provides an overview of legal standards of insurance policy interpretation, and summarizes the uniform rationales used by courts in addressing this issue prior to the circuit split which arose in 2018. Part III of this Comment provides insight into the rationales implemented by courts breaking from precedent and furthering the current trend. Part IV opines that the loosened standards implemented in these decisions will have negative effects on both insurers and insureds. Finally, Part V predicts the impact of the circuit split on the numerous stakeholders involved in social engineering fraud.

II. LETTING INSURERS OFF THE HOOK: PRE-CIRCUIT SPLIT CONSENSUS HOLDS THAT SOCIAL ENGINEERING LOSSES ARE NOT "COMPUTER FRAUD"

Prior to the subject circuit split, the majority of courts distinguished losses involving the direct hacking of a computer system from those involving employee manipulation when determining whether insurance policies covered social engineering fraud.[35] Because human manipulation is key to social engineering fraud, courts generally corroborated the notion that these losses were not covered under "computer fraud" provisions.[36] To understand both the initial posture and the subsequent split, one must first understand the distinct character of social engineering fraud, the practices used by underwriters to draft policy language, the principles used by courts to interpret insurance policies, and the nature in which these topics shaped the view unanimously shared by courts prior to 2018.[37]

A. *Reeling in Employees with a Red Herring: An Overview of the Deceptive Nature of Social Engineering Fraud*

Social engineering is a term established long ago that encompasses a wide variety of schemes used by criminals to prey on human tendencies and commit "theft with the absence of strong-armed tactics such as violence or the threat of violence."[38] By one commentator's definition, social engineering is "the act of

34 For further discussion of the effects of technological developments on the insurance industry, see *infra* notes 148–50 and accompanying text.

35. *See, e.g.*, Tidewater Holdings, Inc. v. Westchester Fire Ins. Co., 389 F. Supp. 3d 920 (W.D. Wash. 2019) (holding social engineering fraud losses not covered under computer fraud policy provisions) Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627 (9th Cir. 2017); *see also* Alex Selarnick et al., *Recent Developments in Insurance Coverage*, 53 TORT TRIAL & INS. PRAC. L.J. 477, 478–85 (2018) (describing recent trends in computer fraud and social engineering fraud policy interpretation and identifying regional trends in courts' determination of whether coverage exists under policy terms).

36. *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 255–59 (5th Cir. 2016) (asserting that policy terms required losses be "direct result" of computer fraud, rather than caused by actions of employees); *see also* Bird & Dorvilier, *supra* note 14, at 16 (discussing pre-2018 majority view that direct entry through hacking, rather than manipulation of employees, qualifies for coverage under computer fraud insurance provisions).

37. *See generally* Schmookler & Kahler, *supra* note 7, at 70 (explaining importance of analyzing "the nature of the social engineering scheme to determine whether the insured suffered a covered loss").

38. *Id.* at 6 (recognizing term "social engineering" was coined in 1894 and discussing long

influencing a person to accomplish goals that may not be in the person's best interest."[39] In the modern context, social engineering is commonly used to describe the tactics employed by criminals to target information and funds from institutions or companies.[40]

Typically, relevant forms of social engineering fraud fall into one of four categories.[41] These categories include: (1) client impersonation fraud, (2) the executive impersonation scam, (3) the vendor impersonation scam, and (4) the law firm collection scam.[42] Understanding the basic plots of these schemes will aid in understanding the factual scenarios underlying social engineering fraud claims as well as the dangerous threat social engineering constitutes to institutions of all sizes.[43]

1. *Client Impersonation Fraud*

In client impersonation fraud, which usually targets banks, criminals contact a financial institution by email, phone, or fax and impersonate a client.[44] The fraudster then informs the targeted employee that the client has a new bank account which they would like their funds transferred to.[45] After the employee wires the funds, the employee typically cannot recover or recall the completed transfer.[46] These schemes are especially detrimental to banks because the financial institution must immediately compensate the real client once the fraud is discovered and then attempt to recover

history of social engineering). As the article explains, the term social engineering has been used in different capacities, such as to describe "the principle that government or other institutions could manipulate citizens to act in a desired manner or adhere to a particular political belief." *Id.* Furthermore, the article describes that social engineering in general "encompasses all forms of crime, such as the classic con game and Ponzi scheme," positing that "[s]uch implementation of manipulation and persuasion is timeless." *Id.* at 6–7.

39. *Id.* at 7 (internal quotation marks omitted) (quoting Lillian Ablon, *The Outsider Threat*, CIPHER BRIEF (Oct. 19, 2015), https://www.thecipherbrief.com/the-outsider-threat [https://perma.cc/CG3K-4BTE]. This somewhat ominous article, penned during the early rise of social engineering fraud, details the potential risks involved due to such threats from outsiders attempting to gain access to funds or information through people, and why social engineering schemes are so successful due to human nature. *See id.*

40. *See* Schmookler & Kahler, *supra* note 7, at 7–14 (explaining how general definition of social engineering fraud has now become more applicable to certain sets of fraudulent activities, being utilized through email and phone).

41. *See* Wilson et al., *supra* note 2, at 13 (describing general categories into which social engineering fraud schemes fall and detailing varying factors which contribute to success of each).

42. *See id.* (enumerating four most popular types of social engineering fraud).

43. *See* Schmookler & Kahler, *supra* note 7, at 70 (stating importance of understanding nature and scope of these schemes to be fully cognizant of risks associated with each for insurers and insureds).

44. *See id.* (discussing first step of client impersonation scam).

45. *See id.* (explaining purported client will typically explain that they have new account and need their funds transferred); *see also* Chris Griesemer, *Social Engineering: How Financial Institutions Can Prepare for Cyber Scams*, WHITLOCK CO. BLOG, http://www.whitlockco.com/social-engineering-financial-institutions-can-prepare-cyber-scams/ [https://perma.cc/HR8Y-TPUC] (explaining how "new phishing attacks can look like a legitimate customer request" with increasingly realistic methods).

46. For further discussion of wire transfers and why companies or financial institutions cannot typically recover wire transfers after completion, see *supra* note 8.

the funds under their own crime or fidelity insurance policy.[47]

2. *Executive Impersonation Fraud*

Executive impersonation fraud is particularly successful when used to manipulate employees of larger companies with equally sizable financial departments.[48] The perpetrator impersonates a high-ranking member of the company with whom the lower ranked employee likely does not have a close working relationship.[49] The fraudster typically contacts the employee by email or phone in an urgent tone, enlisting the employee's assistance with a transfer that is "last-minute" or "secret."[50] This scheme is ordinarily successful because the employee shirks authorization and security protocol in favor of obeying orders from a superior.[51] If a criminal can closely spoof or even gain access to the true email account of the executive to send the fraudulent message, this scheme is especially difficult to spot.[52]

3. *Vendor Impersonation Fraud*

Vendor impersonation fraud is similar to the client impersonation scam; however, the criminal instead impersonates an employee of an entity that is a vendor of the targeted organization.[53] The fraudster then states that the vendor needs to update its banking information.[54] The fraud is usually not discovered until after the

47. *See generally* VASCO, SOCIAL ENGINEERING: MITIGATING HUMAN RISK IN BANKING TRANSACTIONS 3 (2015) (ebook), https://www.onespan.com/resources/social-engineering-mitigating-human-risk-banking-transactions-0 [permalink unavailable] (explaining in quarter 1 of 2015, "over 37% of phishing attacks were trading on the names of banks and financial organizations"); *see also* Wilson et al., *supra* note 2, at 13 (noting victim must first reimburse its client then seek reimbursement from its insurer).

48. For further discussion of how and why social engineering fraudsters target companies with large finance departments, see *supra* notes 2–10.

49. *See, e.g.*, Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118 (2d Cir. 2018) (explaining social engineering fraud method through which criminals spoofed email to employees to appear as though it was sent from company's CEO).

50. *See* Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 473 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018) (conveying factual scenario in which employees were induced to complete fraudulent transfer in social engineering fraud). In the lower court decision later affirmed by the Second Circuit, the court explained that the targeted employees "received a group email purportedly sent from Medidata's president stating: 'I'm currently undergoing a financial operation in which I need you to process and approve a payment on my behalf.'" *Id.* (quoting Joint Exhibit Stipulation Exhibit 6, *Medidata*, 268 F. Supp 3d at 473 (ECF No. 41)); *see also* Wilson et al., *supra* note 2, at 13 (explaining that, for executive impersonation fraud, the "pretext is often an emergency payment relating to a 'top secret' acquisition, merger or emergency situation").

51. For further discussion of the pressures upon employees to follow orders from a superior in both factual and fictional circumstances, see *supra* notes 1–10 and accompanying text.

52. *See, e.g.*, *Medidata*, 268 F. Supp. 3d at 473 (detailing methods used by social engineering fraudsters to make email appear as though it was sent from company's president in case holding coverage under computer fraud provision). The court emphasized that "[t]he email contained the president of Medidata's email address in the 'From' field and a picture next to his name," making the request especially believable. *Id.*

53. *See* Wilson et al., *supra* note 2, at 13 (describing steps taken by criminals in perpetrating vendor impersonation scam).

54. *See id.* (explaining that in vendor impersonation scam "[t]he fraudster purports to be an

vendor realizes that the victim has not paid them but has instead wired money to the criminal's bank account.[55]

4. *Law Firm Collection Fraud*

Social engineering fraud also impacts the legal profession.[56] In a law firm collection fraud scheme, the criminal contacts a lawyer asking for assistance in settling a debt collection matter.[57] This fake "client" then gives the lawyer fraudulent information for the "debtor," who is in fact another criminal in collusion with the "client."[58] The lawyer then uses contact information from the "client" to collect the money from the "debtor."[59] The "debtor" presents the lawyer with a counterfeit check; subsequently, the "client" will ask for the funds collected.[60] Believing that the check is authentic, the lawyer transfers money from the lawyer's own trust account to the "client" before the check is returned as fraudulent.[61]

Therefore, although these schemes often involve a computer, there are several different methods gaining popularity among criminals that are categorized as social

employee of a legitimate vendor of the victim, and contacts the victim's employee to request that the vendor's banking information be changed").

55. *See, e.g.*, Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 253–54 (5th Cir. 2016) (describing company's vendor impersonation social engineering fraud claim). In this case, Petrofac was a legitimate vendor of Apache. *See id.* The fraudster impersonated a representative of Petrofac and called an Apache employee, asking to update Petrofac's account information for future transfers. *See id.* Apache transferred the funds for Petrofac's invoices in accordance with the new bank information and, within a month, was notified that Pretrofac had not been paid. *See id.* at 253.

56. *See generally* Wilson et al., *supra* note 2, at 13 (emphasizing that lawyers are routinely impacted by this type of scheme and explaining "limited scope of trust account overdraft coverage under most lawyers' professional liability policies"). The article explains how, in most cases, the criminals will use the names of known entities to induce the lawyer to assume that this is a legitimate venture and ask for assistance in settling a collections matter. *See id.* It is normally after the criminal has told the lawyer they need a transfer of the check amount "urgently" and the lawyer completed a transfer from their own trust account that the lawyer realizes the check is a counterfeit. *See id.* Because most lawyers do not have adequate trust account overdraft coverage, they must obtain crime or fidelity insurance policies to account for these risks. *See id.*

57. *See id.* (detailing steps in law firm collection fraud scheme). Because most lawyers do not have adequate trust account overdraft coverage, they must obtain crime or fidelity insurance policies to account for these risks. *See id.*

58. *See, e.g.*, Owens, Schine & Nicola, P.C. v. Travelers Cas. & Sur. Co. of Am., No. CV095024601S, 2011 WL 3200296, at *1 (Conn. Super. Ct. June 24, 2011), *vacated*, 2012 WL 12246940 (Conn. Super. Ct. Apr. 18, 2012) (discussing claim for coverage under computer fraud provision in which "plaintiff entered into an agreement with the client, through the use of computer e-mail, to collect a debt allegedly owed to the China client from a business located in Connecticut"). Although this judgment was vacated by the Superior Court of Connecticut, it assists in explaining the nature of a law firm collection social engineering fraud scheme. *See id.*

59. *See* Wilson et al., *supra* note 2, at 13 (describing next step in law firm collection fraud scheme).

60. *See Owens*, 2011 WL 3200296, at *1 (explaining that "client" of attorney requested plaintiff to wire funds to bank in South Korea before plaintiff realized check was fraudulent).

61. *See id.* (detailing that attorney victim to debt collection fraud scheme was informed that check was fraudulent after sending funds to client). The court explained that the plaintiff's bank "subsequently debited the plaintiff's IOLTA account because the check from the Connecticut debtor that the plaintiff had deposited into his account was fraudulent." *Id.*

engineering fraud.[62] Each involves tricking an employee into inducing the transfer of information or funds, preying upon human tendencies, and using an indirect method of taking information.[63] Currently, there is no existing common law that interprets policy provisions specifically for social engineering fraud.[64] Although some insurers have started to add coverage for these losses to their standard policies or offer it as an optional coverage addition to companies, this does not remedy the fact that most insureds are still dealing with crime or fidelity policies merely insuring against "computer fraud."[65] Therefore, when an insurance company denies an insured's social engineering fraud claim and the insured then brings a claim for coverage against the insurer, interpretation of the policy becomes a question for courts.[66]

B. *Opening a Policy's Can of Words: How Courts Interpret Language in Insurance Policies*

Insurance policies are elucidated by courts under state-specific common law standards.[67] If a claim involving insurance policy interpretation reaches a federal court, those sitting in diversity will abide by the *Erie* doctrine and apply state law to resolve claims implicating insurance matters.[68] Nevertheless, most states recognize uniform principles when interpreting matters of insurance law.[69]

---

62. *See id.* (noting different methods of perpetrating social engineering fraud).

63. *See* Schmookler & Kahler, *supra* note 7, at 6–21 (opining why social engineering fraud is becoming increasingly common as alternative to direct hacking and describing different methods used by fraudsters). As posited in the article, "[r]ather than use direct attacks on a business's computer system," tricking an employee to essentially give them information, "allows the criminal to avoid the 'brute force' necessary to circumvent the technological protections a corporation may employ; such as firewalls and password security." *Id.* at 7–8. As the opening to this Comment suggests, technology has become strong in comparison to human nature making it easier to manipulate humans. *See id.*

64. *See* Kronstadt, *supra* note 27 (assessing current coverage landscape where interpretation is focused on computer fraud provisions, with courts yet to assess coverage under social engineering fraud provisions). As the article states, "courts have yet to address coverage for social engineering fraud under cyberliability policies, and given the lack of uniformity in policy language, it is difficult to predict how a court will decide coverage." *Id.* at 6.

65. *See id.* (explaining that some insurers have begun to introduce social engineering fraud provisions to their policies). While insurers have begun to introduce this type of coverage, the author warns that "[p]olicyholders should scrutinize the language of these endorsements," because the insurers may have made the coverage subject to certain exclusions and sublimits. *Id.*

66. For a discussion of courts' methods of insurance policy interpretation, see *infra* notes 67–84 and accompanying text.

67. *See* Provau v. State Farm Mut. Auto. Ins. Co., 772 F.2d 817, 819 (11th Cir. 1985) (noting construction of insurance contracts is governed by substantive state law); *see also* 16 WILLISTON ON CONTRACTS § 49:14 (4th ed. 2019) (describing manner in which insurance policies are to be interpreted and general model rules of interpretation). While insurance policies are interpreted as contracts, the nature of a policy is taken into account when courts make decisions regarding policy language. *See* WILLISTON ON CONTRACTS, *supra.* Therefore, the general policy argument is that ambiguities in insurance policies are to be construed against the insurer. *See id.* Nevertheless, a court must adhere to a plain reading of the policy language to balance this favoring of insureds with the necessity of insurance industry uniformity in interpreting identical policy provisions. *See id.*

68. *See generally* Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938) (holding that when cases are decided in federal courts using diversity jurisdiction, courts will apply state substantive law); *see also* Russo v. Frasure, 371 F. Supp. 3d 586, 589–90 (E.D. Mo. 2018) (holding Missouri state substantive law applied in insurance policy claim).

69. *See generally* Eric M. Larsson, *Insured's "Reasonable Expectations" as to Coverage of Insurance*

Courts treat insurance policies as contracts between the insurer and insured.[70] Thus, courts apply contractual legal principles when questions of policy interpretation arise.[71] The language used in particular types of endorsements and exclusions, such as those contained in commercial crime policies for "computer fraud," tends to be universal in content and phrasing because it is based on standard forms issued by the Insurance Services Office (ISO).[72]

Most insurers rely on the standard forms issued by the ISO to create their own policies.[73] While insurers may make slight modifications to the industry-standard provisions, the ISO is the leading authority in the insurance industry for drafting legal language and providing risk assessments for insurers based upon the selected language.[74] Therefore, insurers make an important assumption when adopting ISO standard forms that they can reasonably project the risks associated with each provision and add exclusions to further calculate, with a degree of certainty, the likely financial risk associated with each policy endorsement.[75] Insurance policies protect policyholders from bearing the costs of what is arguably unforeseen; thus, it is crucial for insurers to have specific policy language that allows them to prepare for the

Policy, 108 AM. JUR. 3D PROOF OF FACTS 351, Westlaw (database updated Sept. 2019) (surveying standards used by courts throughout United States in interpreting insurance policies, and elaborating on importance placed on contractual notion of analyzing "reasonable expectations of the parties" and how this affects courts' holdings and insurance industry's decisions in response).

70. *See* Steven Plitt et al., 2 COUCH ON INSURANCE § 22:38 (3d ed. 2019) (explaining insurance policy "is to be given the meaning which would be attached to the contract by a reasonably intelligent person acquainted with all the operative usages and knowing all of the circumstances existing prior to and at the time of the contract"); *cf.* Larsson, *supra* note 69 (discussing reasonable expectations in insurance policy interpretation).

71. *See, e.g.*, Olin Corp v. Am. Home Assur. Co., 704 F.3d 89, 98 (2d Cir. 2012) (establishing that, "under New York law, insurance policies are interpreted according to general rules of contract interpretation"). This case was cited in the beginning of the analysis in *Medidata Solutions, Inc. v. Federal Insurance Co.*, 268 F. Supp. 3d 471, 476 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018); however, this notion is in accord with the insurance policy interpretation principles of each state, and each state's own adoption of this principle typically is cited as the opening to a court's analysis of an insurance policy when the issue arises. *See id.*

72. *See* McDonald et al., *supra* note 18, at 111 (explaining ISO's influence in creating industry standard forms for different types of policy coverages and the endurance of initial language used in computer fraud policy form issued by ISO); *see also* Julie Davoren, *What Does ISO Stand for in Insurance?*, CHRON, https://smallbusiness.chron.com/iso-stand-insurance-60067.html [https://perma.cc/7WW5-2C72] (last visited Nov. 14, 2019) (explaining that ISO has been leading organization of its kind since its inception in 1971, and is a "principal source of information for insurance companies and provides comprehensive data, technical services, policy language, fraud-identification tools, underwriting, statistical and decision-support services to numerous players such as the federal government, insurance industry regulators, and public- and private-sector customers").

73. *See* Marianne Bonner, *Insurance Services Office (ISO)*, BALANCE SMALL BUS., https://www.thebalancesmb.com/insurance-services-office-iso-462706 [https://perma.cc/J343-JRAB] (last updated May 16, 2019) (noting services and responsibilities offered by ISO and explaining how insurers calculate rates and risk based upon data provided by ISO).

74. *See id.* (discussing prominence and importance of ISO in insurance policy formation).

75. *See id.* (asserting that data and standard policy forms provided by ISO are crucial to most insurers when shaping their own policy forms). As this article explains, "[i]nsurers develop rates *based on projections of future losses*," and many insurers rely on the ISO to provide this risk data in conjunction with the language in their standard forms. *Id.* (emphasis added); *see also* McDonald et al., *supra* note 18 (explaining how insurers' utilization of ISO industry standard forms has affected development of "computer fraud" policy provisions and language contained therein).

scope of losses and to predict how courts will interpret their policy if a claim for coverage arises.[76]

The ISO industry-standard form for "computer fraud" was introduced in 1983.[77] Although it has undergone several changes since its inception thirty-six years ago, it retains language that intends to cover theft carried out by "directly" taking information or funds through computer hacking.[78] Due to the increased risks of technological ubiquity, any changes made to the original policy since its inception have narrowed the scope of coverage "to what is traditional theft . . . not a swindle whereby an insured is duped to depart with its money under a belief."[79] These exceptions are meant to prevent "computer fraud" coverage from becoming a general fraud provision.[80] Therefore, this narrow language employed by the ISO for the "computer fraud" provision further supports the notion that the only losses anticipated by the ISO and insurers were those in which a criminal "breaks into" the computer system.[81]

Because insurers must reasonably anticipate the risks associated with the language implemented in their policy provisions out of fairness to insureds that rely on coverage, courts identify the parties' reasonable expectations when the policy was enacted.[82] Additionally, when interpreting policy language, courts emphasize

---

76. *See* Bonner, *supra* note 73 (noting that insurers view ISO forms as containing risk-predictive language because they have been in use for decades and courts have already interpreted the specific words and phrases within them).

77. *See* McDonald et al., *supra* note 18, at 111 (explaining how insurers utilize ISO industry standard forms has affected development of "computer fraud" policy provisions and language contained therein). For further discussion of the reasonable expectations of parties to an insurance contract and how this affects courts' interpretation of policy language, see *supra* note 69 and accompanying text.

78. *See id.* (explaining ISO's relevant form for computer fraud, "Commercial Crime policy (CR 00 22 05 06)"). The standard form provides a definition for computer fraud which is included in almost every standard policy provision for computer fraud. *See id.* The ISO's form provides the following definition: "'*Computer Fraud*' means '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 (other than a 'messenger') outside those 'premises' or to a place outside those 'premises.'" *Id.* at 111–12 (second emphasis added) (quoting ISO CR 00 07 (10 90)).

79. *See id.* at 111, 113–14 (detailing inception of ISO "computer fraud" standard coverage form). This form has existed since 1983, which is "longer than one would likely think." *Id.* at 111. Although the form has undergone a few changes, "the same general concept first found in the ISO form seems to have survived. The focus is on providing protection for the third-party theft of assets through the use of a computer." *Id.* at 112. The article explains that changes that have been made have focused mostly on excluding employee actions from coverage under the policy, regardless of whether the actions surrounding their involvement in the loss were fraudulent. *See id.* at 112–13.

80. *See, e.g.*, Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am., 656 F. App'x 332 (9th Cir. 2016) (holding computer fraud coverage is limited to hacking incidents through unauthorized entry into computer systems, as parties could not have reasonably anticipated that the provision would cover losses due to authorized entry).

81. *See* McDonald et al., *supra* note 18, at 112 (explaining exclusions included in original standard ISO computer fraud policy which elucidate intent of drafters and reaffirming intent of "direct" loss from a computer to constitute computer hacking).

82. *See generally* Larsson, *supra* note 69 (identifying how courts determine reasonable expectations of parties to an insurance contract); *see also* McDonald et al., *supra* note 18, at 112 (enumerating exclusions for computer fraud contained in original ISO policy). The article notes that the exclusions in the ISO computer fraud policy form are broad, "precluding coverage regardless of the employee's intent and regardless of when the employee acts." McDonald et al.,

insurance policies' unique nature and that both insurers and insureds benefit from cross-jurisdictional uniformity in interpreting similar provisions.[83] With insurers issuing policies containing the same language across state lines and insureds holding policies that apply to differing geographical regions, many courts emphasize a policy argument favoring uniformity in decisions strictly interpreting policy language.[84]

C. *Smooth Sailing: Pre-Circuit Split Decisions Follow Plain Interpretation of Policy Language*

In earlier decisions interpreting whether coverage existed for social engineering fraud under computer fraud insurance provisions, courts generally adhered to reading the plain language of the policy at issue.[85] Prior to courts' recent trend of favoring coverage for insureds after social engineering fraud losses, most courts found that losses were not covered under the plain policy language because the losses either did not constitute computer fraud or the claims were precluded by a policy exclusion.[86] The rationale in prior decisions is displayed by the Fifth, Ninth, and Eleventh Circuits' holdings, which all deny "computer fraud" coverage for social engineering losses.[87]

1. *Shark in the Water: Fifth Circuit First to Address Social Engineering in* Apache

The question of whether social engineering fraud victims can recover under computer fraud insurance provisions first arose in the 2016 decision issued by the Fifth Circuit in *Apache Corp. v. Great American Insurance Co.*[88] In this case, fraudsters used a vendor impersonation scam to induce Apache's employee, through several

supra note 18, at 112. Furthermore, the article notes that the language precludes losses caused by inside parties and "makes clear that coverage is intended to protect against third-party access." *Id.*

83. *See* Apache Corp. v. Great Am. Ins. Co., 662 F. App'x 252, 258 (5th Cir. 2016) (explaining court's policy goal of promoting cross-jurisdictional uniformity for methods of insurance policy interpretation).

84. *See id.* at 255–56 (asserting policy terms requiring that fraud be "direct result" of computer fraud are not ambiguous). As stated by the *Apache* court, "mere disagreement about the meaning of [an insurance policy] does not render it ambiguous," necessitating a plain reading of the language. *Id.* at 255.

85. *See, e.g.*, Taylor & Lieberman v. Fed. Ins. Co., 681 F. App'x 627, 629 (9th Cir. 2017) (holding plain language of "computer fraud" coverage provision did not provide coverage for social engineering fraud losses). In this case, the policy stated that, to trigger computer fraud coverage, the computer fraud must have involved "(1) 'entry into' its computer system, and (2) 'introduction of instructions' that 'propogate[d] themselves' through its computer system." *Id.* (alteration in original). In holding that this language clearly did not include coverage for employee manipulation rather than direct computer system hacking, the court concluded the company's social engineering fraud losses were not covered. *See id.*

86. *See, e.g.*, Tidewater Holdings, Inc. v. Westchester Fire Ins. Co., 389 F. Supp. 3d 920, 923–25 (W.D. Wash. 2019) (holding social engineering losses in which fraudulent supplemental funds transfer was initiated were not covered under "computer fraud" provision). The court believe social engineering losses were precluded by exclusions in the main policy that were subdivided, such that each specific exclusion referenced the policy portion limited by it. *See id.* While this case was issued after the circuit split at issue arose, it exemplifies the rationale instituted in such decisions. *See id.* For further discussion of the pre-circuit split majority view and examples of rationales instituted by courts in these opinions, see *supra* notes 23–27 and accompanying text.

87. For further discussion of the pre-2018 majority view and the key decisions constituting this view, see *supra* note 23–27 and accompanying text.

88. 662 F. App'x 252 (5th Cir. 2016).

phone calls and emails sent from a fraudulent domain, to change the account information of a company vendor.[89] Apache then transferred money to the new account and faced losses totaling $2.4 million.[90] When Apache's insurer, Great American, denied its claim for coverage under the "computer fraud" provision in its policy, Apache brought a claim against Great American.[91]

The Fifth Circuit vacated the district court's finding of coverage for Apache and ruled that Great American did not owe coverage to its insured.[92] In its decision, the court emphasized the goal of attaining cross-jurisdictional uniformity among courts' interpretations of insurance policy provisions.[93] In the Fifth Circuit's view, the mere fact that an email was involved in the chain of events, which ultimately resulted in employees paying legitimate invoices to the wrong bank account, was not enough to trigger coverage under the computer fraud policy provision language.[94]

2. Pestmaster *Proves There Are More Fish in the Sea: Ninth Circuit Decides Another Social Engineering Fraud Claim*

In 2016, the Ninth Circuit issued a similar decision in *Pestmaster Services, Inc. v. Travelers Casualty and Surety Co. of America*.[95] In affirming the lower court's decision, the Ninth Circuit found that Pestmaster's transfer of funds to a payroll company was not covered under its computer fraud policy provision for "fraudulently caus[ing] a transfer" when the payroll company took the money for personal gain without reviewing or completing invoices.[96] The Ninth Circuit found that losses

89. *See* Melissa J. Sachs, *No Coverage for $2.4 Million Transfer to Criminals, 5th Circuit Court Says:* Apache Corp. v. Great American Insurance Co., WESTLAW J. COMP. & INTERNET, Nov. 4, 2016, at 1–2, 2016 WL 6565858 (describing decision in *Apache* and factual scenario underlying case).

90. *See id.* at 2 (explaining losses incurred by *Apache*); *see also Apache*, 662 F. App'x at 259 (explaining court's analysis of events which unfolded in social engineering fraud at issue and found that transfers were not covered under "computer fraud" because Apache's employees authorized the transfers). The court's rationale was that, even though the fraud involved a computer, "the computer-use was but one step in Apache's multi-step, but flawed, process that ended in its making required and authorized, very large invoice-payments, but to a fraudulent bank account." *Apache*, 662 F. App'x at 259. The court also noted the criminals' use of a phone in the scheme, and that their use of a computer to further defraud the company "was in response to Apache's refusing, during the telephone call, to . . . transcribe the change-request." *Id.* Therefore, while the court acknowledged that contacting Apache by email through a computer was successful, the court noted that the transfer occurred "only because, after receiving the email, Apache failed to investigate accurately the new, but fraudulent, information provided to it." *Id.* Apache elected to pay legitimate invoices, but to the wrong bank account; therefore, "the invoices, not the email" caused the losses. *Id.*

91. *Id.* at 254 (stating Apache's claim for coverage due to insurer's denial of coverage for social engineering fraud claim under "computer fraud" provision).

92. *See id.* at 253, 259 (vacating district court decision and finding no coverage for claim at issue).

93. *See id.* (noting interest in maintaining cross-jurisdictional uniformity and declining to extend coverage because the transfer was not directly caused by use of computer).

94. *See id.* at 259 (emphasizing transfer was not caused by computer fraud as covered by policy, but by actions of Apache employees).

95. 656 F. App'x 332 (9th Cir. 2016).

96. *Id.* at 333 (explaining that "Computer Fraud" provision does not cover authorized transactions). The court in *Pestmaster* stated:

> We interpret the phrase "fraudulently cause a transfer" to require an unauthorized transfer of funds. When Priority 1 transferred funds pursuant to authorization from

covered under computer fraud require an unauthorized transfer due to hacking; here, the court found that, although the claims were fraudulent, the use of the system by authorized users did not trigger coverage.[97] As in *Apache*, the Ninth Circuit found that the use of a computer in a scheme was not sufficient to bring the claim into the scope of the computer fraud provision.[98] This decision was echoed two years later when the Ninth Circuit found that a company's social engineering losses due to a vendor impersonation scheme were not covered in *Aqua Star (USA) Corp. v. Travelers Casualty & Surety Co. of America*.[99]

3. *Running a Tight Ship: Eleventh Circuit Solidifies Narrow Interpretation of Computer Fraud Provisions in* Interactive Communications

Only a month after the Ninth Circuit's opinion in *Aqua Star*, the Eleventh Circuit issued a similar opinion in *Interactive Communications International, Inc. v. Great American Insurance Co.*[100] Interactive Communications (InComm) is a company that sells "chits" to consumers, which involves putting money onto reloadable debit cards issued by an external financial institution.[101] Fraudsters, realizing that

---

> 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 Crime Policy into a "General Fraud" Policy. While Travelers 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.

Id.

97. *See id.* (explaining why incident is not covered here and noting broader interpretation of computer fraud converts provision into general fraud policy).

98. *See id.* (explaining why claim is not covered in this case); *see also Apache*, 662 F. App'x at 258 (finding use of computer to be "merely incidental" and fraudulent events not "directly by the computer use").

99. 719 F. App'x 701 (9th Cir. 2018) (holding that an exclusion for input of electronic data by a natural person excluded coverage for social engineering fraud losses). In *Aqua Star*, the court's decision largely hinged on interpretation of an exclusion meant to limit coverage for computer fraud, and held that the exclusion at issue "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'"; therefore, because the employees were authorized to change the information and authorize the four wires, their "conduct fits squarely within the [e]xclusion." *Id.* at 702. The court noted that other exclusions "may also bar coverage," but did not proceed with further analysis of other exclusions. *Id.*

100. 731 F. App'x 929 (11th Cir. 2018).

101. *See id.* at 931–32 (explaining facts giving rise to claim and stating that social engineering fraud losses were not "direct"). When analyzing directness, the court stated:

> What does it mean for a result to follow a cause "directly"? Common-language and legal dictionaries provide a clear (and essentially the same) answer. *Webster's Second*, for instance, defines "direct" to mean "(1) straight; proceeding from one point to another in time or space without deviation or interruption; not crooked or oblique . . . ; (2) Straightforward; going straight to the point . . . ; (3) Immediate; marked by the absence of an intervening agency or influence; making contact or effected without an intermediary[.]" . . .
>
> The theme is unmistakable. In accordance with the term's ordinary meaning, we hold that, for purposes of InComm's policy, one thing results "directly" from another *if it follows straightaway,* immediately, and without any intervention or interruption.

InComm's computerized voice recognition phone system allowed the redemption of one single chit multiple times, initiated duplicate instructions for the financial institution to authorize transfers to debit cards, which caused InComm to incur over $11 million in losses.[102] While the Eleventh Circuit disagreed with the lower court's determination that the fraud did not involve computer use, it affirmed the lower court's holding that the losses incurred did not "result[] directly" from the use of the computer system.[103]

In this determination, the court stated that "one thing results 'directly' from another if it follows straightaway, immediately, and without any intervention or interruption."[104] Because InComm authorized the transfers to the financial institution following the call, the court could not say the losses resulted directly from the use of a computer.[105] By plainly reading the policy language, the court reached an interpretation that matched the underwriters' intent for the coverage provision, namely, to cover only direct theft and to exclude employees' intervening acts.[106] In the years following these decisions, other circuits followed this rationale either by finding that social engineering fraud did not trigger computer fraud coverage or that policy exclusions applied.[107]

Id. at 934 (emphasis added) (citation omitted).

102. *See id.* at 931 (explaining fraudulent activity and noting losses). The court continued its analysis by outlining each step in the social engineering fraud scheme to determine whether the loss resulted "directly" from the use of computers. *Id.* at 934. First, the fraudsters manipulated InComm's system to enable a duplicate chit redemption where, for each redeemed chit, "a fraudster's debit card is immediately credited with purchasing power, but InComm's funds are neither transferred, nor disturbed, nor altered in any way." *Id.* Second, InComm transferred money corresponding to the redeemed chits to a bank account, where the money remained until "needed to cover purchases made on a consumer's debit card." *Id.* Third, the fraudsters used the debit card to make purchases, which incurred a debt from the bank account. *Id.* at 934–35. Fourth, the bank transfers money from the account to the merchant. *Id.* at 935. InComm argued that its losses occurred in the second step when it transferred money to the account; however, the court held:

> *Accordingly, InComm's loss did not occur with the Step-2 transfer of funds to the account held by Bancorp. Rather, the loss did not occur until—at Step 4—Bancorp actually disbursed money from the InComm-earmarked account to pay merchants for purchases made by cardholders.* That was the point at which InComm could not recover its money. That was the point of no return.

Id. at 935 (emphasis added).

103. *See id.* at 933–35 (holding that, although social engineering claim constituted "use of a[] computer" under the policy language, the losses did not result "directly" from computer fraud, as required by policy (alteration in original)).

104. *Id.* at 934 (stating that "if the phrase 'resulting directly' has a 'common signification'—*i.e.*, an ordinary meaning—then we have to find and enforce it"). In its decision, the Eleventh Circuit explained that it is "a fundamental principle of Georgia law—and law more generally—that words in contracts 'generally bear their usual and common signification[.]'" *Id.* at 933–34 (alteration in original) (quoting GA. CODE ANN. § 13-2-2(2) (2019)).

105. *See id.* at 935 (holding employees' presence as intervening act and lack of immediacy precluded claim for coverage because losses were not caused "directly" by computer fraud).

106. *See id.* at 933–35 (explaining rationale for policy interpretation and finding that intent of "direct" in policy language required greater immediacy than indirect causation due to computer fraud).

107. *See generally* Kronstadt, *supra* note 27 (reviewing decisions comprising pre-2018 majority view and discussing courts rationales in making these decisions). While acknowledging that the majority of courts making social engineering fraud coverage determinations under computer fraud provision language have "favored insurers," the author notes that the decisions have an "impact on a company's bottom line." *See id.*

III. SIT DOWN, YOU'RE ROCKING THE BOAT: A CIRCUIT SPLIT EMERGES

The judicial notion that social engineering fraud schemes and the losses incurred by their perpetrators are not covered under insurance provisions for computer fraud was seemingly solidified in courts throughout the United States prior to 2018.[108] Nevertheless, several 2018 decisions issued by the Second and Sixth Circuits turned the tide in the insured's favor.[109] These cases both determined that social engineering fraud schemes were covered under insurance provisions for computer fraud.

A. *A Fish Out of Water: The Second Circuit Decision for Coverage in* Medidata

On July 6, 2018, the Second Circuit decided *Medidata Solutions, Inc. v. Federal Insurance Co.*[110] This case departed from prior decisions in other circuits.[111] In its holding, the Second Circuit broadly interpreted the policy term "direct" in reference to the insured's computer fraud policy provision and found coverage for a social engineering fraud claim.[112] Here, criminals formatted an email to appear as though it was from the corporation's (Medidata's) president to induce a transfer to the fraudsters' account.[113] In affirming the holding issued by the district court, the Second Circuit held that this email was a "violation of the integrity of the computer system," even though the criminals did not directly access Medidata's server to send the email to employees.[114] While the finance department personnel actually transferred the funds, the Second Circuit held that the spoofed emails were the proximate cause of the transfers.[115]

---

108. *See* Schwartz & Willmott, *supra* note 23, at 2 (describing emerging circuit split over coverage determinations for social engineering fraud in light of prior decisions from other circuits).

109. *See generally* Medidata Sols. Inc. v. Fed. Ins. Co., 729 F. App'x 117 (2d Cir. 2018); Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455 (6th Cir. 2018). For further explanation of how these decisions subverted from the pre-2018 consensus, see *infra* notes 110–24 and accompanying text.

110. 729 F. App'x 117 (2d Cir. 2018).

111. *See* Michael S. Levine & Latosha M. Ellis, *Year in Review: Top Insurance Cases of 2018*, WESTLAW J. ENVTL., Feb. 27, 2019, 2019 WL 615838 (discussing Second Circuit's decision in *Medidata* and its potential impact on insurance coverage litigation landscape). In this article, the authors describe *Medidata* as "one of the most closely watched social engineering cases," affirming the lower court's decision to find coverage. *Id.* For further discussion of *Medidata* and the how it diverted from the majority of courts' determinations in finding coverage under a computer fraud policy provision for a social engineering fraud loss, see *supra* note 29 and accompanying text.

112. *See Medidata*, 729 F. App'x at 118–19 (holding that, under de novo review, fraudster changing appearance of email to impersonate high ranking superior in company constituted "violation of the integrity of the computer system" (quoting Universal Am. Corp. v. Nat'l Union Fire Ins. Co. of Pittsburgh, Pa., 37 N.E.3d 78, 81 (N.Y. 2015)). Furthermore, the Second Circuit instituted a proximate cause standard and found that the lower court erred in its determination that coverage for the social engineering fraud claim was improper because the "direct" policy language allowed an instance like this, in which a computer proximately caused the chain of events giving rise to the losses, even though the employees themselves effectuated the transfer. *See id.* at 119.

113. *See id.* at 118 (describing executive impersonation scheme used by criminals).

114. *See id.* at 118–19.

115. *See id.* (explaining proximate cause of losses and holding that "New York law does not have so strict a rule about intervening actors" to find that social engineering losses were not direct loss).

B. *Hook, Line, and Sinker: The Sixth Circuit Reinforces the Trend in* American Tooling

Only one week later on July 13, 2018, the Sixth Circuit Court of Appeals reversed a district court ruling in favor of an insurer in a social engineering fraud claim to find coverage in *American Tooling Center, Inc. v. Travelers Casualty and Surety Co. of America*.[116] In deciding this case, the court weighed in on the circuit split, deciding that a vendor impersonation scam was covered under computer fraud.[117] The Sixth Circuit held that various exclusions, which barred coverage in other jurisdictions, did not preclude coverage for the social engineering fraud scheme.[118]

Although the court acknowledged the paucity of Michigan law dealing with interpretation of "direct," the court adopted the notion that a "direct" loss is one resulting from an "immediate *or* proximate" cause.[119] The court contended that "[i]f [the insurer] had wished to limit the definition of computer fraud . . . it could have done so."[120] Yet, the court quickly dismissed the assertions that several other policy exclusions were the insurer's way of limiting the computer fraud policy.[121]

Despite the tide shifting to find coverage for insureds suffering from social engineering fraud losses under computer fraud provisions, the Ninth Circuit has declined to follow *Medidata* and *American Tooling* in subsequently issued opinions dealing with social engineering fraud.[122] Nevertheless, decisions recently issued in

---

116. 895 F.3d 455 (6th Cir. 2018) (explaining holding of court to find that social engineering fraud scheme fit within policy's computer fraud provision).

117. *See id.* at 465 (holding that social engineering loss "is covered by the Policy and none of the asserted Policy exclusions apply").

118. *See id.* at 463–65 (reversing district court's decision and holding that company suffered "direct loss", scheme constituted computer fraud under policy, and policy exclusions did not apply here even though some policy exclusions had decisively precluded coverage in other circuits). For further discussion of the policy exclusions relevant to *American Tooling* and the court's rationale in holding that the policy exclusions did not apply, see *supra* note 30 and accompanying text.

119. *See Am. Tooling*, 895 F.3d at 460, 463 (emphasis added) (declining to accept insurer's argument in brief that, under established Michigan law applicable to interpretation of word "direct" in context of employee-fidelity bonds, court should apply narrower definition). Although the court acknowledged the scarcity of Michigan law dealing with interpretation of the word "direct," it noted that the insurer supported its brief with a plethora of cases interpreting "direct" in the context of employee-fidelity bonds. *See id.* These cases applied a narrower definition of "direct," and the court posited that the lower court's decision, which granted summary judgment in favor of insureds, is based upon interpretation of "direct" in this precise context. *See id.* Instead, the court cited to an unpublished opinion and instituted the court's definition of "direct" as signaling "immediate" or "proximate." *See id.* at 460 (citing Acorn Inv. Co. v. Mich. Basic Prop. Ins. Ass'n, No. 284234, 2009 WL 2952677, at *2 (Mich. Ct. App. Sept. 15, 2009). The court then concluded that the company "immediately lost its money when it transferred the approximately $834,000 to the impersonator; there was no intervening event." *Id.*

120. *Id.* at 462 (opining that insurer's "attempt to limit the definition of 'Computer Fraud' to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer is not well-founded").

121. For further discussion of the *American Tooling* policy exclusions that the court found were not applicable to preclude coverage, see *supra* note 30 and accompanying text.

122. *See* Tidewater Holdings, Inc. v. Westchester Fire Ins. Co., 389 F. Supp. 3d 920 (W.D. Wash. 2019) (holding social engineering fraud losses not covered under computer fraud policy provisions); *see also* Medidata Sols., Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118–19 (2d Cir. 2018) (holding, unlike the Ninth Circuit, that social engineering losses were covered under "computer fraud" provision); *Am. Tooling*, 895 F.3d at 465 (holding social engineering losses were not precluded by various exclusions to "computer fraud" provision).

district courts indicate a growing preference toward a looser standard in interpreting "computer fraud" provisions.[123] The impact of these decisions, not only upon social engineering fraud losses but also upon interpretation of "direct" language in insurance policies, will become clear as insurers and insureds react to the opinions.[124]

IV. DON'T TAKE THE BAIT: WHY THE TREND TOWARD COVERAGE FOR INSUREDS DOES NOT SOLVE THE ISSUE

Courts should discontinue the current trend toward finding coverage for insureds suffering from social engineering fraud losses under computer fraud policy provisions because the loosened proximate cause analysis in these cases departs from the standard method of insurance policy interpretation.[125] Because social engineering presents an entirely different and more complicated threat, courts should allow insurance companies to provide separate coverage for social engineering.[126] This will allow insurers to appropriately assess the monetary risks of social engineering claims and will allow insureds to be confidently protected against these schemes without legal ambiguity.[127]

Both *Mediata* and *American Tooling* strained to shoehorn social engineering coverage within computer fraud provisions, abandoning precedential methods of insurance policy interpretation.[128] First, the court in *Medidata* interpreted the criminals' spoofing and email formatting to appear as though it was sent from

123. *See generally* Childrens Place, Inc. v. Great Am. Ins. Co., No. 181-1963 (ES) (JAD), 2019 WL 1857118, at *3–4 (D.N.J. Apr. 25, 2019) (denying motion to dismiss due to factual issue of whether hacker's activities could be interpreted as infiltration pursuant to policy language and because denying coverage would produce absurd result). *But see Tidewater Holdings*, 389 F. Supp. 3d at 925 (holding that social engineering losses where fraudulent supplemental funds transfer was initiated were not covered under "computer fraud" provision and were precluded by original exclusions in main policy, which were subdivided so each specific exclusion referenced limited policy portion).

124. *See generally* Joshua Dobiac, *I Came, I Saw, I Underwrote: D & O Liability Insurance's Past Underwriting Practices and Potential Future Directions*, 14 CONN. INS. L.J. 487 (2008) (explaining underwriting process and how underwriters assess risk). Though this article deals particularly with Directors & Officers liability insurance, it provides an excellent explanation of the cycle insurance writers go through to constantly assess risk and update their policies. *See id.* at 495–96. To assess risk and update polices, insurance writers look to court decisions and legal trends to determine the risk factors associated with specific policy provisions. *See id.* at 488–89.

125. *See generally* Park & O'Neill, *supra* note 8 (describing shift in new court decisions that interpret identical policy provisions in different manners). In this article, the authors compare the various pre-*Medidata* decisions, post-*Medidata* decisions, and policy language with each other and continually come to the same conclusion: "court[s] examining similar policy language . . . come to a different conclusion." *Id.* at 8. Therefore, at this point in time, there is an inherent inconsistency in social engineering fraud loss interpretations under computer fraud policy provisions. *See id.* at 4–5 (noting various interpretations of provisions).

126. *See* Bird & Dorvilier, *supra* note 14, at 16 (discussing insurers making social engineering fraud coverage available to insureds). For more information regarding the methods criminals use to carry out social engineering fraud schemes and how they differ from hacking methods, see *supra* notes 38–66.

127. For further discussion of how companies may deem adding social engineering fraud coverage as premature in light of the subject legal trend and therefore avoid creating separate policy provisions, see *infra* note 142 and accompanying text.

128. For further discussion of why these cases diverged from the typical method of narrow insurance policy interpretation, see *infra* notes 129–35 and accompanying text.

Medidata's president to constitute "fraudulent entry of data or deletion of data from a computer system."[129] Despite the fact that this provision clearly denotes direct taking by hacking, the court's finding that merely receiving an email with a deceptive address satisfies this definition demonstrates a misconception of what traditionally constitutes a computer system breach.[130] Even if the fraudsters *had* gained access to the email server to communicate the fraudulent instructions, the monetary losses would *still* not have stemmed directly from this "entry"; instead, this provision contemplates, in light of previously discussed ISO language, the entry or deletion of data which *on its own* causes the loss, rather than an employee completing the process.[131]

Immediately after *Medidata*, the Sixth Circuit held similarly in *American Tooling*.[132] By basing its definition of "direct" upon an unpublished opinion and passing over jurisprudence in Michigan that clearly found "direct" to denote "immediate," the Sixth Circuit broadly interpreted "direct" beyond its plain and common meaning.[133] Furthermore, by opining that "[i]f [the insurer] had wished to limit the definition of computer fraud to [hacking] it could have done so," the Sixth Circuit discounted the history of computer fraud coverage language.[134] Additionally, the court overlooked underwriters' inability to anticipate the recent rise of social engineering; in other

---

129. *See* Medidata Sols., Inc. v. Fed. Ins. Co., 729 F. App'x 117, 118–19 (2d Cir. 2018) (describing method through which criminals changed email format and courts' interpretation of this practice as hacking computer system). Although changing the email format or making it appear a certain way necessarily involves coding, the court categorized this practice as computer hacking in opposition to other courts' decisions. *See id.* In finding that the email spoofing caused a change to Medidata's computer system, the district court elaborated:

> [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*.

Medidata Sols., Inc. v. Fed. Ins. Co., 268 F. Supp. 3d 471, 473 (S.D.N.Y. 2017), *aff'd*, 729 F. App'x 117 (2d Cir. 2018) (emphasis added) (citations omitted). The court therefore equated this "computer code" to change the email format with hacking. *See id.*

130. *Compare* Interactive Commc'ns Int'l, Inc. v. Great Am. Ins. Co., 731 F. App'x 929, 932 (11th Cir. 2018) *with Medidata*, 729 F. App'x at 117. The Eleventh Circuit stated: "[t]he question is whether the fraudsters 'use[d]' both phones and computers to perpetrate their scheme—namely, *using* the phones to manipulate—and thereby *use*—the IVR computers." *Interactive Commc'ns*, 731 F. App'x at 932. Therefore, the Eleventh Circuit, like other courts, found that manipulation of the computer is crucial to a computer fraud claim. *See id.*

131. For further discussion of the ISO and the coverage contemplated in drafting the ISO's standard policy language for "computer fraud," see *supra* notes 73–84 and accompanying text.

132. *See* Am. Tooling Ctr. v. Travelers Cas. & Sur. Co. of Am., 895 F.3d 455, 460 (6th Cir. 2018) (finding American Tooling Center experienced "direct loss"); *cf. Direct*, WEBSTER'S NEW INTERNATIONAL DICTIONARY (2d ed. 1939) (defining "direct" as "marked by the absence of an intervening agency or influence").

133. *See Am. Tooling*, 895 F.3d at 459–61 (explaining "direct" word interpretation); *see also* Acorn Inv. Co. v. Mich. Basic Prop. Ins. Ass'n, No. 284234, 2009 WL 2952677, at *2 (Mich. Ct. App. Sept. 15, 2009) (defining "direct" as "immediate"). For further discussion of "direct" interpretation under its plain and common meaning, see *supra* notes 85–104.

134. *See Am. Tooling*, 895 F.3d at 462 (explaining why policy should be read to include situation at issue). For a further discussion of the history of the computer fraud coverage form and the various exclusions that have been added since its inception to accommodate and specify coverage, see *supra* notes 67–78 and accompanying text.

words, the underwriters could not have anticipated the need to distinguish terms within computer fraud provisions from aspects of social engineering fraud because these risks were not contemplated—or were not sufficiently prevalent to warrant consideration—during the policy's drafting.[135]

Courts must respect the insurance policy's unique nature because there is a strong policy argument for preserving underwriting techniques and respecting the relevant markets available for insurers to create different coverage for distinct types of risks.[136] The insurer's reasonable expectations are largely based on projections and statistics surrounding policy language to determine their risk level.[137] Thus, the recent expansion of terms like "direct," coupled with courts' disregard of clear exclusion language, will make it difficult for insurers to accurately determine rates for coverage as well as fund allocation for riskier provisions.[138]

By keeping social engineering fraud distinct from losses arising directly from a computer, courts will induce underwriters to add separate social engineering fraud coverage to crime and fidelity policies.[139] In turn, companies who want to protect against this type of crime will have the assurance of coverage.[140] Due to the

135. For further discussion of the importance of insurance providers anticipating the risks associated with their policies and how courts evaluate the reasonable expectations of the insurer and insured, see *supra* notes 67–84 and accompanying text.

136. *See generally* Larsson, *supra* note 69 (describing how courts assess reasonable expectations of insurer, especially out of respect for unique nature of insurance market). Although it should not be the policy argument guiding already issued insurance policies, there is a market for insurers to include or give companies the option of social engineering fraud coverage. *See id.* As these losses grow increasingly larger, and arguably could surpass the average loss amounts of those merely from computer fraud due to hacking, insurers should have the right to distinguish computer fraud coverage from social engineering fraud coverage. *See id.* Other commentators argue the trend toward providing coverage for social engineering fraud losses under computer fraud provisions "undermines insurers' interest in uniformity in the meaning of their policy forms." Bird & Dorvilier, *supra* note 14, at 16 (warning insurers may see these newer decisions as reason to "rewrite the computer fraud provisions to explicitly limit coverage to attacks on the insured's computer system itself").

137. For further discussion of how insurers calculate risk and draft policies accordingly, see *supra* notes 67–84 and accompanying text.

138. *See generally* Dobiac, *supra* note 124, at 495 (describing underwriting cycle of assessing risk). The author explains the underwriting cycle and how underwriters assess risk in selecting policy drafting language. *See id.*

139. *See* 18 U.S.C. § 1030 (2018) (displaying preeminence of traditional approach to "computer fraud" as third-party accessing information through hacking, as it does not include activities that could be considered social engineering, and therefore coverage for this would need to be added separately into policies). This federal statute focuses on incriminating fraud and related activity regarding computers. *See id.* The statute's language echoes the pre-2018 majority stance on whether social engineering fraud constitutes computer fraud and gives a definite answer: no. *See id.* In pertinent part, the computer fraud statute forbids one from "knowingly and with intent to defraud, access[ing] a protected computer without authorization;" therefore, the statute would not apply to the authorized transactions involved in social engineering fraud schemes. *Id.* §§ (a)(2)–(4). To constitute federal criminal computer fraud, one must obtain access to a computer without authorization. *See id.* Arguably, in social engineering fraud schemes, the perpetrator's goal is not to access the computer and obtain information independently without the involvement of an employee. *See id.* While this statute is not binding on courts' interpretations of the policy language found in insurance policies, this statute establishes that a common understanding of computer fraud necessitates hacking and does not include social engineering. *See id.*

140. *See id.* § (e)(1) (defining "computer" under statute favorable to insurance policies looking to clarify coverage). The United States Code provides the following definition of

ambiguity created by courts loosening the standards used to interpret insurance policies, these decisions, which seemingly benefit insureds, may ultimately create more harm than good.[141]

V. BIGGER FISH TO FRY: THE POTENTIAL UNFORESEEN IMPACTS OF THE CURRENT TREND TOWARD COVERAGE

Although policy underwriters are adding social engineering fraud provisions to insurers' standard crime and fidelity policies, companies will likely find that adding this coverage to their policies is premature in light of the trending decisions favoring insureds and affording them social engineering coverage under existing computer fraud provisions.[142] Believing themselves to be protected under their current policies, companies may elect to forego additional coverage options that specifically deal with social engineering fraud.[143] Yet, if the claim is litigated in a court that adheres to narrower insurance policy interpretation methods or the social engineering fraud is instigated by phone, fax, or an in-person interaction, the insured will be left defenseless.[144] Furthermore, a lack of legal uniformity for businesses

---

"computer" within the meaning of the statute as it relates to fraudulent criminal activities:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]

Id.; *see also* John R. Felice, *The Computer Crime Coverage Conundrum*, HERMES NETBURN (2013), https://www.hermesnetburn.com/E40D62/assets/files/News/JRF-The%20Computer%20Crime%20Coverage%20Conundrum.pdf [https://perma.cc/4FEK-PEFA] (noting that, because technology is constantly evolving, insureds may not have full coverage under computer fraud provisions). In this paper, the author deals with the problem of identifying what, precisely, constitutes a computer. *See* id. Even if the court agrees with the notion that computer fraud denotes hacking, the author questions whether an employee's hacked smartphone that gives away information or funds to a criminal, for example, constitute computer fraud. *See id.* The author posits that this difficult question will, until insurers more clearly define coverage and distinguish between different types of fraud, "continue to present challenges that can be overcome by the addition of definitions establishing the scope of the coverage provided. Until such time, the arguments for and against finding a covered loss resulting from 'use of a computer' remain as broad as the imagination will allow." *Id.*

141. *See* Bird & Dorvilier, *supra* note 14, at 16 (stating that in response to more lenient coverage decisions, few newer social engineering provisions written by insurers have come with various exclusions and will likely not limit continuance of such claims under provisions for computer fraud). As stated by the authors, due to the circuit split, they "do not foresee the availability of social engineering fraud coverage deterring insureds from making claims for computer fraud coverage." *Id.* at 16. Therefore, coverage under computer fraud policies will remain an important issue until the circuit split is resolved. *See id.* at 17.

142. *See id.* at 16 (explaining impact recent court decisions will likely have on insurance policies). As previously discussed, companies will likely abstain from taking further precautions to insure themselves against these types of losses if they have computer fraud coverage, as the circuit split and trend toward coverage suggests that changing their policy or purchasing extra social engineering coverage may be premature. *See id.*

143. *See* Selarnick et al., *supra* note 35, at 483–84 (noting that, while companies should take precautions, social engineering fraud interpretation under existing policy provisions is developing field of litigation that companies should consider when negotiating policy provisions).

144. For further discussion of cases in which courts found coverage was precluded for social engineering losses under "computer fraud" provisions, see *supra* notes 79–102 and accompanying

working across state lines will make it difficult for companies to select adequate crime and fidelity insurance coverage.[145]

Additionally, cases interpreting the meticulously worded coverage provisions in all types of policies may look at the more lenient decisions and expand coverage beyond the enumerated terms.[146] Courts already have begun to cite these cases and their loosened policy language interpretation in subsequent decisions.[147] While these decisions have and will continue to change the insurance coverage litigation landscape, they especially will affect claims implicating technology.[148] As technology becomes ubiquitous, it is extremely important for courts to extract the nature of the crime or legal action at issue from the technology used.[149] In doing so, insurers will have the freedom to develop and adapt policy language to account for an increasingly virtual world.[150]

---

text.

145. For further discussion of how courts' interpretation of insurance policies affects businesses, see *supra* notes 67–84 and accompanying text.

146. *See* Selarnick et al., *supra* note 35, at 485 (explaining efficient proximate cause doctrine, which applies to losses resulting from both covered and uncovered causes). By expanding "direct" to a proximate cause standard, and without seeking guidance from legal doctrines applying a proximate cause standard in insurance policy provisions, courts bypass rhetorical methods used to comb through murky proximate cause issues; this may now be relevant as insurers may narrow coverage and social engineering losses may be categorized as caused by both a covered and uncovered type of loss. *See id.*

147. *See, e.g.*, Childrens Place, Inc. v. Great Am. Ins. Co., No. 18-11963 (ES) (JAD), 2019 WL 1857118, at *3 (D.N.J. Apr. 25, 2019) (denying motion to dismiss because court found that whether hacker's activities could be interpreted as infiltration pursuant to policy language was factual issue and therefore denying coverage would produce an absurd result).

148. *See* David Hollander, *Position of Influence, Beyond Traditional Roles*, INS. & TECH., Nov. 2012, at 11, https://dsimg.ubm-us.net/envelope/282372/477953/insurance-technology-november-2012-elite-8_2780398.pdf [https://perma.cc/7FKA-9XCN] (stating that "the demand for technology-enabled change throughout the [insurance] business has never been greater").

149. *See* Schmookler & Kahler, *supra* note 7 (questioning whether manipulation of humans, as is carried out through social engineering schemes, constitutes computer fraud). As is detailed in their article, social engineering fraud is nothing new. *See id.* at 4. This extremely general fraud category preys upon human emotions and favors human weaknesses to gain access to information and funds. *See id.* at 5. The article acknowledges that "[t]he growing use of technology-enabled processes exposes a wide variety of businesses to cybercrime[,]" and technology is merely a means of achieving that crime; one example is identity theft. *Id.* at 1. However, the focus should be on the direct nature of these crimes through the computer, as they are extremely different from schemes requiring employee involvement. *See id.* at 40.

150. *See generally* Doug Bonderud, *The Evolution of Technology: From Unusual to Ubiquitous*, PROGRESS (June 20, 2016), https://blog.ipswitch.com/evolution-technology-unusual-ubiquitous [https://perma.cc/R88P-TTWR] (detailing technology's ubiquity in modern life and how this notion will only increase over time).