dri™ The Brief Case: DRI Committee News
May 2023 | Volume 2 Issue 5

Insurance And Information Security Culture: Professional Liability Insurance Coverage Lacking for Social Engineering Attacks Committed by Third Parties

By Brian Bassett and Danielle Kegley

Edited by Allyson L. Moore, Associate at Sulloway & Hollis

It is widely reported that the frequency as well as the costs flowing from social engineering attacks on companies and other organizations are at an all-time high. Who bears these costs? Impacted policyholders that provide professional services may look to their professional liability insurers for coverage of these losses.

Professional liability policies, however, generally only provide coverage for those risks that are inherent in the practice of the insured's professional services. In evaluating coverage for social engineering attacks, professional liability carriers should not only look to the language in their policies' insuring agreements, but exclusions that are frequently found in such policies.

What Are Social Engineering Attacks?

Social engineering attacks typically involve third-party actors trying to "hack" the people within organizations using psychological manipulation and relying on human error to extract confidential information for a big payday. *What is Social Engineering? Attacks and Prevention*, Crowdstrike (Aug. 18, 2022), https://www.crowdstrike.com/cybersecurity-101/social-engineering-attacks/. Phishing, SMSishing, spear phishing, baiting, quid pro quo, pretexting, tailgating—these are all types of social engineering attacks committed by third parties.

These attacks use various media, such as emails, websites, SMS or video to induce individuals to act and disclose confidential information. These often appear to be from an outside entity, such as a bank, delivery or government agency, or from an internal department within the target's own company, such as human resources, information technology or finance. *Id.*

Fraudsters then use confidential information obtained from the attack in order to divert funds from these companies and/or their clients. This article focuses on "phishing" attacks. One example of a "phishing" attack involves the situation wherein a third-party hacks an employee's email account and then sends spoofed emails with fake invoices to the company's clients to divert funds. Once the funds have been diverted, the victim companies are then exposed to claims by their clients, for example, with no opportunity for recovery against the fraudster.

Professional Liability Policies Should Not Cover the Diverted Funds and Associated Costs of Social Engineering Attacks

Professional liability carriers evaluating coverage for claims involving social engineering attacks, like the ones described above, should first consider whether these claims fall within the insuring agreements of the relevant policies by satisfying the definition of "professional services." Insurers should then also evaluate whether such claims are also excluded by theft or misappropriation exclusions.

These Claims Do Not Involve an Insured's "Professional Services"

Courts generally recognize that professional liability policies do not afford coverage where the alleged acts do not arise out of the rendering or failure to render covered professional services. *See*, *e.g.*, 7A John Appleman, Insurance Law & Practice § 4504.01, at 310 (Bender rev. ed. 1979). Thus, the main question is whether there is a wrongful act arising out of the insured company's covered "professional services." In the example of a third-party sending spoofed emails with fake invoices to a company's clients through a hijacked employee's email account, the act at issue (i.e., sending fake invoices to the insured company's clients) arose from an act of a third-party, such that it could not involve the insured company's "professional services."

Circumstances may arise, however, when an insured is sued and faces claims that it acted negligently in preventing the attack. In that scenario, the focus is on whether the negligent act of the insured involved the rendering of its "professional services." *See*, *e.g.*, *Mut. Assurance Adm'rs v. United States Risk Underwriters*, 993 P.2d 795 (Okla. Ct. App. 1999) (finding no coverage because the alleged acts were not of those wrongful acts contemplated by the professional liability policy). As discussed below, insurance companies have a strong argument that such acts do not, in fact, involve an insured's rendering of "professional services."

It is a generally accepted principle of professional liability coverage law that not every action professionals take in the course of providing professional services are "professional services." Rather, an act will only constitute a "professional service" when the professional utilizes his or her professional knowledge, experience, and training in taking some action. *See Gulf Coast Env't Sys., LLC v. Am. Safety Indem. Co.*, No. 4:13-CV-539, 2015 U.S. Dist. LEXIS 75551 (S.D. Tex. June 11, 2015); *First Mercury Ins. Co. v. Shawmut Woodworking & Supply, Inc.*, 48 F. Supp. 3d 158, 174-75 (D. Conn. 2014); *Gen. Ins. Co. of Am. v. City of New York*, No. 04 CIV. 8946 (JCF), 2005 U.S. Dist. LEXIS 35864 (S.D.N.Y. Dec. 23, 2005); *Food Pro Intl., Inc. v. Farmers Ins. Exch.*, 169 Cal. App. 4th 976, 991 (2008); *S.T. Hudson Engineers, Inc. v. Pennsylvania Nat'l Mut. Cas. Co.*, 909 A.2d 1156, 1165–66 (N.J. Super. Ct. App. Div. 2006); *Am. Nat'l Prop. & Cas. Co. v. Select Mgmt. Grp., LLC*, 528 F. Supp. 3d 1188, 1198–99 (N.D. Okla. 2021); *Penn. Nat'l Mut. Cas. Ins. Co. v. Roberts Bros.*, 550 F. Supp. 2d 1295, 1306–08 (S.D. Ala. 2008); *St. Paul Fire & Marine Ins. Co. v. Era Oxford Realty Co. Greystone, LLC*, 572 F.3d 893, 899 (11th Cir. 2009).

Consider, for instance, a law firm facing claims of negligence in failing to prevent an unknown third-party from hacking its email system and providing fraudulent wire transfer instructions to a client. Insureds generally have the burden of proving a policy provides coverage for a claim. Therefore, the law firm in this scenario would need to prove that the deficiencies in its internal security systems leading to the business email compromise involved the professional knowledge, experience, or training of lawyers. Finding that such actions constitute "professional services" would improperly expand professional liability coverage beyond its intended scope and provide coverage for all aspects of an insured's business operations.

Next, contrast that situation to one where there is a physical break in into a law firm's brick and mortar office. During the break in, the attacker replaced an authentic physical check to a client with a fraudulent one. After processing the fraudulent check, the law firm is then sued by a client for negligently permitting the theft to occur and negligently retaining a security company to protect its premises. Under this scenario, it seems a little clearer that the underlying loss would not arise from the performance of "professional services" as a lawyer. Rather, it would arise from the law firm's failures in keeping its premises safe from intruders.

Professional liability policies only provide coverage for claims arising from an insured's "professional services," and are not meant to function as commercial crime or cyber policies, which are expressly designed to respond to such claims. Professional liability policies are also not underwritten to provide coverage for all aspects of an insured's business. Insurance companies, therefore, have a strong argument that coverage does not exist for social engineering attacks under a professional liability policy.

Application of Theft or Misappropriation Exclusions

When evaluating coverage for social engineering claims, professional liability carriers should also consider the application of theft or misappropriation of funds exclusions. Such exclusions typically preclude coverage for claims arising out of the actual or alleged theft, stealing, conversion, commingling, embezzlement or misappropriation of funds or monies.

Recently, courts have enforced these types of exclusions and held that they preclude coverage for theft or misappropriation of funds caused by social engineering schemes or attacks. See *Authentic Title Servs. v. Greenwich Ins. Co.*, No. 18-4131 (KSH) (CLW), 2020 U.S. Dist. LEXIS 215018, at *14–15 (D.N.J. Nov. 17, 2020) (exclusion for any claim "based upon or arising out of . . . the commingling, improper use, theft, stealing, conversion, embezzlement or misappropriation of funds or accounts" barred coverage for a title insurance agent's loss of more than $480,000 after the agent was tricked into sending the funds to a fraudster posing as an employee of a mortgage lender); *Attorneys Liab. Prot. Soc'y, Inc. v. Whittington Law Assocs*. PLLC, 961 F. Supp. 2d 367 (D.N.H 2013) (exclusion for claims arising out of "[a]ny conversion, misappropriation or improper commingling by an person of client or trust account funds or property" precluded

coverage for an underlying loss against an insured law firm due to a Nigerian check scam in which the insured was fraudulently induced to deposit a check into the insured's bank account and then wire the majority of the funds to a foreign bank); *Landmark Am. Ins. Co. v. Esters*, No. 2:20-CV-1263, 2022 U.S. Dist. LEXIS 97119, at *14 (W.D. La. May 3, 2022) (exclusion for "commingling, conversion, misappropriation or defalcation of funds or other property, or the inability or failure to pay, collect, disburse, or safeguard any funds held by an Insured" applied to "theft claims" but not to "non-theft claims" alleged); *Res. Real Estate Servs., LLC v. Evanston Ins. Co.*, No. CV GLR-16-168, 2017 WL 660800, at *1 (D. Md. Feb. 17, 2017) (exclusion for claims "arising out of any actual or alleged conversion, misappropriation, commingling, defalcation, theft, disappearance, [or] insufficiency in the amount of escrow funds, monies, monetary proceeds, funds or property, or any other assets, securities, negotiable instruments or any other thing of value" precluded coverage for a scheme perpetrated by a fraudster that hacked into the email account of the insured's client).

It is important for insurers to review the specific language of theft exclusions. Some exclusions may only apply to theft committed by "an insured," whereas other exclusions may apply to theft committed "by any person," including third parties. Some provisions are silent as to who must have committed the theft for the exclusion to apply. *See ABL Title Ins. Agency, LLC v. Maxum Indem. Co.*, No. 15-7534 (CCC), 2022 U.S. Dist. LEXIS 61391 (D.N.J. Mar. 31, 2022). Where the exclusion is silent as to the applicable actor, insurers have an argument that these exclusions include acts committed by both the insured and by third parties, based on other exclusions in the policies that include language confining their application to acts "by the insured." *See id.*

For instance, in *ABL Title Ins.*, the exclusion at issue provided that there was no coverage for claims based upon or arising out of commingling, conversion, misappropriation, or defalcation of funds or other property. Id. The court agreed with the insurer that the exclusion directly addressed the factual scenario where funds were wired to third-party scammers who had no entitlement or right to the funds, and therefore engaged in an act of conversion under New Jersey law when it defrauded the title agency. *Id.* at *12–13. The title agency sought coverage for claims made by the parties whose checks from the title agency had bounced or whose payments could not be made because the title agency had insufficient funds in its escrow account to cover the disbursements. *Id.* The court, therefore, held that the exclusion applied to preclude coverage, even though it was not the insured who committed the conversion. *Id.*

Insurers will have the burden to prove that these exclusions apply, such that they will need to establish a causal relationship between the claims asserted against their insureds and the alleged or actual theft or misappropriation of funds in order to disclaim coverage to their insureds on this basis.

As discussed above, the purpose of social engineering is to divert funds from a company or its clients through the extraction of confidential information. Thus, it would follow

that theft or misappropriation exclusions exclude such claims from coverage under professional liability policies.

Practical Application

Professional liability policies are not designed to provide coverage to policyholders for social engineering schemes, as evidenced by the language in their insuring agreements and exclusions. That does not mean that professionals cannot procure insurance to cover these claims. There are many standalone polices or endorsements available to organization that are specifically tailored to respond to these kinds of social engineering matters. As social engineering schemes persist, courts will continue to address these issues in the context of professional liability policies and other liability policies. For now, courts have sided with professional liability carriers in denying coverage for these claims.

Brian Bassett is a partner and Danielle Kegley is an associate in Traub Lieberman's Chicago office. Brian and Danielle focus their practice on litigating and managing insurance coverage disputes involving several lines of insurance across jurisdictions nationwide. Brian is the Vice Chair of the Professional Liability SLG of the DRI Insurance Law Committee. Danielle recently became a member of DRI and is excited to become more involved with the DRI community.