Further Clarity Regarding Coverage for Funds Transfer Fraud

By Alex Cogbill and Jane Warring

At this point, your IT department has almost certainly warned you to approach your e-mail inbox with skepticism--for good reason. Cybercriminals regularly and effectively impersonate our legitimate contacts for illegitimate gain. They may be targeting your servers and systems—through attacks like malware, ransomware, viruses, and hacking—or they may just be targeting you to authorize transmission of your company's data and money without ever infiltrating your computer. This distinction between manipulating computer systems and manipulating people is an important one. Your IT department has comparatively fewer tools to prevent you from being manipulated (sometimes called social engineering). Education is the best—and, perhaps, only—protection against social engineering attacks. As cyber insurers attempt to align coverages and policy limits to the risks inherent to each industry and each insured, the risk of social engineering remains difficult to measure. For this reason, coverages for this risk are sometimes limited.

Given this limited coverage for social engineering schemes, insureds often claim that social engineering risks come within coverages written to insure risks of computer system manipulation. Courts responding to these arguments in the context of disputed claims have taken divergent approaches with respect to this legal question. For example, a circuit split in the federal courts has developed in deciding whether social engineering triggers coverage for "[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property.".[1] Some circuits interpret this language to apply only where bad actors gain control over an insured's computers, while others have employed a chain-of-causation analysis with differing results. This split introduces uncertainty for insureds and insurers alike when social engineering claims arise under policies containing this "Computer Fraud" provision.

In contrast, there is consistent series of cases holding that the "Computer and Funds Transfer Fraud" provision—which appears in the ISO Computer Fraud form—does not extend to social engineering. *Abraham Linc Corp. v. Spinnaker Ins. Co*. [2] from the Northern District of West Virginia provides a notable example of this emerging trend. In that case, the policyholder's cyber policy contained both a $2,000,000 Computer and Funds Transfer Fraud Endorsement and a $100,000 Social Engineering Incident Endorsement. The insured suffered losses in excess of the $100,000 Social Engineering Incident sublimit and sought coverage under both provisions.

The Computer and Funds Transfer Fraud Endorsement at issue in that case provided coverage for "Loss resulting directly from a fraudulent entry of electronic data… in… a computer system, by a person or organization without authorization to access such computer system"[3] or "Loss resulting

[1] https://www.zellelaw.com/Conflicts_in_Circuits_Approach_to_Email_Scams_Hold_Lessons

[2] 1:23-cv-98, 2024 WL 3433661 (N.D. West Virginia July 16, 2024).

[3] **i.** **Loss** resulting directly from a fraudulent:
1. Entry of **Electronic Data or Computer System** into; or
2. Change of **Electronic Data or Computer System** within

from an electronic debit…. which purports to come from the insured, but which was in fact fraudulently issued by someone else without your knowledge or consent." This coverage was focused, therefore, on the consequences of a breach of the insured's systems rather than losses arising out of the actions of authorized employees. In contrast, the Social Engineering coverage applied to the "intentional misleading of an insured to transfer money to a person… resulting from [an authorized] employee's good faith reliance upon an instruction transmitted via e-mail purporting to be from a natural person or entity… under contract [with the insured]."[4]

In that case, the policyholder was a flooring distributer who regularly purchased materials from a supplier in Changzhou, China. The supplier was hacked. Using the supplier's e-mail account, the hackers repeatedly e-mailed the insured regarding legitimate, outstanding invoices. Once the insured engaged, the hackers convinced the insured to wire the money into the hackers' bank account. Various employees interacted with these fraudulent e-mails and, believing they were

---

a **Computer System,** by a person or organization without authorization to access such **Computer System,** provided the fraudulent entry or fraudulent change causes, with regard to Paragraphs **a.i.(1)** and **a.i.(2):**

a. **Your** money, securities or other property to be transferred, paid or delivered; or

b. Your account at a financial institution to be debited or deleted, or

ii. **Loss** resulting directly from a **Fraudulent Instruction** directing a financial institution to debit your **Transfer Account** and transfer, pay or deliver money or securities from that account ...

In the context of this coverage, the Policy defined Fraudulent Instruction to mean:

> **(a)** A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic instruction directing a financial institution to debit Your **Transfer Account** and to transfer, pay or deliver money or securities from that **Transfer Account,** which instruction purports to have been issued by You, but which in fact was fraudulently issued by someone else without Your knowledge or consent.
> **(b)** A written instruction issued to a financial institution directing the financial institution to debit Your **Transfer Account** and to transfer, pay or delivery money or securities from that **Transfer Account,** through an electronic funds transfer system at specified times or under specified conditions, which instruction purports to have been issued by You, but which in fact was issued, forged or altered by someone else without your knowledge or consent.
> (c) A computer, telegraphic, cable, teletype, telefacsimile, telephone or other electronic or written instruction initially received by You, which instruction purports to have been issued by an **Employee,** but which in act was fraudulently issued by someone else without Your or the **Employee's** knowledge or consent.

4 [T]he intentional misleading of an **Insured** to transfer **Money** to a person, place or account beyond the **Named Insured's** control resulting directly from the **Named Insured's** employee's good faith reliance upon an instruction transmitted via email, purporting to be from:

i. a natural person or entity who exchanges, or is under contract to exchange, goods or services with the **Named Insured** for a fee (other than a financial institution, asset manager, broker-dealer, armored motor vehicle "named insured" or any similar entity); or

ii. an employee of the **Named Insured;**

but which contained a fraudulent and material misrepresentation and was sent by an imposter. As a condition precedent to coverage, the **Insured's** established and documented verification procedure must have been followed before acting upon such instruction.

legitimate, transferred "substantial sums" via ACH transfer to the bank account provided. By the time they caught the mistake, the funds could not be recovered.

Consistent with holdings from the District of Minnesota[5] and Southern District of Indiana[6], the court in *Abraham Linc* concluded that social engineering alone did not trigger the Computer and Funds Transfer Fraud Endorsement. This is because the endorsement requires access to the insured's computers "without authorization" or a "fraudulent instruction" to the insured's bank. The court reasoned that the hackers did not gain unauthorized access to the insured's system. Rather, employees with authority authorized transfers using the hacker's wire instructions provided by e-mail. The hackers neither infiltrated computers nor initiated unauthorized bank transfers using that access.

The policyholder's primary counterargument was that the hacker's scheme resulted in transfers it would not have authorized and involved manipulated data. But this argument failed under a close reading of the clause. The only unauthorized access was to the *supplier's* e-mail system, not the policyholder's computer system. The provision required "unauthorized access" to the policyholder's systems. Not only did the hackers fail to gain unauthorized access, they never "fraudulent[ly] entered electronic data" into the policyholder's computer system. Rather, the bad actors convinced the policyholder's employees to act on their behalf. The court observed that a more expansive interpretation of that provision would "turn [the cyber policy] into a general fraud policy."

As to the Social Engineering Endorsement, the court recognized that the provision might apply but requested discovery on whether the insured met a condition precedent to comply with its verification procedures. Whereas the Social Engineering coverage premised coverage on the insured following "established and documented verification procedure," the policyholder had no documented procedure or protocol. Rather, the policyholder insisted that its employees acted consistent with "unwritten protocol" by communicating with the bad actor via e-mail and contended that calls were impractical because the vendor worked in a different time zone. The insurer argued that the absence of a protocol violated the condition precedent, and the policyholder argued that the insurer tacitly approved the lack of protocol by binding the risk.

The case settled a few months after the court's ruling on the Computer and Funds Transfer Fraud provision. Hopefully, this ruling and others will provide more certainty around these coverages and reduce the need for litigation.

Increasingly, sophisticated social engineering schemes are a reality for businesses and their cyber insurers. And until businesses implement robust verification procedures and employees heed IT's trainings, social engineering losses will remain a significant risk. Consistent caselaw on fraudulent transfer and social engineering provisions will serve both insurers and insureds.

---

[5] *Interstate Removal, LLC v. National Specialty Ins. Co*., 2024 WL 1332006 (D.Minn. Mar. 28 2024)

[6] City of Aurora, Indiana v. National Fire & Cas. Co., 2023 WL 8113605 (S.D. Ind. Nov. 21, 2023)