SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Insurance Coverage for Cyber Deception and Social Engineering

Vincent J. Vitkowsky

New York Connecticut New Jersey

SEIGER GFELLER LAURIE LLP
ATTORNEYS AT LAW

Insurance Coverage for Cyber Deception and Social Engineering

Vincent J. Vitkowsky

Businesses are facing an endless stream of attempted and often successful deceptive funds transfers. Although insureds instinctively think of these as "cyber losses," they have not been covered by most cyber insurance policies. Rather, they most often involve interpretation of Commercial Crime Policies and Financial Institution Bonds.

There are at least seven potential scenarios for deceptive funds transfers:

1) The transfer is effected entirely by a hacker independently penetrating a computer system, and making the transfer;
2) The hack and transfer are enabled by employee negligence;
3) The fraudster convinces an employee to reveal credentials, enters the network by using them, and then transfers funds;
4) The fraudster gets an employee to open an attachment or click on a link, thereby allowing the network to be penetrated, and allowing the transfer of funds;
5) The fraudster, through emails or telephone calls or both, posing as a company's executives, vendors or customers, convinces an employee to transfer funds;
6) An employee enters data believed to be accurate, but which in fact is fraudulent; and
7) A rogue employee makes an improper transfer or enters fraudulent data.

Numbers 3, 4 and 5 are variants of methods which have come to be known as "social engineering," a term for the manipulation of humans into performing acts or divulging confidential information.

Commercial Crime Policies are often broadened to cover some deceptive funds transfers, typically by insuring agreements or endorsements for Computer Fraud and Funds Transfer Fraud.

The application of Computer Fraud and Funds Transfer Fraud coverages to deceptive funds transfers involving computers has arisen in several recent cases, and courts have reached various rsults. The main issues have been whether the policy applies to activities of authorized users or only to activities of outside hackers, and whether there is causation when the deception involves multiple elements, such as emails, telephone calls, and employee acts or negligence.

Recent Decisions

Authorized User Analysis

Universal American Corp v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA*,* 25 N.Y. 3d 675 (2015). The New York Court of Appeals (New York's highest court) held that there was no coverage under a Financial Institutions Bond for losses arising when healthcare providers who were allowed to submit claims directly into the computer system of a health insurer (the insured) submitted over $18 million in fraudulent claims. The Bond excluded "losses resulting directly or indirectly from fraudulent instruments which are used as source documentation in the preparation of Electronic Data, or manually keyed into a data terminal." The Court found that the Bond provided coverage for losses incurred through unauthorized access to the computer system, *i.e.,* deceitful and dishonest acts of outside hackers, but not to fraudulent information entered by authorized users.

Pestmaster Services Inc. v. Travelers Cas. and Surety Co. of America, 2016 WL 4056068 (9th Cir. July 29, 2016). Applying California law, the court affirmed a district court holding that there was no coverage for lost funds transferred by the insured to a payroll company that failed to remit the portion representing payroll taxes to the IRS. It found that neither the Computer Fraud nor the Funds Transfer Fraud insuring agreements applies where the transfer is made by an employee who was an authorized user of the system. Also, "[B]ecause computers are used in almost every business transaction, reading [the Computer Fraud] 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."

Causation Analysis

Apache Corp. v. Great American Ins. Co., 2015 WL 7709584 (S.D.Tex. Aug. 7, 2015). The court found coverage for a social engineering induced transfer of funds under a Crime Protection Policy which insured against "loss . . . resulting directly from the use of any computer to fraudulently cause a transfer of [money] from inside the premises." The insured was duped by a telephone call, a follow-up email, and then a "verifying" telephone call, all involving a fraudster claiming to be a vendor. It was defrauded into sending payments to a new bank account. The court ruled that under Texas Law, the phrase "resulting directly from" is synonymous with a "cause in fact," which in turn means "a substantial factor in bringing about the injuries." The court found that without the email, the harm would not have occurred, so it was a substantial factor. It rejected the argument that only fraud perpetrated through a direct "hacking" would be covered. This case is on appeal to the Fifth Circuit.

Aqua Star (USA) Corp. v. Travelers Cas. And Surety Co. of America, 2016 WL 3655265 (W.D. Wa. July 8, 2016). This court found no coverage under a very similar scenario, this time involving a hack of a vendor of shrimp. The hacker directed the vendor's customer, a seafood importer, to change the bank account to which it made wire transfer payments. An employee of the importer did this and the company lost $713,890. The court applied an exclusion providing that the Policy "will not apply to loss resulting directly or indirectly from the input of Electronic Data by a natural person having the authority to enter the Insured's Computer System." It found that the actions of an authorized employee in effecting the wire transfers were an indirect cause of the loss, so coverage was barred. The case is on appeal to the Ninth Circuit.

The State Bank of Bellingham v. BancInsure, Inc., 2016 WL 2943161 (8th Cir. May 20, 2016). The court found coverage under a Financial Institution Bond when a hacker broke into a network and performed fraudulent wire transfers, notwithstanding that the hack was enabled by employee negligence. Employees left computers on overnight with tokens still inserted, giving access to the Federal Reserve's FedLine Advantage Plus system. Applying Minnesota law and the concurrent causation doctrine, the court held that the "efficient and proximate cause" of the loss was the transfer by the hacker, not the negligence of the employees.

Principle Solutions Group, LLC v. Ironshore Indemnity, Inc, 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016). This case found coverage when an employee of the insured transferred $1.7 million as a result of a scheme in which a fraudster posing as an executive sent an email to the employee instructing her to make the transfer, but the specifics as to where to wire the funds were provided in a subsequent telephone call. The insurer argued that because of the intervening telephone call and the company employee's actions in setting up and approving the transfer, the loss was not covered. The policy provided coverage for loss "resulting directly from a 'fraudulent instruction' directing a 'financial institution' to debit [the insured's] 'transfer account' and transfer pay, or deliver 'money' or 'securities' from that account." The court found that this provision was ambiguous and should be construed in favor of the insured.

(cont'd next page)

Pending Cases

There are many other cases pending in the courts. Here is a sampling of some of the more interesting ones.

Medidata Solutions, Inc. v. Federal Ins. Co., No. 1:15-cv-00907 (S.D.N.Y., filed February 6, 2015). This case involves a claim for a social engineering induced funds transfer under a Crime Policy providing coverage for "the unlawful taking or fraudulently induced transfer of money . . . resulting from a Computer Violation." "Computer Violation" is defined as "the fraudulent entry of data into . . . a Computer System" and "change to data elements or program logic of a computer system." The insurer denied coverage on the grounds that there was a voluntary transfer by authorized users. It says its policy only covers manipulation or unauthorized entry into a computer system, and involuntary transfers effected by hackers, forgers or impostors. In March 2016, the court denied cross-motions for summary judgment, and granted leave to conduct expert discovery. The discovery is "to be limited to establishing the method in which the perpetrator sent its emails to [Medidata] and discussing what changes, if any, were made to [Medidata's] computer systems when the emails were received." If the case proceeds to a further decision, it could be an important precedent.

***Ameriforge Group, Inc. v. Federal Ins. Co.*,** No. 16-cv-377 (S.D. Tex, filed February 12, 2016.) A fraudster posing as a company's CEO sent an email to an employee directing the transfer of $480,000 to a Chinese bank. The Crime Policy contained the same language as in *Medidata*. The insurer denied coverage on the grounds that (i) the Forgery coverage in the policy does not extend to fraudulently signed emails, (ii) the Computer Fraud coverage only applies to a direct hack, and (iii) the Funds Transfer coverage does not extend to funds knowingly transferred, even if induced by fraud.

BitPay, Inc. v. Massachusetts Bay Ins. Co., No. 1:15-cv-03238 (N.D. Ga. Filed Sept. 15, 2015.) The CFO of a Bitcoin payment processor was duped into providing his credentials to a hacker pretending to be a journalist for the publication yBitcoin. This allowed the hacker to make fraudulent transfers of Bitcoin from the processor. The insurer denied on the grounds that the policy only provides coverage for a direct hack into the insured's system. Here, it was the hack into another system (yBitcoin's system) that allowed the hacker to impersonate a journalist, which ultimately led to the transfer.

InComm Holdings Inc. v. Great American Ins. Co., No. 1:15-cv-02671 (N.D. Ga. filed July 28, 2015). This case presents a unique factual background. The insured is a provider of prepaid cards and payment networks. It suffered $11 million in losses when customers were able to dial into its computer system simultaneously and re-use chits to obtain duplicate deposits onto reloadable debit cards. It sought coverage under the Computer Fraud portion of its Crime Policy. The insurer denied on the grounds that the losses were caused by a programming error, not "the use of any computer." The

insurer also argues that the loss resulted from more than 25,000 separate acts, none of which met the per-occurrence deductible.

Maxum Indemnity Co. v. Long Beach Escrow Corp., No. 2:16-CV-05907 (C.D. Ca. filed Aug. 8, 2016). This is a case under a Professional Liability Policy. Hackers gained control of the email account of a manager of a real estate company, and by email directed the company's escrow agent to make 3 transfers totaling over $250,000. The insurer denied coverage based upon a Funds Exclusion (barring coverage for "damages arising out of . . . misappropriation or defalcation of funds"), and the Fiduciary Duty Exclusion.

Industry Reaction

Some Crime insurers now offer Crime Policies that expressly provide coverage for various deceptive funds transfers, including those effected through social engineering. They tend to be subject to sub-limits, frequently $250,000.

Also, an increasing number of ***cyber*** insurers now expressly provide coverage for some of these risks. According to The Betterley Report's June 2016 Cyber/Privacy Insurance Market Survey, of 31 cyber insurers surveyed, 13 offer some coverage for various types of deceptive funds transfers. Coverage is most often afforded with sub-limits of $250,000, although some insurers have sub-limits of $500,000 or $1,000,000, and possibly more, "subject to underwriting."

An important distinction is that Crime Policies do not provide coverage for theft or loss of data. In contrast, cyber insurers provide coverage for first-party expenses from theft or loss of data. And also unlike Crime Policies, some Cyber Policies also provide coverage for the loss of a customer's proprietary business information that the insured was contractually obligated to protect.

In conclusion, cyber deception and social engineering losses provide a fertile ground for dispute within the context of a rapidly-evolving insurance market. They will continue to present coverage issues for resolution by the courts.

September 2016

Vince Vitkowsky is a partner at Seiger Gfeller Laurie LLP, resident in New York. He serves insurance and reinsurance companies in litigation, counselling, and product development in many lines of business, including cyber, E&O, D&O and CGL insurance. Vince created a Cybersecurity Podcast and Symposium Series featuring leading cyber experts, consultants, present and former government officials, and journalists. Over the years, he has been included in various directories of leading lawyers, including Chambers America's Leading Lawyers for Business (describing him, among other ways, as "a well-prepared operator") and Euromoney's Best of the Best. He can be reached at vvitkowsky@sgllawgroup.com. More information on the firm can be found at www.sgllawgroup.com.