COMPUTER FRAUD AND FUNDS TRANSFER FRAUD COVERAGES

John J. McDonald, Jr.
Joel T. Wiegert
Jason W. Glasgow

I.
INTRODUCTION

Over the last twenty years electronic commerce has gone from novelty, to convenience, to necessity. Quite simply, in today's world a financial institution or business cannot compete without the ability to conduct transactions electronically and, even more so, without the ability to relay that convenience to its customers. Face-to-face transactions have long given way to a click of the mouse and instant credits or debits to the customer's account that can be viewed in real-time.

But the necessary convenience also gives rise to new risks. Although the risk of on-premises fraud will always exist, from the defalcator's perspective the possibility of achieving the same goal without having to be seen is proving to carry with it an allure difficult to resist. Furthermore, the prospect of being able to swindle much larger amounts by simply entering instructions from a computer carries an obvious incentive as well. Although one is by no means completely invisible behind a computer screen, the concept is certainly proving to be empowering and providing many otherwise innocuous individuals with the confidence to act in ways they likely would never undertake were they required to personally appear before their victim.

This is not to say computer theft is risk-free. Quite the contrary, many times the trail can be easier to follow than that of the clever

John J. McDonald, Jr. is a partner, and Joel T. Wiegert is an associate, with Meagher & Geer, PLLP in Minneapolis, Minnesota. Jason W. Glasgow is Claim Counsel with Travelers Bond and Financial Products in Hartford, Connecticut.

identity thief appearing on the insured's premises. But the mechanisms allowing forensic computer technicians to follow the trail is not the subject of this paper. Just as the methods of catching the thief evolve, so do the methods of the thief; consequently, so must the coverage available to the insured. Just as with any risk, the difficulty is in allocating those parts of the risk that should be maintained by the insured and those parts that are accepted by the insurer.

In light of the phenomenal boom in electronic transactions, it goes without saying that computer-related fraud is a growing concern to even the smallest businesses and banks. Computer crimes present real risks, and the stakes are high to any business when, ultimately, a thief can access its entire portfolio with the touch of buttons. The threats of theft are far greater than the "on premises robbery" or "safe burglary." With a set of stolen wire transfer instructions, a foreign bank account, and telephone, email or fax transfer instructions, a thief can make off with millions in virtually an instant, all from the comfort of his or her own home. With the right equipment, the thief can be somewhat confident that he or she will have sufficient time to make a "get-away" before the theft is even discovered.

That the ability to act covertly carries with it the power to act grandly is evidenced by the recent statistics regarding the prevalence of computer crime. In 2007, United States companies responding to a CSI Computer Crime and Security Survey reported that average annual losses from computer crime more than doubled from $168,000 reported in 2006 to $305,424 in 2007.[1] Notably, according to this report, financial fraud overtook virus attacks as the source of the greatest financial loss to the responding companies in 2007.[2]

The insurance industry has "responded" to this new sophisticated set of risks with two interrelated additions to the crime coverage: the Computer Fraud and Funds Transfer Fraud Insuring Agreements.[3] The

[1] Computer Security Institute, *2007 CSI Computer Crime and Security Survey, available at* http://www.gocsi.com/index.html.

[2] *See id.*

[3] Hereinafter Agreements. In light of the time such coverages have actually been available, one could argue that the industry did not "respond" to the risks, but rather "foresaw" them.

objective of this paper is to examine these relatively modern additions; distinguish between the two, often intertwined Agreements; and annotate the few decisions and how courts have interpreted the Agreements in recent cases.

II.
THE COVERAGE PROVIDED

A. The Computer Fraud Coverage Insuring Agreement

The ISO Computer Fraud Coverage Form (Form F) has been around longer than one would likely think. First appearing in 1983, the coverage has gone through a number of revisions to its present form. The coverage is granted in the traditional sense, in that it identifies what property is to be covered in light of the specific cause of loss and then incorporates the exclusions, definitions, and conditions specific to its coverage in addition to those found in the main body of the crime policy. The coverage provided is as follows:

> **A. Coverage –** We will pay for loss of and loss from damage to Covered Property resulting directly from the Covered Cause of Loss.
>
> **1. Covered Property:** "Money," "Securities" and "Property Other Than Money and Securities."
>
> **2. Covered Cause of Loss:** "Computer Fraud."[4]

The additional definitions place the coverage into context, and, most notably, "computer fraud" is itself defined as follows:

> **"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

[4] ISO CR 00 07 (10 90) (Form F).

> (other than a "messenger") outside those "premises" or to a place outside those "premises."[5]

The standard coverage includes two additional exclusions to the Crime General Provisions: Acts of Employees, Directors, Trustees or Representatives and Inventory Shortages. The Inventory Shortages exclusion is self-explanatory and similar to the traditional exclusion that precludes a loss for which the proof of such is dependent on an inventory or profit and loss computation. The more pertinent of the initial exclusions is the first, which precludes coverage for loss resulting directly from any dishonest or criminal acts committed by what could be referred to as an "inside" party, such as an employee, director, trustee, or authorized representative of the insured, whether acting alone or in collusion with other persons, ***or*** while performing services for the insured or otherwise.

The exclusion is fairly characterized as broad, precluding coverage regardless of the employee's intent and regardless of when the employee acts. The disjunctive context of the exclusion makes clear that there is no coverage for the situation, for example, where an employee, in the wee hours of the morning, is able to commit the dishonest act from the comfort of his own home due to his knowledge of various passwords and other encrypted and protected information. By precluding losses involving "inside" parties, the exclusion makes clear that coverage is intended to protect against third-party access.[6]

More recently, the market seems to have gone towards an insurer-specific form of coverage with respect to computer fraud. The risk has presented insurers with the opportunity to address their insured's needs through niche endorsements that depend on the insured's particular business. However, 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. For example, one such coverage currently available provides the following:

---

[5] "Premises" itself is defined to mean "the interior of that portion of any building you occupy in conducting your business."

[6] The exclusion is discussed in more detail below in Section III.C.1.

> 1. Computer Fraud. We will pay you for your direct loss of, or your direct loss from damage to, Money, Securities, and Other Property directly caused by Computer Fraud.

The definition provides that "Computer Fraud" means "[t]he use of any computer to fraudulently cause a transfer of Money, Securities, or Other Property from inside the Premises or Banking Premises:

> 1. to a person (other than a Messenger) outside the Premises or Banking Premises; or
>
> 2. to a place outside the Premises or Banking Premises."

Similar to the ISO form, the Employee Acts exclusion does not include the Computer Fraud Insuring Agreement as an exception.

Although the general concept behind the original coverage remains, the more recent policies have obviously been refined to limit the scope of coverage due to the ever-evolving scope of risk. The limitation has been primarily confined to the exclusions that apply to the coverage grant. For example, most modern policies contain an exclusion precluding coverage for loss due to the giving or surrendering of covered property in any purchase or exchange, whether legitimate or fraudulent.[7] Thus, there is no coverage for loss of property that the insured gives up in connection with a fraudulent sale transaction or exchange that involves the computer. If the insured voluntarily pays a vendor, for example, for goods and services provided by making electronic payments to the vendor's bank accounts through instructions that had been fraudulently modified, there is likely no coverage available. This is because the exclusion makes clear that it does not matter whether the insured may have been fraudulently induced to depart with its money, as long as the insured does so in connection with a purchase or exchange, there is no coverage. The coverage is designed to limit its application to what is the traditional theft—but off-premises—not a swindle whereby the insured is

[7] Some policies, however, limit the application of this exclusion to those transactions with a party not in collusion with an Employee.

duped to depart with its money under the belief of a legitimate transaction.

Another exclusion that is often relevant in the context of Computer Fraud coverage precludes coverage for loss resulting directly or indirectly from the input of "Electronic Data" by someone having the authority to enter the insured's computer system. The pertinent issue with respect to this exclusion is understanding the scope of what is identified as "electronic data." Electronic data generally includes those facts or information converted to a form that the computer system can utilize in performing its function. In other words, it is the data, not the program. As such, the exclusion does not preclude coverage for loss resulting from someone altering the computer program, but it does preclude coverage for loss resulting from someone entering incorrect or fraudulent data that does not allow the computer program to accurately perform its function.

Finally, another of the more relevant exclusions (there are others) makes clear that the extent of coverage applies only to the loss of covered property—most often money—and does not include intangible property or confidential information. Many policies will specifically identify "electronic data" and "computer programs" as falling within the scope of the exclusion. The intent behind this exclusion is to limit coverage to that which can be readily quantified, as valuating the data or program itself can often be a difficult assessment. The information can usually be replaced for a value much less than the value (and dependence) the insured places on it. Other property coverages may encompass this risk, but the crime coverage does not.

B. The Funds Transfer Fraud Insuring Agreement

The Funds Transfer Fraud Coverage is usually written as a direct corollary to the Computer Fraud coverage. It may be added to the crime policy in the same endorsement; however, the two coverages are distinct and protect against separate risks. A typical example of the coverage afforded by the Funds Transfer Fraud coverage in today's market is as follows:

> **Funds Transfer Fraud:** We will pay you for your direct loss of Money and Securities contained in your

Transfer Account on deposit at a Financial Institution directly caused by Funds Transfer Fraud.

"Funds Transfer Fraud" means:

1. an electronic, telegraphic, cable, teletype or telephone instruction fraudulently transmitted to a Financial Institution directing such institution to debit your Transfer Account and to transfer, pay or deliver Money or Securities from your Transfer Account which instruction purports to have been transmitted by you, but was in fact fraudulently transmitted by someone other than you without your knowledge or consent;

2. a fraudulent written instruction, other than one covered under Insuring Agreement B., issued to a Financial Institution directing such Financial Institution to debit a Transfer Account and to transfer, pay or deliver Money or Securities from such Transfer Account by use of an electronic funds transfer system at specified intervals or under specified conditions which written instruction purports to have been issued by you but was in fact fraudulently issued, Forged or altered by someone other than you without your knowledge or consent; or

3. an electronic, telegraphic, cable, teletype, telefacsimile, telephone or written instruction initially received by you which purports to have been transmitted by an Employee, but which was in fact fraudulently transmitted by someone else without your or the Employee's consent.

While the Computer Fraud Coverage Insuring Agreement and the Funds Transfer Fraud Insuring Agreement are similar (so much so they have sometimes been combined into one insuring agreement), they obviously differ in the risks they cover. The Funds Transfer Fraud Insuring Agreement was intended to provide coverage to losses caused

by fraudulent written, telephonic, or teletype instructions, mirroring the way business was transacted before computers became ubiquitous. Once computers started being used not just in banking but also in business as well, such that they controlled the flow of not only money but also securities and inventory, a new insuring agreement was necessary. Thus, the two insuring agreements are not intended to cover the same loss—indeed, the ISO policy is structured such that the two are mutually exclusive. Exclusion 4.b. provides that Insuring Agreement A.6 (Computer Fraud) does not cover loss resulting from a "fraudulent instruction" directing a financial institution to transfer, pay or deliver "funds" from your "transfer account." Similarly, Exclusion 5 states that Insuring Agreement A.7 (Funds Transfer Fraud) does not cover loss resulting from the use of any computer to fraudulently cause a transfer of "money," "securities," or "other property."

Exclusion 4.b. mentioned above begs the question of what is a transfer account. "Transfer account" is a defined term in the ISO form of the Commercial Crime policy (CR 00 21 05 06): an account maintained by the insured at a financial institution from which the insured can initiate the transfer, payment, or delivery of "funds":

> a. By means of electronic, telegraphic, cable, teletype, telefacsimile or telephone instructions communicated directly through an electronic funds transfer system; or
>
> b. By means of written instructions (other than those described in Insuring Agreement A.2.) establishing the conditions under which such transfers are to be initiated by such financial institution through an electronic funds transfer system.

This raises the question as to whether there are any standard accounts in today's business world that are not a transfer account under this definition. It is an important inquiry, as a fraudulent instruction to transfer money from a company's bank account is unlikely to be covered under the Computer Fraud coverage of the ISO form due to the simple fact that the loss was probably from a transfer account. "Transfer account" is defined in other forms as an account the insured maintains at

a Financial Institution from which the insured "can initiate the transfer, payment or delivery of Money or Securities." Thus, specifying the means by which the transfer can be made appears to be a limitation in the breadth of what may qualify as a "transfer account."

Another notable difference is what the coverages apply to. While the Computer Fraud Coverage generally encompasses "Money, Securities, and Other Property," the Funds Transfer Fraud Coverage is generally limited to the loss of "Money or Securities," or in some policies, "funds." The limitation with respect to what the Funds Transfer Fraud coverage applies is necessary in light of the fact that the coverage itself is limited to theft from the insured's "Transfer Account" maintained at a Financial Institution. Obviously, what is held in that account is likely limited to "funds" or "Money or Securities," and, as such, the distinction is merely a more practical one. Furthermore, the "other property" in the Computer Fraud coverage encompasses inventory, which may be fraudulently accessed through the computer system.

III.
APPLICATION OF THE COMPUTER FRAUD AND FUNDS TRANSFER FRAUD COVERAGES

There is a surprising dearth of cases—and, more so, reported cases—addressing the application of the Computer Fraud or Funds Transfer Fraud Coverages. However, the cases available provide good discussions of the issues relevant to the coverage. With respect to the Computer Fraud Coverage, *Brightpoint, Inc. v. Zurich American Insurance Co.*[8] identifies several issues that often arise in the context of that coverage. With regard to the Funds Transfer Fraud Coverage, the limited cases provide insight into the common coverage issues as well. Each is discussed below.

A. The Computer Fraud Insuring Agreement

Brightpoint, Inc. v. Zurich American Insurance Co. involved the theft of nearly $1.5 million through a scam involving prepaid telephone cards. The insurer provided coverage under a Commercial Crime Policy

[8] No. 1:04-CV-2085, 2006 WL 693377 (S.D. Ind. Mar. 10, 2006).

that included coverage very similar to the ISO Standard Coverage Form F. The insured sought coverage, arguing that the computer fraud was carried out by a fraudulent facsimile purchase order.[9]

The insured's subsidiary was a wholesale distributor of prepaid mobile telephone cards. As was its customary practice, the insured received a facsimiled purchase order from one of its regular prepaid phone card dealers. Along with the faxed purchase order, the insured would accept a post-dated check from the dealer and, in addition, would require the dealer to provide a bank guarantee certifying the sufficiency of the funds in the dealer's account and committing the bank to honoring the post-dated check when it was presented on the maturity date. The dealer normally sent copies of the post-dated checks, guaranties, and purchase orders to the insured by facsimile. The insured would then purchase the phone cards from a telecom company and deliver them to the dealer in exchange for the original check, guaranty, and purchase order.[10]

On two occasions the insured received, by facsimile, purchase orders, post-dated checks, and guaranties thought to be from the dealer. After receiving the faxed orders, the insured sent a representative to the telecom company from which it purchased the phone cards to be distributed to the dealer. Literally, after leaving the telecom company's building, the insured's representative then met with a known employee of the dealer who had, in fact, been present at previous exchanges. The dealer's purported employee delivered to the insured the original copy of the post-dated check and bank guarantee in exchange for the $1.5 million worth of prepaid phone cards.[11]

A few days after the exchange, the dealer met with the insured to advise that it had not authorized issuing the purchase order, denied authorizing the bank to issue the guaranties, and denied authorizing its employee to pick up the cards. Ultimately, the phone cards were never recovered, and the insured never received payment for the stolen cards. The insured claimed a loss under the Computer Fraud/Wire Transfer insuring agreement, contending that the facsimile constituted the use of a

[9] *Id.* at *1.
[10] *Id.* at *2.
[11] *Id.*

computer. The insurer denied coverage, maintaining a computer was not used to fraudulently cause a transfer of the phone cards.[12] On summary judgment the insurer set forth several defenses in support of its coverage denial, each of which is worth discussing below.

1. Ownership Requirement

The insurer's first defense to coverage was that the phone cards were not the insured's property at the time it received the fraudulent facsimile.[13] The general conditions of the crime policy required that "covered property" be property that the insured owns or holds, or for which the insured is legally liable. Because the insured did not acquire the phone cards until after it received the fraudulent purchase order, the insurer argued they were not the insured's property. The court did not agree with this distinction and held the ownership requirement was satisfied because the insured clearly owned the property at the time the cards were turned over to the defrauding party.[14] Thus, it was ownership at the time of departing with the property, as opposed to ownership at the time the scheme was initiated, that the court held was dispositive to the ownership requirement.

2. "Covered Property"

The insurer also argued that the phone cards were not "covered property," as defined by the policy.[15] Obviously the phone cards were not "Money" or "Securities." But the insurer claimed that the cards also could not be considered under the third category: "Property Other than Money and Securities." The insurer's position was based on its argument that the loss resulted only from the economic value attached to the phone cards and not the cards themselves. Therefore, the phone cards could not be considered "tangible" property.

The court agreed that, to fall under the "Property Other than Money and Securities" category, the property must be "tangible." The

[12] *Id.* at *3. However, this defense was not developed in the summary judgment motion.

[13] *Id.* at *4.

[14] *Id.* at *5.

[15] *Id.* at *5.

court also recognized that the property must have "intrinsic value" and not be any property specifically excluded by the policy.[16] But finding the holding (to the contrary) in ***People's Telephone Co., Inc. v. Hartford Fire Insurance Co.***,[17] unpersuasive, the court held that the phone cards were tangible because they could be physically transferred.[18] In addition, the court held that the cards had an intrinsic value because each had a specific value attached to it.[19] Therefore, the court held that the stolen prepaid telephone cards did qualify as "covered property" under the policy.

3. "Premises"

Next the insurer asserted that the theft of the phone cards was not covered under the policy because the phone cards were not transferred from inside the "premises" or "banking premises," as required under the policy definition of "Computer Fraud." "Premises" was defined as "the interior of that portion of any building you occupy in conducting your business."[20] On this issue, the court had "no problem" agreeing with the insurer's position.

The insured argued that the definition of "premises" should be interpreted broadly to include any location where one of its employees carries out the company's interests. For example, even though the transactions in this case did not take place at the insured's offices, it argued that both the office of the telecom company from which it purchased the phone cards to be distributed and the location where the phone cards were actually exchanged should be covered as a "premises" because they were places the insured's employees conducted business.[21]

---

[16] *Id.*

[17] F. Supp. 2d 1335 (S.D. Fla. 1995). The United States District Court for the Southern District of Florida had held telephone cards were not tangible property, but the stolen property in that case was lists of combinations of electronic serial numbers and identification numbers that were used to program "clone" phones.

[18] *Brightpoint, Inc*., 2006 WL 693377, at *6.

[19] *Id.*

[20] *Id.*

[21] *Id.*

Unsurprisingly, the court adopted a narrower view of the "premises" concept, limiting its application to the context of the policy definition and holding that only the places that the insured *occupies* in conducting its business is included in the definition. The court held that the term "occupy" necessitated a narrow interpretation of the term "premises" because it could not find that an insured "occupied" any building where its employee happened to be pursuing some interest of the company. Applying the relevant rules of contract interpretation, the court found that the limitation on coverage to property transferred out of the insured's premises (or its bank's) would be made meaningless by adopting the insured's broad interpretation. As a result, because the phone cards were never inside an office building occupied by the insured, the loss did not result from a transfer from "inside the premises or banking premises" as required by the policy. The court, therefore, agreed with the insurer's denial of coverage on this aspect.[22]

4. "Directly Caused by Computer Fraud"

Finally, the insurer focused on the direct loss requirement and contended that the facsimile transmission did not "fraudulently cause a transfer" of the phone cards, as required under the "Computer Fraud" definition.[23] Rather, the insurer argued that the fraudulent facsimile simply alerted the insured to the fact the dealer, or someone purporting to be the dealer, wished to place the order. Indeed, based on the insured's established practices, it would not have exchanged the phone cards simply on the basis of the facsimile itself. It was only after the insured received the physical documents that it would release the cards. Therefore, the insurer argued, the fraud was carried out through the use of unauthorized checks and guaranties and was not directly or proximately caused by the use of the facsimile machine, much less a computer.[24]

---

[22] *Id.*

[23] *Id.* at *7.

[24] *Id.* A seemingly threshold issue presented in *Brightpoint* was whether the facsimile machine itself was a "computer" for purposes of the policy. However, the insurer did not address the issue in the summary judgment motion. The court did take note, however, and addressed it in a footnote. The issue is discussed under Section III.D.1.

On the other hand, the insured argued that the policy only required that the theft follow and be directly related to the use of a computer. Moreover, the insured argued that the policy did not contain a modifier such as "proximate cause," "predominate cause," or the like. Accordingly, the insured argued all that was required by the policy is the use of a computer followed by a theft that is in some way connected to that initial use of the computer.[25]

The court rejected the insured's interpretation of the term "directly related" and found that the insured's loss did not flow immediately from the use of the facsimile machine. Rather, the court held that intervening events or circumstances became the direct, proximate, predominate, and immediate cause of the insured's loss.[26] Consequently, the court held that this was another ground for which the insurer was justified in denying coverage under the Computer Fraud policy.

B. The Funds Transfer Fraud Insuring Agreement

Several cases have addressed the availability of coverage under the Funds Transfer Fraud Coverage Insuring Agreement. Each of the two discussed below raises issues unique to the coverage.

1. *Northside Bank v. American Casualty Company of Reading*

In *Northside Bank v. American Casualty Company of Reading*,[27] the insured opened an account for its client-merchant pursuant to a merchant services agreement. Pursuant to the agreement the client-merchant would accept orders for merchandise by debit and credit card payments. Upon receipt of electronically transmitted debit and credit card authorizations from the client-merchant, the insured would then transfer money into the client-merchant's account. However, it turned out that the client-merchant never actually delivered the purchased merchandise to its customers. When the client-merchant's customers exercised their rights under federal law to rescind their debit and credit

[25] *Id.*

[26] *Id.*

[27] No. GD 97-19482, 2001 WL 34090139 (Pa. Commw. Pl. Jan. 10, 2001).

card payments for the undelivered goods, the creditors refused to pay, or charged back the amounts they had paid to, the insured. When the insured similarly attempted to charge back the client-merchant's account, it discovered that the account had been completely depleted.[28]

The insured sought coverage under its financial institution bond for what it deemed to be fraudulent electronic fund transfers and computer crimes. The insured argued that the loss should be covered because the submission from the client-merchant was an electronic instruction and the subsequent failure to ship the merchandise should be viewed as a "modification" or "alteration" of the electronic instruction with the intent to deceive.[29]

Although the insured argued "modified or altered" was ambiguous, the court held that the insured was trying to "place a square peg in a round hole."[30] The electronic instructions sent from the client-merchant were never modified or altered but were paid according to the intended instruction. In what is proving to be an encouraging pattern with respect to the decisions involving these coverages, the court, in affirming the denial of coverage under the Bond, found the insured's claim to be at odds with the "obvious intent of the insurance policy."[31]

Viewing the policy as a whole, the court found that the purpose of the Electronic Funds Transfers and Computer Crime coverages was to protect the insured from someone breaking into the electronic funds transfer system and pretending to be an authorized representative or altering the electronic instructions to divert monies from the rightful recipient.[32] To the contrary, the funds transfer instructions at issue in

---

[28] *Id.* at *96.

[29] *Id.* at *101. The definition of "fraudulent electronic instruction or advice"—to which both the Electronic Funds Transfers and Computer Crime coverages referred—involved two subparts: when someone other than a customer defrauded the insured; and when an electronic instruction or advice was "modified or altered with intent to deceive after being sent by another financial institution or automated clearing house or by a customer of the insured." *Id*.

[30] *Id*. at *101.

[31] *Id.*

[32] *Id.* at *101-102.

Northside Bank, whether fraudulent or not, were sent directly from the client-merchant to the bank unaltered. Therefore, the court agreed that this was not the type of risk that was contemplated by the coverage.

2. *Morgan Stanley Dean Witter & Co. v. Chubb Group of Insurance Cos.*

Morgan Stanley Dean Witter & Co. v. Chubb Group of Insurance Cos.[33] involved the issue of whether coverage was available under an Electronic and Computer Crime Policy for fraudulent telephone-initiated funds transfers. Morgan Stanley sought indemnification for over $21 million it paid to defend and settle a lawsuit which stemmed from the fraudulent actions of one of its customers, London and Bishopsgate International.[34]

Morgan Stanley had agreed to provide custodial services for property owned or held by London/Bishopsgate. According to the written custodial services agreement between them, Morgan Stanley was to be responsive to instructions from London/Bishopsgate, which could come from several specifically authorized persons. In order to facilitate the instructions, Morgan Stanley provided London/Bishopsgate with computer software allowing access to Morgan Stanley's computer programs.[35]

London/Bishopsgate later entered into an investment management contract with First Tokyo Index Trust Limited (First Tokyo), allowing London/Bishopgate to manage First Tokyo's investments. To facilitate the management of First Tokyo's investments, London/Bishopsgate opened an account with Morgan Stanley, which was subject to the custodial services agreement between the two parties.[36]

Two years later, the company owning the controlling share of London/Bishopsgate made a public offer to purchase First Tokyo. Once the offer became unconditional, the purchasing company requested that

---

[33] No. L-2928-01, 2005 WL 3242234 (N.J. Super. Ct. App. Div. Dec. 2, 2005)

[34] *Id.* at *1. Hereinafter London/Bishopsgate.

[35] *Id*.

[36] *Id.*

there be no changes to First Tokyo's securities portfolio without its consent. As such, First Tokyo ordered London/Bishopsgate to cease all trading on its behalf; however, Morgan Stanley was not informed that London/Bishopsgate was no longer authorized to trade for First Tokyo.[37]

Despite the lack of authority, London/Bishopsgate later instructed Morgan Stanley to liquidate the bulk of First Tokyo's portfolio through several transactions; and the sale proceeds were delivered to London/Bishopsgate-affiliated accounts. The transactions were accomplished through instructions sent by computer, fax, and voice to Morgan Stanley by persons who were specifically authorized by London/Bishopsgate.[38]

Morgan Stanley did have coverage under its crime policy for loss as a result of fraudulent instructions communicated by voice, fax, and computer. After settling the claim First Tokyo made against it, Morgan Stanley argued that its loss was covered by those insuring agreements, covering "computer systems," "customer voice initiated transfers," and "facsimile transfer instructions."[39]

The court held that there was no coverage under the fraudulent facsimile transfer instruction agreement. The facsimile insuring agreement was recognized to limit coverage to situations "where an unauthorized person poses as a customer or other authorized person to issue the fraudulent transfer instructions."[40] As the instructions at issue had been made by persons authorized to act for London/Bishopsgate, they were not "imposters," as the court referred to them.[41] Consequently, the failure to satisfy this requirement precluded coverage.

With respect to the "computer systems" insuring agreement, the court held that there was no coverage because any such coverage otherwise available was excluded. The applicable exclusion precluded coverage for "loss by reason of the input of Electronic Data at an authorized electronic terminal…or a Customer Communication System

[37] *Id.*
[38] *Id.* at *2.
[39] *Id.*
[40] *Id*. at *3.
[41] *Id.*

by a customer or other person who had authorized access to the customer's authentication mechanism."[42] The court held this exclusion also unambiguously excluded coverage for fraud committed by customers or other authorized persons. Again, there was no dispute that the fraudulent instructions were made by authorized employees of London/Bishopsgate, but Morgan Stanley tried to argue that London/Bishopsgate was not a customer. Citing the custodial agreement, the court dismissed this argument and held there was no "computer systems" coverage.[43]

However, the court held the "customer voice initiated transfers" agreement was not as limited as the others. Contrary to the lower court, the appeals court found the voice initiated transfer agreement was not limited to "imposters or hackers."[44] Rather, this agreement covered voice transfer instructions that:

> [1] fraudulently purport to have been made by a person authorized and appointed by a Customer to request by telephone the transfer of such funds but which instructions were not made by said Customer or by any officer, director, partner or employee of said Customer or [2] were fraudulently made by an officer, director, partner or employee of said Customer whose duty, responsibility or authority did not permit him to make, initiate, authorize, validate or authenticate customer voice initiated funds transfer instructions.[45]

The insurers first argued that coverage was limited to the transfer of "funds" and, therefore, did not include securities. "Funds" was not defined in the policy, and the court held the concept was ambiguous and could be more broadly interpreted to include assets other than money.[46] The insurers also contended the agreement, like the other coverages, was limited to "imposter or hacker" coverage. The court interpreted the insurers' position regarding the scope of the agreement as one conceding

---

[42] *Id.*
[43] *Id.*
[44] *Id*. at *4.
[45] *Id*.
[46] *Id*.

ambiguity. Nonetheless, the court found there was no ambiguity with respect to the second provision and held the voice initiated transfer agreement covered the losses attributed to the transactions made by telephone because, when the London/Bishopsgate employees issued the telephone instructions, they were no longer authorized by First Tokyo to do so. Thus, it became a matter of exceeding authority, and, therefore, the court held that there was coverage.[47]

C. Common Exclusions To The Computer Fraud And Funds Transfer Fraud Insuring Agreements

Three common exclusions applicable to the Computer Fraud and Funds Transfer Fraud Coverages have been recently addressed by courts. Encouragingly, the court, in each case relying on an exclusion, applied a plain and ordinary interpretation of the intent of the exclusion in the context of the coverage provided.

1. The dishonest acts of Employees or Authorized Representatives

In *Milwaukee Area Technical College v. Frontier Adjusters of Milwaukee*,[48] the insured sought coverage under its crime policy when it sustained a loss of $1.6 million after the owner of a firm the insured had retained to process its workers' compensation claims defrauded it. The wrongdoer was able to steal the money by telling the insured that he had sent checks to health-care providers when, in fact, he had merely kept them.[49] He then created dummy check ledgers that seemed to support that the checks had been issued and sent the dummy ledger to the insured. The insured would then send a reimbursement check to the wrongdoer, which check he would then steal.[50]

The insured sought coverage under the "Forgery or Alteration" and "Computer Fraud and Funds Transfer Fraud" coverages in its crime

[47] *Id.* at *5.

[48] Nos. 2007AP1549, 2007 AP1918, 2008 WL 1787682 (Wis. Ct. App. Apr. 22, 2008).

[49] *Id*. at *4.

[50] *Id.*

policy.[51] The insured argued that the Computer Fraud subpart[52] was triggered because the wrongdoer used a computer to print the dummy ledgers he sent to the insured when seeking reimbursement[53] and also because he had used a computer to manage his company's bank account into which he deposited the reimbursement checks and those he stole.[54]

Although the court undertook the effort to incorporate every definition in the Computer Fraud coverage, it held an in-depth analysis of the coverage was unnecessary because the dishonesty exclusion "blocked" any coverage at its inception.[55] Recognizing the exclusion included dishonest acts by authorized representatives, the court held there was no dispute the wrongdoer and his company were authorized representatives in connection with managing the workers' compensation claims that gave rise to the theft. Although the insured attempted to argue the act could not have been authorized and, as such, it could not have authorized the wrongdoer to steal from it, the court rejected this argument as it rendered the entire exclusion inutile.[56] Refusing to find the exclusion ambiguous, the court held there was no coverage otherwise available.

The insured also tried to argue the exclusion should not apply because it was intended to merely prevent a double recovery for the insured. This argument was premised on the insured's reference that the fidelity coverage provided for loss caused by employee theft.[57] But because the wrongdoer was not an employee, the court discarded this argument as well. This highlights a potential gap in coverage (one that is often addressed through an endorsement) for loss caused by an authorized representative as opposed to by the employee. Absent an endorsement, if an authorized individual who is not an employee causes the loss, there is no coverage under the policy; whereas, if the loss is

[51] *Id*. at *9.

[52] The insured only sought coverage under the "Computer Fraud" subpart of the coverage.

[53] The ledgers had been printed using a standard accounting software program. *Id*. at *4.

[54] *Id*. at *10.

[55] *Id*.

[56] *Id.* at *11.

[57] *Id*. at *12.

caused by an employee, coverage may still be available under the fidelity coverage.

2. Proprietary Information, Trade Secrets, Confidential Processing Methods and other Confidential Information of any Kind

In *Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, PA,*[58] the insured discovered there had been unauthorized access and theft of customer data on its retail and corporate computer systems. Consequently, the insured paid the cost of several resulting obligations, including re-issuing credit cards to the customer, monitoring the customer credit cards for fraudulent usage, and hiring additional staff to undertake these tasks.[59] Additionally, the insured faced costs in connection with a suit brought by the Ohio Attorney General and suits brought by customers in several other states.[60] The insurer denied the claim under a Computer Fraud Insurance Policy because the policy specifically excluded coverage for "proprietary information, Trade Secrets, Confidential Processing Methods or other confidential information of any kind."[61]

Unfortunately, the decisions with regard to this case pertain to the motion to dismiss (which was denied in *Retail Ventures, Inc. I*) and the insured's motion to compel discovery (which was denied in part and granted in part in *Retail Ventures, Inc. II*). Neither decision specifically addressed whether the insurer's reliance on the proprietary information exclusion was warranted and precluded coverage. However, the reliance on the exclusion does demonstrate its real-world application, and further illustrates that significant portions of losses may be excluded under the breadth of this exclusion.

---

[58] No. 2:06-CV-443, 2007 WL 3376831, at *1 (S.D. Ohio Nov. 8, 2007) (hereinafter "*Retail Ventures, Inc. II*").

[59] *Id.* at *1.

[60] Retail Ventures, Inc. v. Nat'l Union Fire Ins. Co. of Pittsburgh, PA, No. 2:06-CV-443, 2007 WL 943011, at *1 (S.D. Ohio Mar. 27, 2007) (hereinafter "*Retail Ventures, Inc. I*").

[61] *See Retail Ventures, Inc. II*, at *2 n.2.

3. The "Giving or surrendering of Money or Securities in any exchange or purchase"

In *Harrah's Entertainment, Inc. v. Ace American Insurance Co.*,[62] the casino extended gambling credit to its patron after he presented what turned out to be two fraudulent cashier's checks. Whether through luck or skill, the gambler lost $1,461,800 in a matter of hours and cashed out with $38,200 from the casino before his scam was discovered. The casino filed a claim under its blanket crime policy, arguing that the loss was covered by the "Loss Inside the Premises Coverage."[63] Under the language of this agreement, coverage was available for:

> Loss of Money and Securities by the actual destruction, disappearance, wrongful abstraction [or] Funds Transfer Fraud thereof within or from the Premises, Banking Premises or similar recognized places of safe deposit.[64]

The insured claimed that its loss at issue was the result of a "wrongful abstraction." Although the fraud did not constitute "funds transfer fraud," the denial of coverage rested on a particular policy exclusion that was also applicable to the funds transfer fraud provision in the same insuring agreement is therefore relevant here. The exclusion precluded coverage due to "the giving or surrendering of Money or Securities in any exchange or purchase."[65] Applying the exclusion, the court recognized that the insured gave or surrendered gambling credit, which it held constituted "Money or Securities" under the policy.[66]

The insured attempted to argue that the exclusion applied on a much narrower level and was intended to be limited to situations involving a salesperson undercharging a purchase, making incorrect change, or giving an unwarranted refund.[67] As such, the insured argued that the exclusion is limited to salesperson error. The court declined to accept the insured's argument for two reasons, the first of which is the

---

[62] No. 02-6519, 2004 WL 1193958, at *1 (6th Cir. May 27, 2004).
[63] *Id*. Incidentally, the insured, Harrah's, drafted the policy.
[64] *Id.*
[65] *Id.*
[66] *Id*. at *2.
[67] *Id.*

more important. The court held the insured's interpretation did not account for the "natural and ordinary meaning" of the exclusion, which excluded coverage for any "giving or surrendering of Money or Securities in any exchange or purpose."[68] Because the casino had readily handed over the $1.5 million gambling credit in exchange for a fraudulent cashier's check, the exclusion applied.[69]

This exclusion has potential application in a number of similar scenarios. It is akin to the loan-loss exclusion that appears in the Financial Institution Bond in that it often specifically includes the situation where the exchange or purchase (or, as in the loan-loss exclusion, the loan) is procured through fraud. Thus, it is of no import how the insured was duped into departing with its money: as long as it was through a purchase or transaction, there will be no coverage available. The intent behind the exclusion is similar to that of the loan-loss exclusion. The insurer is not providing credit insurance, and the absence of the exclusion would essentially transform the coverage into such by guaranteeing the credit in any transaction.

D. Other common issues

1. What is a computer?

One of the most basic issues with regard to Computer Fraud coverage is what qualifies as a "computer." Most insuring agreements do not include a policy definition for "computer." As a result, it is not clear how broadly the term "computer" is interpreted. Although the issue has been raised in other contexts, it remains, for the most part,

[68] *Id*. at *3.

[69] *Id.* The second point the court cited in rejecting the insured's interpretation was that, at best, the insured had raised an argument that the exclusion was ambiguous. As such, the court was obligated to construe the ambiguity against the drafter—which was the insured. In light of this fact, the court's first and primary point was essential. The court did *not* hold the provision was ambiguous; it merely noted that *at best* that is what the insured could have hoped to establish. The fact the court held the insured's interpretation did not account for the natural and ordinary meaning makes clear it was not a reasonable interpretation susceptible to an ambiguity argument. *Harrah's* does not provide support that the exclusion is ambiguous.

unaddressed by courts interpreting coverage under Computer Fraud policies.

The exception in the context of Computer Fraud coverage is *Brightpoint*. In that case, the insured claimed that the fraudulent use of a facsimile machine constituted the use of a computer for purposes of its Computer Fraud policy.[70] In fact, the insured provided an expert opinion that a facsimile machine is a "computer" for purposes of the policy. Although the insurer addressed the issue in its coverage denial letter, it chose to abandon the defense at summary judgment. The court, however, noted in a footnote that it did not agree with the insured's expert. Although it did not explicitly decide the question, the court opined that that the common and ordinary meaning of "computer," as used and understood in our society and around the world, would be stretched too far by including the use of a facsimile machine.[71] That is the extent of the court's analysis on the issue.

Decisions examining the statutory definition of "computer" in cases under computer crime statutes may prove enlightening. For example, accessing a telephone "voice mailbox" did constitute the use of a computer when the user gained access to the mailbox to change the password.[72] It was the manipulation of data that violated the statute, not the mere use of the telephone.[73] Similarly, the submission of fraudulent unemployment compensation claims to Colorado's automated phone system was held to be sufficient to establish that the defendant had "accessed" a computer or computer system under the state's computer crime statute.[74] In that case, the court explained that, although the defendant used a telephone, she accessed a computer system and

[70] 2006 WL 693377 at *7 n.5.

[71] *Id.*

[72] Commonwealth v. Gerulis, 616 A.2d 686, 693 (Pa. Super. Ct. 1992). The voice mailbox had been created by a computer, and messages in the mailbox were stored on computer disks.

[73] *Id.* at 691-93.

[74] People v. Rice, No. 05CA0931, 2008 WL 2053490, at *4 (Colo. Ct. App. May 15, 2008).

provided fraudulent information to the computer system, rather than to an actual person.[75]

However, the cases are not consistent in this regard. In New Mexico a court held that placing telephone calls—which prosecutors argued fell within the statutory definition of "computer" because the long distances calls were processed by various computerized switches that were controlled by computers—did not constitute a computer or computer network because the defendant was not manipulating the computer technology and was providing the fraudulent information directly to the victims of the fraud.[76] The court held that the technology was simply a passive conduit through which the defendant's criminal activity passed.[77] This more common sense reasoning should be applied to argue that sending a fraudulent communication through the use of a facsimile does not constitute the use of a computer for purposes of the Computer Fraud insuring agreement. The facsimile does not manipulate a computer system nor does it provide the fraudulent information directly to the computer system; rather, the machine is merely the passive conduit through which the communication reaches an actual person. On the other hand, when the wrongdoer is able to manipulate the computer itself—whether through instructions, programs, or other—to effectuate a fraud, it is apparent the computer was beyond a mere conduit, but the facilitation of the fraud. A direct loss analysis should prevent successful arguments based on the reasoning presented in the contrary computer crime cases.

2. What is "theft directly related to the use of a computer"?

This transitions into the next step of any analysis involving a computer fraud claim—to what extent must the use of a computer be involved to trigger coverage? For example, does the use of a computer to create and print fraudulent documents that are submitted to the insured in paper form constitute Computer Fraud? That was the insured's claim in *Milwaukee Area Technical College*.[78] There, the wrongdoer fashioned

[75] *Id.* at *3.
[76] State v. Rowell, 908 P.2d 1379, 1383-84 (N.M. 1995).
[77] *Id.*
[78] 2008 WL 1787682, at *10.

fake check ledgers using standard accounting software.[79] By submitting the fake check ledgers to the insured, the wrongdoer received reimbursements for payments that were never made. The court, however, did not reach the issue of whether this action constituted computer fraud because, as discussed above, coverage was excluded as the fraud was carried out by an authorized representative.

Again, the direct loss analysis should crystallize the potential issue. Direct means direct; consequently, the computer must be used to directly cause the insured's loss, not merely be a passive instrument that happened to be used in facilitating the fraud.

3. What is covered loss?

Royal American Group, Inc. v. ITT Hartford[80] involved a claim under the computer fraud coverage. The coverage issue in that case boiled down to whether the computer theft of long distances access codes from a long distance telephone provider constituted a covered loss. The trial court found that the long distance provider's contracts with three long distance carriers constituted "securities," as defined in the policy, and that the unauthorized long distance charges made with the stolen access codes resulted in the loss of or damage to this "covered property."[81] The insured argued that the contracts with the long distance carriers were "contracts representing […] other property" according to the policy definition of "securities."[82] But the appellate court disagreed, holding that the plain and ordinary meaning of the term "securities" did not include the insured's contractual right to access another company's long distance network.[83] In addition, even if the contracts were "securities" under the policy, the insured could not show how the unauthorized long distance charges resulted in a loss or damage to its rights under the contracts.[84] Therefore, the insured's contractual liability for the unauthorized charges was not a covered loss.

---

[79] *Id.*
[80] No. 16246, 1994 WL 14888 (Ohio Ct. App. Jan. 12, 1994).
[81] *Id.* at *2.
[82] *Id.*
[83] *Id.*
[84] *Id.* at *3.

IV.
CONCLUSION

The Computer Fraud and Funds Transfer Fraud coverages will continue to present issues that one can not even imagine at this point. The schemes are constantly evolving and the coverage responding. Although there is surprisingly little case law on the coverages, it is most certain that that will change in the near future as more and more insureds are suffering losses, as well as larger losses, as a result of computer crimes. Although the vast majority of decisions are unreported, the cases are positive in the that courts' analyses, particularly with the application of exclusions, has indicated an unwillingness to interpret the language out of context as to what the coverage is intended to provide. Coverage is available for third-party access to the systems for the purpose of theft. The coverage grant, and the exclusions, make this intent clear and unambiguous. Thus far, the courts have agreed.