The Computer Crime Coverage Conundrum

By John R. Felice

Many of you may be reading this article on your handheld device, your laptop, or your desktop computer. In fact, most of you would feel lost if you had to go even one hour without those electronic devices. All of those devices simplify your lives, yet they complicate the lives of those in the insurance industry because, despite how much computerized devices infiltrate every aspect of our daily lives, computer crime insurance policies remain vague and complicated. Language contained in those policies has failed to keep pace with technological advances, leaving insureds and insurers in a netherworld of determining the scope of necessary insurance protection and the protection policies provide. The boundless creativity of individuals seeking to exploit opportunities made possible by our electronic freedom leaves financial institutions and businesses, and the insurers that cover their losses, significantly burdened by this ambiguity.

There are several computer-related insuring agreements, all of which purport to provide coverage for crimes committed while using a computer, but none of which define the term ñcomputerò or the phrase ñuse of a computer.ò What constitutes a computer is obvious, you would think. But does a smartphone fall within the definition of computer? What about a simple cell phone from which someone could send a text message to set a chain of events into action that leads to a loss? Is a fax machine a computer? Does the simple act of reading an e-mail with instructions on how to perpetrate a crime constitute the use of a computer? This article examines all of these issues and offers practical solutions for both policy holders and insurance companies to navigate their way through this coverage abyss.

Insuring Agreements

The Insurance Services Office (ISO) has two forms that provide coverage for computer fraud. Both forms specify that the loss must result directly from the use of a computer.

Commercial Crime Policy (CCP) – ISO CR 00 22 05 06

6. Computer Fraud

We will pay for loss of or damage to ñmoneyò, ñsecuritiesò and ñother propertyò resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the ñpremisesò or ñbanking premisesò:

a. To a person (other than a ñmessengerò) outside those ñpremisesò; or

b. To a place outside those ñpremisesò.

Computer Fraud Coverage Form – ISO CR 00 07 10 90

A. COVERAGE ï We will pay for loss of, and loss from damage to, Covered Property resulting directly from the Covered Cause of Loss.

1. Covered Property: ñMoney,ò ñSecuritiesò and ñProperty Other Than Money and Securities.ò

D. ADDITIONAL EXCLUSIONS, CONDITIONS AND DEFINITIONS:

3. Additional Definitions

b. ñComputer Fraudò means ñtheftò of property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the ñpremisesò or ñbanking premisesò to a person (other than a ñmessengerò) outside those ñpremisesò or to a place outside those ñpremises.ò

These insuring agreements intend to protect an insured when an individual uses a computer to fraudulently gain access to an insuredôs internal computer system and transfers funds from the insuredôs premises. These coverage forms make clear that the loss or damage must be caused directly by the use of a computer. As discussed in greater detail below, the phrase ñuse of a computerò is not defined, and the degree of use required to prompt coverage is open to interpretation.

ISO and the Surety Association of America (SAA) have computer crime policies that are substantially similar. Neither policy uses the phrase ñuse of a computer,ò but both provide coverage for losses involving ñcomputer systems,ò and envisioning how the covered acts would not involve the use of a computer is hard. Both policies define the phrase ñcomputer system,ò but the definition in the SAA form is narrower than that in the ISO form. They read as follows.

Financial Institution Computer Crime Policy (FICP) – FI 00 20 09 12

A. Insuring Agreements

1. Computer Fraud

a. We will pay for loss resulting directly from a fraudulent:

(1) Entry of ñelectronic dataò or ñcomputer programò into; or

(2) Change of ñelectronic dataò or ñcomputer programò within;

any ñcomputer systemò owned, leased or operated by you or your contracted electronic data processing firm, provided the fraudulent entry or fraudulent change causes with regard to Paragraphs 1.a.(1) and 1.a.(2):

(a) ñPropertyò to be transferred, paid or delivered;

(b) An account of yours, or of a ñcustomerò to be added, deleted, debited or credited; or

(c) An unauthorized account or a fictitious account to be debited or credited.

SSA – Computer Crime Policy for Financial Institutions

1. Computer Systems Fraud

Loss resulting directly from a fraudulent

(1) entry of Electronic Data or Computer Program into, or

(2) change of Electronic Data or Computer Program within

any Computer System operated by the Insured, whether owned or leased; or any Computer System identified in the application for this policy; or a Computer System first used by the Insured during the policy period, as provided by General Agreement A; provided the entry or change causes

(i) property to be transferred, paid or delivered,

(ii) an account of the Insured, or of its customer, to be added, deleted, debited or credited, or

(iii) an unauthorized account or a fictitious account to be debited or credited.

The coverage afforded by these insuring agreements differs from the computer fraud coverage provided by a Commercial Crime Policy or Computer Fraud Coverage Form because the insuring agreements do not state that the loss has to be caused by the ñuse of a computer.ò Those seeking coverage will argue that coverage applies when a computer is involved to directly cause the loss, not just when the use of the computer itself causes the loss. In other words,

entering data into the computer system can be the first step in a process that directly leads to a loss, and the financial institution coverage would apply. Those contesting coverage will argue that for the loss to result directly from a fraudulent act involving a computer system requires ñuse of a computerò immediately preceding the loss, rather than use at some remote time in a long process leading to a loss.

Computer

Only a few cases analyze computer fraud coverage, and the majority of those cases involve the use of a traditional computer. *See, e.g., Methodist Health System Foundation, Inc. v. Hartford Fire Insurance Company*, 834 F. Supp. 2d 493 (E. D. La. 2011) (involving use of a computer to generate false documents that misled investors and gave the appearance of a legitimate investment operation). As mentioned earlier, a computer isnôt just an electronic box that sits on a desk anymore. Computers come in different shapes, sizes, colors, and capacities. Someone who commits a crime using an electronic device is just as likely to use a handheld device, such as a smartphone, as a traditional computer. None of the coverage forms specifically includes handheld devices, such as a smartphone, in the definition of ñcomputer.ò

The ISO Financial Institution Computer Crime Policy defines ñcomputer systemò to mean ñcomputers, including Personal Digital Assistants (PDAs) and other transportable or handheld devices, electronic storage devices and related peripheral componentsò by which ñóelectronic dataôis collected, transmitted, processed, stored or retrieved.ò Similarly, the SAA Computer Crime Policy for Financial Institutions defines ñcomputer systemò to mean ñcomputers with related peripheral components, including storage components wherever located . . . by which óelectronic dataôis collected, transmitted, processed, stored or retrieved.ò The major difference is that the SAA definition does not include PDAs. The ISO Commercial Crime Policy defines ñcomputer systemò to mean ñcomputers and related peripheral components . . . by which óelectronic dataôis collected, transmitted, processed, stored and retrieved.ò

Even if someone did look outside of the computer crime coverage realm, the definition of ñcomputerò would not include the majority of what most of us consider a computer to be. For example, the United States Code defines ñcomputerò in connection with fraud and related activity to mean

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

18 U.S.C.A. §1030. Is a smartphone a ñdata processing device,ò or does it fall into the ñother similar deviceò category to exclude it from the definition of computer? The case law does not

examine this issue, and someone could make a reasonable argument either way.

So looking back at the questions posed at the outset, does a smartphone fall within the definition of computer? What about a traditional cell phone, or a ñdumb phoneò as some might call it? All of the definitions mentioned here are ambiguous, and courts usually resolve ambiguities in favor of an insured. The FICP definition most nearly includes modern technology because it includes PDAs and ñother transportable or handheld devices.ò But newer technologies, such as smartphones, basically have rendered PDAs obsolete. Those seeking coverage should argue that ñother transportable or handheld devicesò is broad and could include a smartphone or even cell phone. Those contesting coverage should argue that the ñother transportable or handheld devicesò refers to devices such as PDAs, and smartphones are functionally distinct from those devices.

It is important to read closely the insuring agreements, definitions, and exclusions used by a particular insurer because slight changes or additions to the standard form language could make a big difference. For example, in *Brightpoint, Inc. v. Zurich American Insurance Company*, 2006 WL 693377, at *1 (S.D. Ind. Mar. 10, 2006), the insured experienced a loss at one of its subsidiaries in the Philippines as a result of a scam involving prepaid telephone cards. The scam was set in motion when Brightpoint received, by fax machine, copies of purchase orders, post-dated checks, and bank guarantees. Brightpoint was the insured under a crime policy issued by Zurich. The Zurich policy followed ISO form CR 00 07 10 90, defining ñcomputer fraudò as ñóthe theftô of property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the . . . ópremisesô or óbanking premisesô to a person (other than a ómessengerô) outside those ópremisesô or to a place outside those ópremises.ôò The Zurich policy added a sentence to the computer fraud definition, which stated that the ñmeans by which a fraudulent transfer is initiated includes: written, telephonic, telegraphic, telefacsimile, electronic, cable, or teletype instructions.ò This additional sentence may have caused the court to accept the insuredôs position that a facsimile machine was a computer more easily.

Brightpoint argued that ñthe facsimile it received (which it alleges constitutes the use of a computer) of the checks and bank guarantees caused it to take actions which eventually led to it being defrauded when it released the phone cards to the defrauding party.ò *Id.* at *4. In discussing whether the receipt of the fraudulent checks caused the loss, the court stated:

> The fraud in this instance occurred through the use of the unauthorized checks and guaranties, not the manipulation of numbers or events through the use of a computer, facsimile machine or other similar device. The facsimile transmission caused Brightpoint to purchase the cards from its supplier, not to transfer them to its purchaser, and the use of the fax thus cannot be viewed as having directly or proximately caused the theft.

Id. at *7. In reaching its decision, the court apparently assumed that a facsimile machine constituted a computer, perhaps because the Zurich policy specifically made reference to a

telefacsimile machine in the definition of computer fraud. Smartphones are capable of performing many more functions than a fax machine and, therefore, an argument could be made that, if a fax machine is considered a computer, then a smartphone is too.

Use of a Computer

Which types of electronic equipment the parties to an insurance contract intended to be viewed as a ñcomputerò for purposes of fraud coverage is not always clear. Equally challenging is determining whether a computer actually was used in perpetrating the allegedly fraudulent activity. Does ñuseò mean communicating manipulated and stored electronic information to a third party at some remote location? Or is it simply a few keystrokes on a keyboard in place of a typewriter? Might it involve exploiting knowledge about how an entityôs computer system operates? The answers are not easily found in this minimally charted territory.

The insuring agreement itself serves as the first source of information about what the parties meant when they included the limiting phrase ñuse of a computerò in the computer fraud coverage insurance. Clear expressions of what the parties intended may end the inquiry there. As noted above, however, most policies do not define the phrase. When the policy language does not define the phraseôs meaning, insureds and insurers must turn to judicial interpretation and legal and professional commentary for guidance.

Few cases have addressed this issue directly and none with precision. What the case law does make clear is that ambiguity of the often undefined phrase ñuse of a computerò is construed against the drafting insurer consistent with standard rules of contract interpretation. In *Owens,* the plaintiff insured sought indemnity from its insurer under a crime insurance policy that covered computer fraud. *Owens*, 2010 WL 4226958, at *1, 50 Conn. L. Rptr. at 665. E-mails and electronic wire transfers were used to perpetrate the fraud. Relying on the *Brightpoint* decision, the insurer moved for a summary judgment arguing, among other things, that the claim did not constitute computer fraud under the policy because ñfor computer fraud to exist, the transfer must occur by way of a ócomputer hackingô incident, such as the manipulation of numbers or events through the use of a computer.ò The insured in the *Owens* case disagreed with the elevated standard that the insurer sought to impose and responded that ñthe only required level of computer usage to constitute Computer Fraud under the subject insurance policy is óthe use of any computerô and the word óuseô is not further defined or described under the policy.ò *Id.* at *7. The trial court agreed and held that ñthe policy is ambiguous as to the amount of usage necessary to constitute computer fraud. This ambiguity is resolved in favor of the plaintiff [insured].ò *Id.* at *7. The trial court in *Owens* also concluded that the holding in *Brightpoint* did not require a showing of something such as a ñcomputer hacking incident.ò *Owens*, 2010 WL 4226958, at *7.

It should be noted that, in April, 2012, an order of vacatur was entered on the docket indicating that, among other things, the September 17, 2010, memorandum of decision, published September 20, 2010, was vacated by stipulation of the parties. On May 5, 2012, the judge who wrote the September 17, 2010, memorandum of decision, Judge Richard E. Arnold, objected to the order of vacatur, stating, ñThe trial court, Arnold J., does not consent to the

vacating of its decision denying the defendantôs Motion for Summary Judgment, said decision being dated September 17, 2010. It is the trial courtôs position that the court issuing the Order of Vacatur lacks the authority to order the vacating of the trial courtôs decision dated Sept. 17, 2010 and has not presented legal authority for its Order. *See U.S. v. Munsingware*, 340 U.S. 36, 40ï 41 (1950); *Private Healthcare Systems, Inc. v. Torres*, 278 Conn 291, 303 (2006); *State v. Singleton*, 274 Conn. 426, 439 (2005); *Comm. Motor Vehicles v. DeMilo*, 233 Conn. 254, 272ï 73 (1995).ò As of the date of this article, the *Owens* docket has not received further entries.

In *Brightpoint*, the insured sought coverage from its insurer under a crime policy for a multimillion dollar loss occasioned by a scam involving prepaid telephone cards. 2006 WL 693377, at *1 (S.D. Ind. Mar. 10, 2006). The trial court determined that the insured had not suffered a covered loss, finding that ñthere is nothing in the Proof of Loss that proves that a computer was used to fraudulently cause a transfer of the phone cards.ò *Id.* at *3. Although the policy defined the ñmeans by which a fraudulent transfer is initiatedò to include ñtelefacsimile,ò the trial court concluded that it was not the facsimile that caused the fraudulent transfer; rather, the facsimile simply alerted the insured that the distributer ñwished to place an order.ò *Id.* at *1, *7. The order would be processed on receiving the faxed documents in hand, and the exchange of the cards occurred in person. It was the release of the phone cards after receiving the physical documents and the use of unauthorized checks and guaranties that caused the loss. The trial court concluded that the fraud in that case did not occur through ñthe manipulation of numbers or events through the use of computer, facsimile machine or other similar device.ò *Id.* at *7. The fact that a fax machineð an electronic device apparently viewed by the court as a computerð was used during one step in a series of events that culminated in the fraudulent activity for which coverage was sought was not enough to bring the loss within the coverage.

Consider another situation. An employee uses a bankôs computer as part of his fraudulent scheme, not by directly accessing data contained in that computer, but instead by using the employeeôs intimate knowledge of the way the bankôs computer operates. Does that constitute ñuseò that results in a covered loss? *See* Frank L. Skillern, Jr., *Recent Developments Under the Bankers Blanket Bond* (Summer 1982) (referencing the MAPS-Harold Smith/Wells Fargo Bank transactions). The MAPS-Harold Smith/Wells Fargo Bank transactions involved a bank manager who manipulated a settlement account by debiting the account and then submitting offsetting credits within the time designated by the computer system to detect the missing funds and under a dollar amount that would prompt notice to another banking department. *Id.* at 10ï 11. The scheme was detected when the manager erroneously submitted a credit instead of a debit. The computer was not used to transmit information to a third-party source, but it was the bank managerôs knowledge of the computer operating system that permitted him to commit this fraud. *Id.* Under the *Brightpoint* standard requiring manipulation of numbers or events, such a claim arguably involves use of a computer that may present a covered loss. However, under policies requiring computer transmission outside the premises, such as the ISO CR 00 22 05 06 and 00 07 10 90 forms discussed above, the use of the computerð though fraudulentð may not constitute a use that gives rise to a covered loss.

Most recently, the Supreme Court of New York examined a similar situation and held

that the Computer Systems Fraud policy did not cover the insuredôs losses. In *Universal American Corp. v. National Union Fire Insurance Company of Pittsburgh, PA*, 2013 WL 69241, Universal American submitted a proof of loss in which it claimed that it suffered more than $18 million in losses from fraudulent claims made against one of its plans. The losses were caused by providers, who were authorized to use the Universal American computer system, submitting fraudulent claims through that computer system. National Union issued a Computer Systems Fraud Rider to Universal American using ISO form FI 00 20 09 12. Universal American relied upon the *Owens* case to argue that the clause in the insuring agreement, ñloss resulting directly from a fraudulent é entry of Electronic Data é into [Universalôs] proprietary Computer Systemé ,ò was vague and therefore covered the entry of fraudulent information, even by an authorized user such as a provider. The *Universal American* court refused to adopt the plaintiffôs argument, finding that the clause at issue in *Owens* was much broader because it did not define how much computer use was required or in what manner the computer had to be used. *Id.* at *3. Therefore, ñPlaintiffôs interpretation of the policy would expand coverage to any fraudulent underlying claim that was entered into its computer system by any user, even by an authorized user. This interpretation is not supported by the language of the Rider.ò *Id.* at *4. Instead, the court concluded, ñNothing in this clause indicates that coverage was intended where an unauthorized user utilized the system as intended, *i.e.* to submit claims, but where the claims themselves were fraudulent.ò *Id.*

The case law leaves open the question whether some manipulation of numbers or events as the *Brightpoint* case suggests or something less as allowed in the *Owens* case is necessary to establish a covered loss. Insurers that want to protect themselves should incorporate in their crime policies a definition for ñuse of a computerò because the trend remains to construe ambiguities in an insurance policy against the insurer. Until such a definition appears, insureds likely will rely on cases such as *Owens* to highlight the ambiguities in the undefined terms and gain the interpretive benefit of those ambiguities. Insurers are left then with the uphill battle of arguing that the words ñuse of a computerò cannot simply mean whatever the inventive insureds wish them to mean, but instead they logically require some *Brightpoint*-like activities to demonstrate a covered loss.

Direct Cause and Loss

Even more confusing than the question of what constitutes the use of a computer is whether the use directly caused the lossð that is, did the use of a computer or computer system cause damage to some tangible property? As the Owens judge wrote, ñA direct causation requirement in a crime policy or fidelity bond requires more than a ódut forô or factual causation alone, but requires a ódirectô causation.ò *Owens*, 2010 WL 4226958, at *7. Additionally, ñ[i]t is well settled that the words ódirect causeô ordinarily are synonymous in legal intendment with óproximate cause,ô a rule applicable to causes involving the construction of an insurance policy.ò *Id.* at *7 (quoting *Steiner v. Middlesex Mutual Assurance Company*, 44 Conn. App. 415, 434, 689 A.2d 1154 (1997)). And ñproximate causeò does not mean ñthat which is last in time or place, not merely that which was in activity at the consummation of the injury, but that which is the procuring, efficient, and predominant cause.ôò *Owens*, 2010 WL 4226958, at *7 (quoting

Frontis v. Milwaukee Insurance Company, 156 Conn. 492, 497ï 98, 242 A.2d 749 (1968)).

The case law offers very little information about what constitutes a direct loss, and it is not the aim of this article to address the topic in full here. *See, e.g.,* Linda G. Robinson & Jack P. Gibson, *Commercial Property Insurance* (International Risk Management Institute, Inc. Dallas, Tex. Feb. 2005) and Skillern, *supra,* (comprehensively discussing the direct loss issue). However, the fact that a computer must be used in bringing about the fraud cannot be underscored with more emphasis. Losses due to computer vandalism through introduction of a computer virus or theft of trade secrets are not covered activities under most policies requiring evidence of a direct loss. *See* Robinson, *supra*, at XII.D.9, and comments on Coverage for Computer Crime. Indeed, ñ[m]any, perhaps most, insurers would argue that the information stored on a computer cannot suffer direct physical loss or damage and therefore does not qualify as tangible property.ò *Id.*

Conclusion

What constitutes ñuse of a computerò is not easily defined. As technology advances, the potential that newly developed electronic equipment will be characterized as a ñcomputerò and that electronic activity will fall within the ñuseò penumbra grows exponentially. Navigating this quagmire will continue to present challenges that can be overcome by the addition of definitions establishing the scope of the coverage provided. Until such time, the arguments for and against finding a covered loss resulting from ñuse of a computerò remain as broad as the imagination will allow.