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 "computer" or the phrase "use of a computer." 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 "money," "securities," and "other property" resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the "premises" or "banking premises."

   a. To a person (other than a "messenger") outside those "premises" or

   b. To a place outside those "premises."
A. COVERAGE — We will pay for loss of, and loss from damage to, Covered Property resulting directly from the Covered Cause of Loss.


D. ADDITIONAL EXCLUSIONS, CONDITIONS AND DEFINITIONS:

3. Additional Definitions

   b. "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 (other than a "messenger") outside those "premises" or to a place outside those "premises."

These insuring agreements intend to protect an insured when an individual uses a computer to fraudulently gain access to an insured's internal computer system and transfers funds from the insured's 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 "use of a computer" 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 "use of a computer," but both provide coverage for losses involving "computer systems," and envisioning how the covered acts would not involve the use of a computer is hard. Both policies define the phrase "computer system," 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 "electronic data" or "computer program" into; or
Change of "electronic data" or "computer program" within:

any "computer system" 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) "Property" to be transferred, paid or delivered;

(b) An account of yours, or of a "customer" 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 "use of a computer." 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 "use of a computer 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 isn’t 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 "computer."

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

Even if someone did look outside of the computer crime coverage realm, the definition of "computer" would not include the majority of what most of us consider a computer to be. For example, the United States Code defines "computer 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 "data processing device," or does it fall into the "other similar device" 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 "dumb phone" 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 "other transportable or handheld devices." But newer technologies, such as smartphones, basically have rendered PDAs obsolete. Those seeking coverage should argue that "other transportable or handheld devices" is broad and could include a smartphone or even cell phone. Those contesting coverage should argue that the "other transportable or handheld devices" 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 "computer fraud" as "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 (other than a messenger) outside those premises or to a place outside those premises." The Zurich policy added a sentence to the computer fraud definition, which stated that the "means by which a fraudulent transfer is initiated includes: written, telephonic, telegraphic, telefacsimile, electronic, cable, or teletype instructions." This additional sentence may have caused the court to accept the insured's position that a facsimile machine was a computer more easily.

Brightpoint argued that the 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. *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.

*ld.* 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 "computer" 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 "use" 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 entity's 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 "use of a computer" 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 phrase's 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 "use of a computer" 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 "for computer fraud to exist, the transfer must occur by way of a 'computer hacking' incident, such as the manipulation of numbers or events through the use of a computer." The insured in the Owens case disagreed with the elevated standard that the insurer sought to impose and responded that "the only required level of usage to constitute Computer Fraud under the subject insurance policy is 'the use of any computer' and the word 'use' is not further defined or described under the policy." Id. at *7. The trial court agreed and held that the policy is ambiguous as to the amount of usage necessary to constitute computer fraud. This ambiguity is resolved in favor of the plaintiff [insured]. 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 "computer hacking incident." Id., 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, "The trial court, Arnold J., does not consent to the

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 “there is nothing in the Proof of Loss that proves that a computer was used to fraudulently cause a transfer of the phone cards.” Id. at *3. Although the policy defined the “means by which a fraudulent transfer is initiated” to include “telefacsimile,” the trial court concluded that it was not the facsimile that caused the fraudulent transfer; rather, the facsimile simply alerted the insured that the distributor wished to place an order. 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 the manipulation of numbers or events through the use of computer, facsimile machine or other similar device. Id. at *7. The fact that a fax machine—an electronic device apparently viewed by the court as a computer—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 bank’s computer as part of his fraudulent scheme, not by directly accessing data contained in that computer, but instead by using the employee’s intimate knowledge of the way the bank’s computer operates. Does that constitute “use” 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 10–11. 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 manager’s 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 computer though fraudulent 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 insured's 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, "loss resulting directly from a fraudulent... entry of Electronic Data... into [Universal's] proprietary Computer System...", 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 plaintiff's 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, the court concluded, nothing 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. *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 "use of a computer" 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 "use of a computer" 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 loss that is, did the use of a computer or computer system cause damage to some tangible property? As the *Owens* judge wrote, "A direct causation requirement in a crime policy or fidelity bond requires more than a but for factual causation alone, but requires a direct causation." *Owens*, 2010 WL 4226958, at *7. Additionally, it is well settled that the words "direct cause" ordinarily are synonymous in legal intendment with "proximate cause," a rule applicable to causes involving the construction of an insurance policy. *Id.* at *7 (quoting *Steiner v. Middlesex Mutual Assurance Company*, 44 Conn. App. 415, 434, 689 A.2d 1154 (1997)). And proximate cause does not mean that 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. *Owens*, 2010 WL 4226958, at *7 (quoting
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, many, 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. Id.

Conclusion

What constitutes use of a computer is not easily defined. As technology advances, the potential that newly developed electronic equipment will be characterized as a computer and that electronic activity will fall within the 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 use of a computer remain as broad as the imagination will allow.
Crime Policy Does Not Cover Loss of Company Funds Resulting From Social Engineering Scheme

By Thomas Orofino on October 24, 2016
Posted in Coverage, Cyber, Fidelity, Fraud, Insurance

In a long-awaited decision (at least by the parties and fidelity law practitioners) the Fifth Circuit Court of Appeals has held that a “Computer Fraud” Insuring Agreement in a Crime Insurance Policy does not cover the insured’s loss after its employees were tricked into wiring approximately $7 million to a fraudulent bank account set up by criminals posing as one of the insured’s trusted vendors. Apache Corp. v. Great American Insurance Co., No. 15-20499, 2016 WL 6090901 (5th Cir. Oct. 18, 2016).

This case arises from a 2013 social engineering scheme¹ whereby several criminals, suspected to be based in Latvia, posed as representatives of Petrofac, a vendor of Apache, the insured oil-production company. After corresponding with the fraudsters by phone and over email, the imposters convinced Apache to direct payments to a “new” bank account for Petrofac. In brief, the scheme unfolded as follows:

- An Apache employee received a telephone call from a person identifying herself as a representative of Petrofac, Apache’s vendor. The caller instructed Apache to change the bank account information for its payments to Petrofac. The Apache employee responded that such a change could not be accomplished without a formal request on the vendor’s letterhead.
A week later, Apache’s accounts payable department received an email from a “petrofacltd.com” address in which the sender advised that the purported “new” bank account was effective and payments going forward should be made to the new account. The sender attached a letter to the email with both the old and “new” bank account information. This letter was on Petrofac letterhead and contained a signature by a purported Petrofac employee.

In response to the email with attached letter, an Apache employee called the number listed on the letter. An individual posing as a Petrofac employee purportedly confirmed the request to change the banking information.

An Apache employee then entered an internal “change request” with the new Petrofac bank account information. A separate Apache manager then approved the request and thereafter payments began flowing to the new bank account, which was really a fraudulent account set up by the imposters.

The scheme unraveled when the “real” Petrofac contacted Apache regarding several delinquent invoices. Upon investigation, Apache realized that it had been duped. Fortunately, Apache was able to recover a substantial portion of the funds, leaving its total loss at only $2.4 million, of which Apache claimed a loss of approximately $1.4 (after application of the deductible) under the “Computer Fraud” provision of its crime policy.

The Computer Fraud Insuring Agreement

Apache’s crime policy contained, in part, the following “Computer Fraud” Insuring Agreement:

We will pay for loss of, and loss from damage to, money, securities and other property resulting directly from the use of any computer to fraudulently cause a transfer of that property from inside the premises or banking premises: (a) to a person (other than a messenger) outside those premises; or (b) to a place outside those premises.
After analyzing Apache’s loss, Great American denied coverage, in part, because the loss “did not result directly from the use of a computer nor did the use of a computer cause the transfer of funds.” Essentially, the insurer examined the fraud and found that the email did not, by itself, cause the funds transfer and coverage under the Computer Fraud agreement was limited to hacking and unauthorized computer use. Apache disagreed and sued the insurer, claiming that the Computer Fraud agreement said nothing about “hacking” and the denial was improper because the email from the fraudsters constituted computer fraud which directly caused the fraudulent transfer of funds.

The District Court Decision

In August 2015, the U.S. District Court for the Southern District of Texas handed down a decision granting Apache’s motion for summary judgment, noting that “the intervening steps of the [post-email] confirmation phone call and supervisory approval do not rise to the level of negating the email as being a substantial factor” in bringing about the loss, thus presenting a factual scenario sufficient to allow coverage under the “directly resulting from” language in the Computer Fraud Insuring Agreement. According to the district court, “despite the human involvement that followed the fraud, the loss still resulted directly from computer fraud, i.e., the email directing Apache to disburse payments to a fraudulent account.”

The Fifth Circuit Reverses and Gets it Right

On October 18, 2016, the Fifth Circuit vacated the district court decision and entered judgment in favor of Great American, noting that “there is cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use.” After surveying a spate of recent case law involving similar disputes, the court found that the now vacated district court decision was the “only presented decision interpreting the computer-fraud policy language to cover a loss when the computer use at issue was limited to email correspondence.” The Court found that the email Apache highlighted in order to assert coverage under the Computer Fraud agreement was undoubtedly “part of the scheme,” but merely incidental to the occurrence of “the authorized transfer of money.”
Note that the email, by itself, caused no transfer of money; rather, it was just one step in a multi-step process that ended in Apache failing to detect the imposters and making large payments to a fraudulent bank account. To interpret the computer fraud provision as reaching any fraudulent scheme involving an email communication would, as stated by the court, “convert the computer-fraud provision to one for general fraud,” a risk the insurer clearly did not contemplate. Essentially, the Court read the “resulting directly from” language in the Computer Fraud agreement to require the identified “use of a computer” to cause the fraudulent transfer itself (i.e., a true hacking incident), not merely set in motion, or be part of, a chain of events whereby an insured fails to investigate the accuracy of fraudulent information provided to it.

**Takeaways**

Social engineering schemes similar to that described above are on the rise because of the ease in which fraudsters can obtain information about a target online. By using a combination of telephonic and online communication, even large companies are vulnerable to sophisticated schemes of fraud. In response to these threats, certain carriers have introduced specialized extensions of coverage or separate products aimed at covering “social engineering” risks. Nonetheless, certain coverage directed at true “hacking” threats, as was the intent of Great American’s insuring clause here, will likely be subject to challenges from insured’s lacking appropriate “social engineering” coverage. The Fifth Circuit’s Apache decision provides helpful authority to define the limits of standard computer fraud wording as it appears in crime policies and shows that the use of a computer somewhere in the chain of a multistep fraudulent scheme is insufficient to trigger coverage.

---

1 “Social Engineering” is often defined differently based on who is using the phrase (e.g., insurers, brokers, IT professionals). In general, social engineering may be understood to be “the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes, or to induce an individual to take an action in which they otherwise would not engage.” See “Social Engineering” (in the context of information security) Oxford Dictionaries.
Petrofac’s real email domain name is “petrofac.com.” For a recent FBI memo describing the threat of so-called “business email compromise” schemes (a type of social engineering scheme), please click here. See “Scenario 1,” in which the FBI notes: “A business, which often has a long standing relationship with a supplier, is requested to wire funds for invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears very similar to a legitimate account and would take very close scrutiny to determine it was fraudulent. Likewise, if a facsimile or telephone call is received, it will closely mimic a legitimate request.”

The Surety & Fidelity Association of America, a national trade organization consisting of fidelity and surety insurance companies, submitted an amicus brief to the Fifth Circuit urging that the district court’s decision be reversed: “To hold that ‘Computer Fraud’ means any fraud that uses a computer even in some minor way … essentially turns ‘Computer Fraud’ coverage into ‘All fraud’ coverage. It would be impossible to underwrite potential risks for ‘All Fraud’ coverage and … the premiums for such a policy would be prohibitive.”