HACKING IS HACKING IS HACKING, NOT SOCIAL ENGINEERING, OR TRYING TO FIT A SQUARE PEG INTO A ROUND HOLE, PART 1: THE PARAMETERS AND LIMITATIONS OF THE COMPUTER FRAUD INSURING AGREEMENT

PRESENTED BY:

MICHAEL KEELEY
Strasburger & Price, LLP
901 Main Street, Suite 4400
Dallas, Texas 75202

MATTHEW J. PHOTIS
Berkley FinSecure, A W.R. Berkeley Company
849 Fairmount Avenue, Suite 301
Towson, MD 21286
HACKING IS HACKING IS HACKING, NOT SOCIAL ENGINEERING, OR TRYING TO FIT A SQUARE PET INTO A ROUND HOLE, PART 1: THE PARAMETERS AND LIMITATIONS OF THE COMPUTER FRAUD INSURING AGREEMENT

I. Introduction

The term “hacker” was first coined in the 1960s at MIT, when members of the school’s “Tech Model Railroad Club” began tinkering with the electrical systems (basic computers) that ran the model trains. The goal of this early “hacking” was to make the model trains run faster or perform in a way that fit the particular track the train was on. Now, nearly sixty years later, this initially innocent practice has morphed into one of the most significant threats facing American businesses today. The significant risk posed by hacking has caused companies to seek ways to minimize their exposure. Given the high costs associated with fully implementing the necessary security against hacking, companies placed an emphasis on shifting the risks associated with computer theft away from themselves to willing third parties: insurers. Responding to this demand, in 1981, Lloyd’s of London introduced an Electronic and Computer Crime Policy intended to cover “loss due to fraudulent input of electronic data or computer instructions into the insured’s computer by unauthorized access to a terminal, fraudulent preparation of computer programs, and by obtaining access to a bank’s computer lines.” Soon thereafter, The Surety & Fidelity Association of America introduced the Computer Systems Rider to the Bankers Blanket Bond Form No. 24. Today, insurers continue to offer insuring agreements designed to cover the risk of computer hacking.

But hacking, of course, is not the only risk that businesses face. Recently, criminals have turned to various forms of so-called “social engineering,” manipulating people into divulging confidential data or tricking them into transferring data or funds, allowing criminals to commit their crimes without the need to actually hack victims'
computer systems.9 From “phishing” to “baiting” to “business e-mail compromise” scams, cybercriminals are finding new ways to stay ahead of honest businesses and take advantage of individuals to perpetrate their crimes.

These scams are plain old-fashioned fraud that merely happen to tell a lie through a computer (for example, in an e-mail). These “social engineering” schemes do not depend on a sophisticated infiltration into the insured’s computer system. Instead, they use tricks as old as time: they exploit the human instinct to follow instructions and the fear of not following an order that appears to come from a superior. But Computer Fraud insuring agreements are not intended to cover such types of human-to-human fraud, as opposed to computer-to-computer fraud. But this has not stopped insureds from seeking coverage for these schemes under Computer Fraud coverage, even when the loss clearly does not result from hacking, which is what those insuring agreements were designed to cover.10 This article will explore the limits of insuring agreements designed to cover loss resulting from hacking and discuss the key cases in which insureds have attempted to recover a loss resulting from social engineering under a hacking policy. These issues are becoming increasingly important as social engineering continues to grow in popularity. Fidelity professionals need to be aware of these cases and consider them carefully when drafting policies designed to cover hacking.

A. Background

1. History of Computer Usage

For most of human history, the idea of “computing” involved humans performing calculations by hand or on simple machines such as an abacus. However, that all changed in the first half of the twentieth century. In 1939, Professor John Vincent Atanasoff developed the first electronic calculating machine with the ability to solve complicated physic computations.11 Shortly thereafter, Professor Howard Aiken developed the MARK I, an enormous electromechanical computer that could perform three addition operations per second and one multiplication operation every six seconds.12 The MARK I is generally recognized as the first mainframe computer.13 A few years later, in 1946, Dr. John Mauchly, in collaboration with J. Presper Eckert, Jr., created the Electronic Numerical Integrator and Computer14 weighing in at thirty tons, occupying 15,000 square feet, and using 18,000 vacuum tubes.15 The ENIAC had the capability of performing over eighty addition operations or eight multiplication operations

---

12 Id.
14 Hereinafter ENIAC.
per second. These first machines did not use computer programs as we understand them today, but instead performed mathematical functions based on the physical arrangement and structure of the circuits. Nonetheless, the computer age was born.

In 1949, Mauchly and Eckert founded the first computer company, Electronic Controls Company, and began releasing a series of mainframe computers under the name UNIVAC. The UNIVAC 1101 is considered to be the first computer that had the capabilities of storing and running a program from memory. Then, early in the 1950s, the introduction of magnetic core memory and the transistor circuit element improved computers’ reliability and increased their RAM capacities. However, because these machines were very expensive to operate, they were mostly found in large centers operated by industry, government and private laboratories. In 1954, IBM introduced the IBM 650, its first commercial computer.

In the 1960s, with the development of integrated circuits, computer manufacturers were able to increase the computing power and efficiency of computers, which lead to a reduction in the cost of data processing and allowed computers to fall within the budgetary and practical reach of a growing number of businesses. At the same time, this new integrated technology allowed manufacturers to incorporate layers of transistors within the same semiconductor material, greatly reducing the size of computers. By the 1970s, semiconductor chips were being installed on computers, and, as this technology improved, the size of computers continued to shrink while their computing power increased. During this same time, Intel Corporation created the microprocessor, a chip containing the entire control unit of the computer. Through large scale integration of the microprocessor, the microcomputer was developed and came to dominate the industry by the 1980s, with Apple and IBM leading the charge.

These rapid developments in the computer, evolving from large mainframes to personal computers, are reflected in the numbers surrounding computer usage. In 1975, approximately 40,000 computers were sold in the United States. By 2000, the number of computers sold in the United States increased to 46,000,000. And in 2015, that

---

16 See id.
17 Id. at 70-71.
19 See id.
21 See id.
23 Id.
24 Id.
25 Id. at 73.
26 Id.
27 Id.
29 See id.
number further climbed to approximately 71,250,000. These increased sales numbers go hand in hand with the growth of computer usage in the United States. In 1984, United States Census Bureau first began asking about citizens’ computer usage. That year, 1984, only 8.2 percent of households had a computer. However, by 2013, 83.8 percent of United States households reported owning a computer, with 78.5 percent of all households having a desktop or laptop computer and 63.6 percent of all households owning a handheld computer. Computers have become ubiquitous, and with the spread of that technology, criminals are taking advantage.

2. The History of Hacking

Cybercrime is a growing threat. According to one report, in 2001, cybercrime in the United States resulted in approximately $17.8 million in reported damages to the Internet Crime Complaint Center, a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center. By 2015, that same entity reported that the amount of reported cybercrime damages had risen to $1.07 billion. PricewaterhouseCoopers’ 2014 Global Economic Crime Survey found that seven percent of United States organizations lost $1 million or more due to cybercrime in 2013, and another 19 percent reported financial losses of $50,000 to $1 million. So far in 2016, PricewaterhouseCoopers’ 2016 Global Economic Crime Survey shows that it is now fourteen percent of organizations that report losses of $1 million or more due to cybercrime over the last twenty-four months. PricewaterhouseCoopers further explains that, for some businesses, the size of the loss can be devastating: “Losses can be heavy. A handful of respondents (approximately 50 organisations) said they had suffered losses over $5 million; of these, nearly a third reported cybercrime-related losses in excess of $100 million.”

30 See id.
35 See id.
36 See PricewaterhouseCoopers, US Cybercrime: Rising Risks, Reduced Readiness (June 2014).
When it comes to cybercrime, people often think of a criminal in some far-off location, gaining unauthorized access to a company’s system and illegally obtaining information or transferring funds to a secure bank account. In other words, we commonly associate computer fraud with hacking. Hacking broadly describes attempts “to intentionally access or harm information assets without or in excess of authorization by thwarting logical security mechanisms.” More simply, hacking is the direct act by an unauthorized individual to gain access to a company’s or individual’s computer system.

“Hacking” has been around for decades. The first “hackers” were MIT students who, in the 1960s, “hacked” model train sets to make them perform faster. Several of these train enthusiasts later applied their curiosity and hacking skills to the new computer programs being developed on the campus. These students and other early computer hackers were primarily interested in modifying programs to increase their efficiency or customizing them for specific applications. However, in the 1970s, the art of hacking became more sinister. For example, in 1971, so-called “phreakers” discovered and exploited the mechanics behind AT&T’s long distance switching system to make long distance international phone calls free of charge.

The 1980s saw hacking truly take off, as personal computers and modems, which allowed computers to communicate over telephone lines, became more abundant. With the 1983 movie *War Games*, where the main character breaks into the military’s nuclear combat simulator computer, the notion of hacking entered the public sphere. In 1984, *2600: The Hacker Quarterly*, a hacker magazine was first published, followed a year later by another magazine *Phrack*, which provided tips for would-be hackers. In 1986, in response to these and other publications, as well as the rise of the number of governmental and corporate hacking break-ins, the Federal Government passed its first hacking-related legislation, the Federal Computer Fraud and Abuse Act, which made it a felony to tamper with a computer. In 1988, Robert Morris launched the

---

41 See id.
43 See id.
47 See id.
first internet worm, essentially shutting down a large portion of the early internet, and became the first person convicted under the Federal Computer Fraud and Abuse Act.49

By the mid-1990s, several high profile hacking thefts and subsequent arrests had taken place. Kevin Poulsen, already wanted for hacking into federal computers, rigged a radio station’s phone lines to win a Porsche.50 Vladimir Levin used stolen access codes and passwords to transfer more than ten million dollars from Citibank across the United States, Europe, and Israel.51 And Kevin Mitnick, labeled by the FBI as “the most wanted computer criminal in U.S. history,” hacked into the computer systems of several technology companies, including Sun Microsystems, Fujitsu, and Nokia.52

In today’s world, “[s]ecurity experts like to say that there are now only two types of companies left in the United States: those that have been hacked and those that don’t know they’ve been hacked.”53 In 2011, approximately 81% of cybercrime was committed through hacking incidents.54 One recent article estimates that hacking costs the overall U.S. economy as much as $100 billion annually and up to 500,000 jobs.55 But it’s not just businesses that suffer from hacking. In July 2015, the Obama administration revealed that confidential personal information, including financial information, for 21.5 million people was stolen by hackers.56 Given these numbers, it is not a surprise that Americans fear hacking the most of all possible crimes.57 It is the this fearsome crime of hacking that Computer Fraud insuring agreements are designed to protect against.


By the 1980s, as the widespread use of interconnected computer systems in banking created new avenues for bad actors to steal funds without ever having to enter a bank, the insurance industry began exploring whether it could cover this latest risk. In

50 See id.
51 See id.
52 See id.
1981, Lloyd’s of London introduced an Electronic and Computer Crime Policy. Not to be outdone, two years later, in 1983, the SFAA introduced the Computer Systems Rider to the Standard Form No. 24, although the SFAA had begun drafting the rider’s precursor as early as 1977. In 1993, following several revisions to address the ongoing technological developments and in response to insurers’ appreciation of the risks caused by those developments, the SFAA offered a stand-alone Computer Crime Policy for Financial Institutions, which offered seven categories of coverage: (1) computer-systems fraud, as had been offered by the rider introduced in 1983; (2) data processing service operations; (3) voice initiated funds transfers; (4) telefacsimile initiated funds transfers; (5) the destruction of data or programs by a hacker; (6) the destruction of data or programs by a computer virus; and (7) voice computer systems fraud.

4. Evolving Computer Fraud Schemes – Social Engineering

Hacking is the direct, unauthorized accessing of a company’s or individual’s computer system. “Social engineering,” on the other hand, describes a broad array of techniques designed to manipulate others into performing certain actions or disclosing sensitive information. The phrase “social engineering” was popularized by a former hacker, Kevin Mitnick, who found that it was easier to trick a potential victim into unwittingly disclosing confidential information, such as a password or account number, than it was to hack into an account. Cybercriminals take advantage, not of the weaknesses in the computing system itself, but of the weaknesses of humans. “A social engineer is nothing more than a con man who uses technology to swindle people and manipulate them into disclosing passwords or bank information or granting access to their computer.”

Willis, one of the world’s largest insurance brokers, described the risk as follows:

Fraudsters send communications to an employee (most often via email, telephone or a combination of the two), which are doctored to appear as if they are sent by a senior officer of the company or by one of its customers or vendors. Instructing the employee to wire funds to a particular bank account, the communication stresses the need for absolute secrecy, perhaps citing the fact that the fund transfer is related to a pending IPO or

---

other confidential transaction that requires normal authentication procedures be bypassed, while also citing urgency. Some schemes are highly complex and can actually result in the undetected rerouting of phone calls or email domain changes.

For those instructions purportedly coming from a vendor or customer, the schemes can be embroidered by informing the employee that they have changed banks and require the company to provide new wire instructions for all future payments.64

Social engineering can take on several different iterations. But the fundamental aspect of all social engineering scams is the willful manipulation of another’s tendencies. In 2011, according to Check Point Software Technologies, nearly half of the businesses surveyed claimed to be the victim of one form or another of social engineering scams.65

a. Phishing

One of the more common social engineering schemes is “phishing,” which is a form of fraud “in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in e-mail, IM or other communication channels.”66 Cybercriminals send an e-mail that appears to come from the recipient’s bank or a website, such as Amazon or PayPal, where the recipient may have credit card details or cash stored, and ask the user to perform some task in response.67 As an example of such a scheme, an individual may receive an e-mail purportedly from PayPal, containing the PayPal logo, asking the recipient to update his or her credit card details to prevent the account from being suspended. The e-mail will contain a link directing the user to a site that appears to be PayPal but that is actually fake. The unknowing user then enters his or her credit card details into the fake site, allowing the criminal to obtain the user’s credit card information, as well as the individual’s PayPal username and password.68 These scams generally take advantage of the recipient’s gullibility.69 In a 2014 study testing employees’ ability to detect online phishing scams, McAfee Labs found that 80% of the participants failed to detect at least one of seven phishing e-mails sent to them. The participants who worked in their

---

64 WILLIS FINEX NORTH AMERICA, Fraud Advisory: Social Engineering and How to Protect Yourself 1 (Nov. 2014).
68 See id.
employers' finance and human resources departments performed the worst, falling behind the success rate by a margin of 4 to 9 percent.70

In 2012, the global losses from phishing reached $1.5 billion.71 But those numbers can only be expected to increase as the number of phishing campaigns targeting employees rose 55% in 2015.72 As these numbers indicate, phishing has been, and continues to be, a lucrative form of social engineering for cybercriminals.

b. Messages From Trustworthy Sources

In addition to preying on individual’s gullibility, cybercriminals also take advantage of individuals’ innate tendencies to trust others. When someone receives an e-mail, he or she has an inclination to believe that the sender is who he or she claims to be. Relying on this human characteristic, cybercriminals compromise user’s accounts to gain access to their contact lists, and then send messages to all of the users’ contacts, purporting to be the user.73 For example, the cybercriminal may send a link with a message telling the recipient it has an article “you just have to read” or a video that “you just have to see.” Believing the e-mail came from a friend or colleague, the victim clicks on the link, enabling his or her system to become infected with malware, which the criminal can use to control the machine and gather confidential information or even steal funds.74

c. Baiting

Another form of social engineering is “baiting”: taking advantage of individuals’ curiosity or greed by promising items or goods, such as music or movie downloads, if the user surrenders their login information to a certain site.75 Once the user clicks on the link and takes the bait, his or her computer may become infected with malware that can generate any number of avenues for the cybercriminal to manipulate the user’s information, including steal banking information or other confidential information.76

d. Business E-mail Compromise Scams

74 See id.
One of the more recent and costly trends in social engineering scams is the “business e-mail compromise” scam.\(^77\) In January 2015, the FBI released a public service announcement warning of a sophisticated scam targeting businesses working with suppliers and businesses that regularly perform wire-transfer payments.\(^78\) In a follow-up announcement, the FBI found that these business e-mail compromise scams resulted in losses between October 2013, and August 2015, of nearly $750 million with the number of United States victims exceeding 7,000.\(^79\) Taking into account international victims, the total losses from these scams reached more than $1.2 billion over that same timeframe.\(^80\)

There are three main versions of this scam. The first involves the receipt by a business, which has a long-standing relationship with a certain supplier or vendor, of a spoof e-mail from a fraudster purporting to be that supplier or vendor.\(^81\) The fraudulent e-mail asks the business to transfer funds to a different, fraudulent account.\(^82\) These spoof e-mails appear very similar to the legitimate accounts of the supplier or vendor.\(^83\) Believing the spoof e-mail to be legitimate, employees of the business then follow the fraudster’s instructions and forward the requested money to the fraudulent account.\(^84\) This version of the scheme has been referred to as “The Bogus Invoice Scheme” or “The Supplier Swindle.”\(^85\)

The second version, often known as “CEO Fraud,” involves a criminal impersonating an executive or boss and tricking an individual at an organization into wiring funds to the fraudster.\(^86\) The fraudster preys on the individual’s wish to help a superior or the fear of being reprimanded for not promptly responding to the superior’s communication.\(^87\) This scheme has been described as follows:

The e-mail accounts of high-level business executives (CFO, CTO, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is normally responsible for processing


\(^{78}\) See id.


\(^{80}\) See id.

\(^{81}\) See id.


\(^{83}\) See id.


\(^{85}\) See id.

\(^{86}\) See KREBS ON SECURITY, FBI: $2.3 Billion Lost to CEO Email Scams (Apr. 16, 2016), available at http://krebsonsecurity.com/tag/CEO-fraud/ (last visited June 22, 2016).

these requests. In some instances a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.”\(^{88}\)

This very year, 2016, the FBI stated that these CEO fraud scams had seen a 270% increase since January 2015, with estimated losses over of more than $2.3 billion over the past three years.\(^{89}\)

The third version involves the manipulation of an employee’s personal e-mail account.\(^{90}\) The criminal uses the account to send requests for invoice payments to multiple vendors identified in the employee’s contact list, requesting that the payments be made to a fraudulent bank account controlled by the criminal.\(^{91}\) Oftentimes the business may not learn of the fraudulent requests until they are contacted by the vendor asking about the status of the invoice payment.\(^{92}\) These business e-mail compromise scams affect business of all sizes,\(^{93}\) and, as noted above, have led to significant losses for those businesses.

Whether it is taking advantage of another’s trust, fear, gullibility, or greed, social engineering scams all rely on human actions taking place after the sending of a fraudulent or deceitful message. The fraudster’s actions are not the event directly giving rise to any ensuing loss. Rather, they serve only as the impetus for the action that directly causes the loss: the insured’s employee or representative acting upon the fraudulent instructions. As discussed in more detail below, because of these intervening acts, Computer Fraud coverage does not cover these schemes.

5. **Computer Fraud Policy Forms**

a. **SFAA**

The 2000 version of the SFAA’s Crime Protection Policy provided coverage for:

5. **Computer Fraud**

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:

---


\(^{91}\) See id.

\(^{92}\) See id.

\(^{93}\) See id.
a. To a person (other than a messenger) outside those premises; or

b. To a place outside those premises.  

As of 2012, Insuring Agreement 5 of the SFAA’s Crime Protection Policy provides coverage for computer fraud as follows:

5. Computer Fraud

We will pay for loss resulting directly from the use of any computer to impersonate you, or your authorized officer or employee, to gain direct access to your computer system, or to the computer system of your financial institution, and thereby fraudulently cause the transfer of money, securities or other property from your premises or banking premises to a person, entity, place or account outside of your control.  

This version of the language includes revisions that were made in response to incorrectly reasoned cases suggesting coverage was available when the perpetrator merely used e-mail to contact the insured.  

The 2012 revisions to Insuring Agreement 5 were meant to clarify that coverage was intended only for “‘computer to computer’ transactions,” and that coverage did not apply merely because a computer was somehow tangentially involved in the scheme.  

These dual steps for coverage – fraudulent access to the insured’s computer system and a fraudulent transfer of covered property – clearly demonstrate that coverage is only intended to be provided for hacking situations, and not when an insured voluntarily acts upon a perpetrator’s fraudulent instructions.  

b. ISO

The ISO Computer Fraud insuring agreement formerly provided coverage as follows:

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

---

94 SP 00 01 03 00 (March 2000).
95 SP 00 01 04 12 (April 2012).
97 Id.
98 See Scott L. Schmookler, Computer and Funds Transfer Fraud, in COMMERCIAL CRIME INSURANCE COVERAGE 297, 300 (ABA Press, Randall I. Marmor and Susan Koehler Sullivan eds. 2015).
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”.  

Coverage was specifically limited to loss “resulting directly” from the use of a computer, provided that such use of the computer “fraudulently cause[d]” the transfer of property. Moreover, the property had to be transferred from the insured’s “premises” or “banking premises.” It was not enough to trigger coverage for an insured to allege that fraud had occurred and that a computer happened to be involved. This limitation of coverage demonstrated the original intent of the Computer Fraud insuring agreement: to limit coverage to incidents in which thieves, namely hackers, access an insured’s computer system without the insured’s knowledge and steal the insured’s property, without any intervening action by the insured.100

In 2012, the insuring agreement was revised. Coverage is now provided as follows:

6. Computer and Funds Transfer Fraud

a. We will pay for:

(1) Loss resulting directly from a fraudulent:

(a) Entry of “electronic data” or “computer program” into;

(b) Change of “electronic data” or “computer program” within;

any “computer system” owned, leased or operated by you, provided the fraudulent entry or fraudulent change causes, with regard to Paragraphs 6.a.(1)(a) and 6.a.(1)(b):

(i) “Money,” “securities” or “other property” to be transferred, paid or delivered; or

(ii) Your account at a “financial institution” to be debited or deleted.

(2) Loss resulting directly from a “fraudulent instruction” directing a “financial institution” to debit your “transfer

---

99 CR 00 23 05 06 (2005).
100 See Scott L. Schmookler, Computer and Funds Transfer Fraud, in COMMERCIAL CRIME INSURANCE COVERAGE 297, 298 (ABA Press, Randall I. Marmor and Susan Koehler Sullivan eds. 2015).
account” and transfer, pay or deliver “money” or “securities” from that account.

b. As used in Paragraph 6.a(1), fraudulent entry or fraudulent change of “electronic data” or “computer program” shall include such entry or change made by an “employee” acting, in good faith, upon a “fraudulent instruction” received from a computer software contractor who has a written agreement with you to design, implement or service “computer programs” for a “computer system” covered under this Insuring Agreement.101

While the majority of cases address the former version of the insuring agreement, the revised insuring agreement is similarly designed to limit coverage to incidents of hacking.102 As one commentator has noted:

The requirement that the insured prove a fraudulent entry of data or change to data which caused money to be paid or delivered distinguishes between a circumstance where a hacker gains access and control over the insured’s systems and a circumstance where the insured knowingly transfers money based upon a fraudulent email. The latter, given the obligation to prove a fraudulent entry of data or change to data which caused money to be paid or delivered, is not covered.103

When coverage for computer fraud was originally introduced, the words “computer” and “computer system” had much narrower connotations than they do presently. What was originally thought of as a mainframe that permitted users to communicate morphed first into individual desktops, then tablets, and now even includes televisions. As computing technology has rapidly expanded in the last twenty years, our understanding of what a “computer” and “computing system” are has also broadly expanded. Moreover, as the body of case law surrounding the application of these forms of computer fraud coverage becomes more developed, it may be necessary to continue to revise these coverage forms to ensure that the intent of coverage, to cover incidents of hacking, remains clear.

c. Social-Engineering Coverage

In 2014, the Chubb Group of Insurance Companies created a crime insurance endorsement to protect companies against losses when an employee is deceived into making a payment through e-mail, telephone, or other means to a fraudster purporting

101 ISO CR 00 22 08 13 (Revised 2012).
103 Id.
to be a client or vendor. A release from Chubb regarding the development of this social engineering endorsement reads:

Greg Bangs, vice president and worldwide crime insurance manager for Chubb, explained that a typical crime insurance policy will not insure an organization for such fraud losses [when an employee is tricked into making a payment to a fraudster]. He noted that crime policies respond when money or securities are taken by a third party, but a social engineering scam tricks employees into sending money or securities to a fraudster.

As organizations continue to seek to improve their computer security, social engineering scams are taking aim elsewhere – at human beings,” said Bangs. “It’s easy for a thief to pose as a vendor and request by e-mail that a payment be directed to a new bank account. The company may not realize it was defrauded until weeks or months later when the vendor sends out an overdue payment notice.

Since that time, due to increased market demand, additional insurers have begun offering coverage for social engineering losses. But because the risk of loss from such scams can be almost limitless, many insurers are sub-limiting such coverage with lower limits, often no more than $250,000, although some insurers have begun offering increased limits with significantly higher premiums. And many of the coverages are heavily conditioned upon insureds taking important safeguards to prevent social engineering losses. The fact that social engineering coverage is now available on the market to insure against such losses is evidence that computer fraud policies, already offered by the same insurers, are not intended to provide coverage for social engineering losses. Rather, Computer Fraud coverage was intended to cover only those losses resulting directly from hacking.

II. Parameters to Coverage under the Computer Fraud Insuring Agreement

A. Typical Requirements

Computer Fraud coverage is not intended to cover every fraud that may be perpetrated electronically. Rather, it is solely designed to cover losses resulting directly from an sanctioned entry into an insured’s computing system. Thus, under almost all Computer Fraud insuring agreements, for there to be coverage, the insured needs to prove that (1) that the loss incurred was the loss of covered property, (2) that the alleged loss resulted directly from the use of a computer, and (3) that the use of the computer “fraudulently cause[d] a transfer” of the covered property. Each of the

---


105 See id.

106 See Scott L. Schmookler, Computer and Funds Transfer Fraud, in COMMERCIAL CRIME INSURANCE COVERAGE 297, 301 (Randall I. Marmor and Susan Koehler Sullivan eds. 2015).
elements necessary for a Computer Fraud insuring agreement to provide coverage are discussed below.

B. What is a Computer?

Under the Crime Protection Policy and the former version of the Commercial Crime Policy, for there to be coverage, the loss must result directly from the use of a “computer.” However, that term is typically undefined in these policies, and what instrument can be characterized as a “computer” has changed over time. A computer is no longer a box that sits on someone’s desk. Tablets, smartphones, fax machines, and a number of other similar devices all carry out many of the same tasks that a typical desktop computer does. Even watches and televisions now have the capability of connecting us to the internet. These new avenues of connectivity only further provide criminals with more technological options to carry out their fraudulent schemes electronically. It is just as likely that a fraud will be perpetrated by a handheld device as by a traditional computer. But these policies only provide coverage for loss resulting directly from the use of a “computer,” placing insurers and courts in the potentially challenging position of determining what instrumentality must be used for coverage to exist.

Certain coverage forms may at least provide guidance as to what the term “computer” encompasses. The SFAA’s Computer Crime Policy for Financial Institutions defines “computer system” as “computers with related peripheral components, including storage components wherever located . . . by which Electronic Data are electronically collected, transmitted, processed, stored and retrieved.”\textsuperscript{107} But what constitutes “related peripheral components?” On the one hand, it could narrowly only pertain to electronic devices that are themselves plugged in to a computing system. Conversely, and much more expansively, it could encompass any device that has similar computing capabilities to our traditional understanding of what a computer is. The revised ISO Computer Crime Policy goes farther in its definition of “computer system,” defining it as “[c]omputers, involving 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.”\textsuperscript{108} This definition includes PDAs within its definition of computer system and, arguably, its reference to “other transportable or handheld devices” pertains to today’s smartphones. Insureds will take the position that this phrase is broad enough to encompass any device that can be held in one’s hand. At the very least, they will argue that it is ambiguous, and should be construed broadly in their favor.

Because of the lack of a specific definition, it is important to read closely not only the specific insuring agreement, but also the exclusions and definitions because they may provide insight into what devices would fall within the specific policy’s use of the term “computer.” For example, in \textit{Brightpoint, Inc. v. Zurich American Insurance Co.},\textsuperscript{109}

\textsuperscript{107} TSB 6189.
\textsuperscript{108} CR 00 22 08 13.
the insured argued that the fraudulent use of a facsimile machine constituted the use of a “computer” for coverage. That case involved a dispute over coverage stemming from a loss sustained by one of the insured’s subsidiaries as a result of a scam involving prepaid telephone cards. The subsidiary was a wholesale distributor of prepaid mobile telephone cards in the Philippines. The insured had established a business practice with a Philippine dealer to whom the insured sold phone cards whereby the insured accepted payment by post-dated check, provided the check was accompanied with a bank guarantee certifying the sufficiency of the funds in the dealer’s account and committing to honoring the post-dated checks when the insured presented them on their maturity dates. Copies of the post-dated checks and bank guaranties, as well as the dealer’s purchase orders, were sent to the insured by facsimile. The insured would then purchase the phone cards from the appropriate telecom company and deliver them to the dealer in exchange for the original checks, guaranties, and purchase order.

On two occasions the insured received via facsimile copies of post-dated checks, guaranties, and purchase orders believed to be from the dealer. After receiving the faxed documents, a representative of the insured then went to the telecom company’s office and purchased the cards to be distributed to the dealer. On each occasion, upon taking possession of the cards, the insured’s representative, after taking receipt of the original checks, guaranties, and purchase order, turned over the phone cards to a purported representative of the dealer, who had attended previous similar exchanges. A few days after the last exchange, the dealer attended a meeting with the insured where the dealer denied issuing the purchase orders, denied authorizing its representative to pick up the phone cards, and denied authorizing the banks to issue the guaranties. Ultimately, the insured never received payment for the phone cards delivered to the dealer’s purported representative, nor were the cards ever recovered, resulting in a nearly $1.5 million loss.

The insured contended that the loss was covered because “[t]he 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 it to being defrauded when it released the phone cards to the defrauding party.” The policy’s definition of “Computer Fraud” provided that “[t]he means by which a fraudulent transfer is initiated includes: written, telephonic, telegraphic, telefacsimile, electronic, cable, or teletype instructions.” The insured further provided expert testimony that a facsimile machine was a “computer” for purposes of coverage. While not explicitly deciding the question of whether the facsimile machine was a computer for coverage purposes because the insurer had abandoned that argument at the summary-judgment stage, in a footnote, the court disagreed with the insured’s expert, noting that “we think the common and

110 Id. at *4.
111 Id. at *5.
112 Id.
113 Id. at *5-6.
114 Id. at *7.
115 Id. at *10.
ordinary meaning of computer as widely used and understood in our society and around the world is severely stretched by the inclusion of a facsimile.” 116

While the court’s analysis of the issue is limited, it at least indicates that, absent specific references to instruments that may fall within the scope of “computer,” the plain and ordinary meaning of the term does not encompass all electronic devices that may have some computer-like capabilities. Nonetheless, it is an important reminder to scrutinize all the terms of the applicable Computer Fraud insuring agreement.

C. Use of a Computer

Once the threshold question of whether the instrumentality at issue falls within the scope of what is meant by the policy’s term “computer,” it must then be determined what degree of that computer’s usage is sufficient to trigger coverage. Most policies do not elaborate on this requirement. As a result, insureds sometimes contend that all that is needed is minimal use of a computer that is related to the fraud in any way. But the intent of the coverage is that much more is required; the intent is that the insured’s computer must be fraudulently accessed by someone without authorization for that access, and who abuses that access to manipulate the insured’s computer.

An incorrectly decided case concerning the scope of computer usage is Owens, Schine & Nicola, P.C. v. Travelers Casualty & Surety Co. of America. 117 Even though this opinion was vacated in April 2012, 118 removing any precedential value this case may have had, insureds sometimes still cite it. In Owens, Schine, the insured law firm was contacted via an e-mail by an individual claiming to be an attorney in North Carolina named Donna B. Stepp. The e-mail requested the insured’s assistance in a collection matter for a purported client of Stepp’s located in China. The insured was then contacted by e-mail by an individual named Chen Wu, claiming to be the director of Shenzhen Shan Magnetism Industry Company, Ltd., stating that he had been referred by Stepp and claiming that his company was owed money from a Connecticut company named Dynalock Corporation. 119 Wu then scanned and e-mailed an executed retainer agreement to the insured, agreeing to the insured’s representation for the collection of the alleged debt. 120 By way of another e-mail, Wu notified the insured that Dynalock had sent funds to pay the debt to the insured’s office, and the insured soon thereafter received what was purported to be a Wachovia Bank “Official Check” in the amount of $198,610. 121 The insured deposited the check in its Interest on Lawyers’ Trust Account 122 at Chase Bank. Following instructions in another e-mail from Wu, the insured directed Chase to electronically wire $197,110 from its IOLTA account to an account in

116 Id. at *22 n. 5.
119 Id.
120 Id.
121 Id. at *2-3.
122 Hereinafter IOLTA.
South Korea designated in Wu’s e-mail. It was subsequently determined that the Wachovia check was fraudulent and had not been honored by Wachovia. Chase then debited the insured’s IOLTA account for the $197,110. The insured shortly thereafter submitted documentation to its insurer regarding a claim of computer crime under its policy for the amount debited by Chase.

The pertinent crime policy defined “Computer Fraud” as “[t]he use of any computer to fraudulently cause a transfer of Money, Securities and Other Property from inside the Premises or Banking Premises.” The insurer argued that for computer fraud to exist, the transfer had to occur by way of a “computer hacking” incident, such as through the manipulation of numbers or events through the use of a computer. In contrast, the insured argued that the only required level of computer usage to constitute Computer Fraud was “the use of any computer,” and because the word “use” was not defined or described in the policy, an ambiguity arose to be resolved in favor of the insured. The court agreed with the insured, finding that the policy was ambiguous as to the amount of computer usage necessary to constitute computer fraud. Importantly, in finding that the policy was ambiguous, the court affirmatively stated that a “computer hacking incident” was not required.

Apart from the fact that Owens has no authoritative weight, it was also poorly decided. The insuring agreement provided coverage only for “direct loss” “directly caused by” “[t]he use of any computer to fraudulently cause a transfer.” Under the plain terms of the policy, the covered loss must directly result from the fraudulent use of an insured’s computer. In other words, the fraudulent use of the computer must be the immediate cause of the loss. Tangential uses of computers to commit a fraud are not covered under the insuring agreement. Yet, the Owens court refused to place any boundaries on when computer usage would be so far removed from the loss as to not provide a means for coverage. Extrapolating out the opinion, it is conceivable that a fraudster could send a phishing e-mail to an individual who forwards that e-mail on to several others with it eventually ending up at an insured’s computer. If the insured then suffers a loss from following instructions in the forwarded e-mail, even though it was never an intended beneficiary of it and received the e-mail far down the line, according to Owens, because a computer was used at some point in the loss, there would be coverage. That is a ludicrous result.

---

123 Id. at *3.
124 Id.
125 Id. at *9.
126 Id. at *13.
127 Id. at *18.
128 Id. at *19.
129 Id.
130 Id.
Moreover, *Owens* can be differentiated based on its policy’s specific use of the phrase “use of any computer” in its computer fraud definition. The court in *Universal American Corp. v. National Union Fire Insurance Co. of Pittsburgh, PA*\textsuperscript{131} did just that. In that case, the insured was a health insurance company which provided Medicare managed-care plans, Medicare prescription drug benefits and other insurance products. The members enrolled in health care plans offered by private insurers, which plans received reimbursement payments from the Centers for Medicare and Medicaid Services.\textsuperscript{132} The plans also received payments from plan members themselves. Under such plans, health care providers submitted claims for services provided to plan members. Many of these claims were “auto-adjudicated” through the insured’s computer system, with payments rendered without any manual review.\textsuperscript{133} The insured alleged a loss of more than $18 million from fraudulent claims made against its plans. Most of the claims were submitted by providers directly into the insured’s computer system and were then processed. In some cases, the perpetrators enrolled new members in the plan with the person’s cooperation, in return for which the member received a kickback from the provider. In other cases, the provider used the member’s personal information without that person’s knowledge. In either event, the provider itself did not enroll in the plan.\textsuperscript{134}

The policy had a rider which provided indemnification, in relevant part, for loss resulting “directly from a fraudulent” “entry of Electronic Data or Computer Program” or a “change of Electronic Data or Computer Program within the Insured’s proprietary Computer System.”\textsuperscript{135} The insured argued that this clause covered the entry of fraudulent information even by an authorized user such as a provider and a valid identifier.\textsuperscript{136} The insurer, on the other hand, contended that the policy only provided coverage against computer hackers, “i.e., situations in which an unauthorized user accessed the system and caused money to be paid out.”\textsuperscript{137} The court distinguished the insured’s reliance on *Owens* as the policy at issue in that case defined “computer fraud” to include “the use of any computer to fraudulently cause a transfer” of property. Therefore, the *Owens* court concluded that the policy was ambiguous as to what computer usage was required and, as such, the policy was not restricted to incidents of computer hacking.\textsuperscript{138} By contrast the policy at issue used the specific term “fraudulent entry of electronic data.” The computer fraud clause at issue in *Owens* “was much broader than the clause here in that it did not define how much computer use was required or in what manner the computer had to be used.”\textsuperscript{139} The court refused to accept the insured’s interpretation as it would have improperly expanded coverage to

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{132}] Hereinafter CMS.
\item[\textsuperscript{133}] \textit{Id.} at 850.
\item[\textsuperscript{134}] \textit{Id.} at 851.
\item[\textsuperscript{135}] \textit{Id.}
\item[\textsuperscript{136}] \textit{Id.} at 852.
\item[\textsuperscript{137}] \textit{Id.}
\item[\textsuperscript{138}] \textit{Id.}
\item[\textsuperscript{139}] \textit{Id.} at 852-53.
\end{itemize}
\end{footnotesize}
any fraudulent claim that was entered into its computer by any user, even an authorized user, thereby granting summary judgment to the insurer.\textsuperscript{140}

These decisions illustrate the importance of contract drafting, and the effect that drafting can have on subsequent litigation. In particular, as espoused by Owens, the failure to define certain words within the policy, even the most common terms such as the word “use,” can provide grounds for an insured to argue, and the court to find, ambiguity. But just as importantly, while these cases provide arguments for both sides of the coin as to what type of computer usage is required for coverage to trigger, the answer to that question remains open. Until sufficient case law arises, or the industry sets forth a definition, insurers will face stiff resistance from insureds, and potentially the courts, as to the meaning of this coverage requirement. Logically, it requires some form of direct manipulation of an insured’s computing system. But insureds will continue to contend that a multitude of inventive uses of any computer will be sufficient for coverage.

D. To Fraudulently Cause a Transfer

In addition to meeting the initial instrumentality requirements for coverage, the insured must also demonstrate that the use of the computer fraudulently caused a transfer of covered property. The express use of the phrase “fraudulently cause” in the insuring agreement is designed to limit coverage to incidents of unauthorized access to a computer by a perpetrator, i.e. hacking, and to preclude coverage for losses arising from an insured’s deliberate transfer of funds, even if the transfer was influenced by any of the many forms of social engineering.\textsuperscript{141} It is important to distinguish between fraudulently causing a transaction, and a transaction that is caused by sending fraudulent data. The fact that the word “fraudulently” acts as an adverb modifying the word “cause” makes clear that it must be the act of causing the transfer that is fraudulent. In other words, it must be the access to the computer that is fraudulent or unauthorized. The mere sending of data, by accessing a computer in a perfectly legitimate way (such as sending an e-mail) is not “fraudulently causing a transfer”; it is the sending of fraudulent data in a non-fraudulent way. In short, the placement of the word “fraudulently” in the insuring agreement is critical.

The court in \textit{Universal American Corp.}\textsuperscript{142} demonstrates this limitation of coverage. The court rejected the insured’s argument that the policy’s rider, which provided indemnification for loss resulting “directly from a fraudulent” “entry of Electronic Data or Computer Program” or a “change of Electronic Data or Computer Program within the Insured’s proprietary Computer System,” covered the entry of fraudulent information even by an authorized user such as a provider and a valid identifier.\textsuperscript{143} In finding the clause unambiguous, the court stated that “[t]he policy does not extend as far as providing coverage for fraudulent claims which were entered into the system by

\textsuperscript{140} Id. at 853.

\textsuperscript{141} See Scott L. Schmookler, \textit{Computer and Funds Transfer Fraud}, in \textit{COMMERCIAL CRIME INSURANCE COVERAGE} 297, 301 (Randall I. Marmor and Susan Koehler Sullivan eds. 2015).


\textsuperscript{143} Id. at 852.
The court also found the rider's headings, "Computer Systems" and "Computer Systems Fraud," to "indicate that the coverage is directed at misuse or manipulation of the system itself rather than at situations where the fraud arose from the content of the claim, and the system was otherwise properly utilized, e.g. a fraudulent claim was submitted by an authorized user." Coverage was intended only for an unauthorized entry into the system, in the form of an unauthorized user, such as a hacker, or for unauthorized data, such as a computer virus. The court summarily, and correctly, held: "Nothing in this clause indicates that coverage was intended where an authorized user utilized the system as intended, i.e. to submit claims, but where the claims themselves were fraudulent."

In 2015, the Universal American Corp. decision was affirmed by the Court of Appeals of New York. In so doing, the court provided an important analysis of the policy's use of "fraudulent" that unequivocally limits the scope of the policy to incidents of hacking:

Turning to the language of the Rider, we conclude that it unambiguously applies to losses incurred from unauthorized access to Universal's computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users. The term "fraudulent" is not defined in the Rider, but it refers to deceit and dishonesty (see Merriam Webster's Collegiate Dictionary [10th ed 1993]). While the Rider also does not define the terms "entry" and "change," the common definition of the former includes "the act of entering" or "the right or privilege of entering, access," and the latter means "to make different, alter" (id.). In the Rider, "fraudulent" modifies "entry" or "change" of electronic data or computer program, meaning it qualifies the act of entering or changing data or a computer program. Thus, the Rider covers losses resulting from a dishonest entry or change of electronic data or computer program, constituting what the parties agree would be "hacking" of the computer system. The Rider's reference to "fraudulent" does not also qualify what is actually acted upon, namely the "electronic data" or "computer program" itself. The intentional word placement of "fraudulent" before "entry" and "change" manifests the parties' intent to provide coverage for a violation of the integrity of the computer system through deceitful and dishonest access.

Similarly, in Pestmaster Services v. Travelers Casualty & Surety Co. of America, the court held that the placement of the adverb "fraudulently" was important because it signified that the explicit act of causing the transfer must be fraudulent or unauthorized. The court noted that if a person takes advantage of authorized access to

---

144 Id.
145 Id.
146 Id.
147 Id.
the insured’s computer to request an improper transfer, the perpetrator has not “fraudulently caused” the transfer. In that case, Pestmaster, the insured, hired HRC Connections, Inc., to handle employee training, background investigations, drug screening, regulatory compliance, and personnel files. The insured also hired a payroll company, owned by HRC’s sole shareholder, to handle the preparation of the insured’s payroll, payment of payroll taxes, and delivery of payroll checks. Pestmaster entered into an agreement with the payroll company whereby the payroll company was authorized to obtain payment of its approved invoices by initiating ACH transfers of funds from the insured’s bank account to its own bank account.\textsuperscript{150} For each payroll period, the payroll company would prepare and deliver invoices to the insured reflecting amounts owed for employee salaries and payroll taxes. Once Pestmaster approved the invoices, the payroll company would initiate the transfer of funds from the insured’s bank account to its own. Because of a lag in time between the completion of the payroll and the remittance of the payroll taxes, the payroll company’s account would retain the funds for several days until it was required to pay the taxes.\textsuperscript{151} Pestmaster eventually learned that the payroll company had not been submitting payroll taxes to the IRS, and the IRS notified the insured of the unpaid taxes.

Pestmaster sought to recover its loss associated with the payroll taxes under its policy which covered loss resulting from “Computer Fraud,” defined as “[t]he use of any computer to fraudulently cause a transfer of Money, Securities or Other Property from inside the Premises or Banking Premises.”\textsuperscript{152} In construing the definition of “Computer Fraud,” the court stated that it “occurs when someone ‘hacks’ or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer or otherwise uses a computer to fraudulently cause a transfer of funds.”\textsuperscript{153} The insured urged the court to adopt an interpretation of this language to mean that any use of a computer to cause a fraudulent transfer rather than “use of a computer to fraudulently cause” such a transfer was sufficient for coverage.\textsuperscript{154} Relying on the holding in \textit{Universal American Corp.}, the court reasoned:

However, there is an important distinction between “fraudulently causing a transfer,” as “Computer Fraud” is described in the Policy, and Pestmaster’s interpretation of “Computer Fraud” as “causing a fraudulent transfer.” . . . In this case it is undisputed that Pestmaster authorized Priority 1 to initiate ACH transfers from its account to Priority 1’s account so that Priority 1 could pay Pestmaster’s payroll and payroll taxes. In its Opposition, Pestmaster does not argue – nor could it – that Priority 1 was an unauthorized user or hacker or that Priority 1 somehow subverted Pestmaster’s computer in the actual transfer of funds into Priority 1’s account. It is also undisputed that after the transfer of the funds was completed, Priority 1 used the money to pay its own obligations rather than to pay Pestmaster’s obligations as required by their agreement.

\textsuperscript{150} \textit{Id.} at *5.  
\textsuperscript{151} \textit{Id.}  
\textsuperscript{152} \textit{Id.} at *14.  
\textsuperscript{153} \textit{Id.} at *19.  
\textsuperscript{154} \textit{Id.}
However, Priority 1’s fraudulent conduct occurred only after the authorized transfer had been completed and the money was transferred to Priority 1’s account pursuant to its agreement with Pestmaster.

Therefore, Priority 1’s conduct does not constitute “Computer Fraud” as defined by the Policy because the transfer of funds was at all times authorized and did not involve hacking or any other unauthorized entry into a computer system.155

Both the trial court holding and the subsequent affirmation of Universal American Corp., as well as the opinion in Pestmaster, demonstrate that there is an important distinction between fraudulent requests to an authorized user, which are then acted upon, and an unauthorized party fraudulently causing a transfer by the use of a computer. It is the use of the computer that must fraudulently cause the insured to suffer a direct loss for coverage to be triggered. By contrast, an insured’s conscious decision to make a transfer, even if influenced by fraudulent instructions, is insufficient for coverage.

The decision Kraft Chemical Co. v. Federal Insurance Co.156 espouses this principle. There, a client ordered certain products from the insured, who, in turn, placed a purchase order with a third-party company for the products. After exchanging legitimate e-mails with the third-party company, the insured subsequently received an e-mail from a fraudster misrepresenting the bank account information for the third-party company and indicating that future and existing payments should be made to the changed bank account.157 The insured then wire transferred funds to the new account without verifying the new bank account information.158 The insured sought coverage under a Computer Fraud insuring agreement that covered the “direct loss” from the unauthorized (1) entry into or deletion of data from a computer system, (2) change to data elements or program logic of a computer system, or (3) introduction of instructions, programmatic or otherwise, which propagate themselves through a computer system.159

The court held that the mere sending of an e-mail is not an unauthorized entry or change to a computer system that would fall within the scope of the policy.160 Citing to Universal American Corp. for the proposition that “fraudulent entry” “unambiguously applied to losses incurred from unauthorized access to [the insured’s] computer system, and not to losses resulting from fraudulent content submitted to the computer system by authorized users,” the court found that the insurer had met its burden of showing that there was no violation of the insured’s computer system through deceitful and dishonest access by the fraudster.161

155 Id. at *19-21.
157 Id.
158 Id. at *4.
159 Id. at *8.
160 Id. at *15-16.
161 Id. at *17-19.
As these cases hold, in focusing upon the phrase “fraudulently cause” or “fraudulent entry” of data, it is clear that the true intent of the Computer Fraud insuring agreement is to only cover incidents where an unauthorized user gains direct access to an insured’s computer or computer system. In other words, hacking is the peril covered by the insuring agreement. Social engineering schemes, no matter how elaborate, are simply not afforded coverage because an insured cannot demonstrate the fundamental requirement to coverage that the access to its computer was fraudulent.

E. Covered Property

Assuming an insured is able to demonstrate that its alleged loss was fraudulently caused by the use of a computer, an insured must additionally prove that the alleged loss is one covered by the policy. Generally speaking, most policies enumerate the covered losses as “money,” “securities,” or “other property.” Each of these terms is, in turn, defined within the policy. Whereas “money” and “securities” are limited in their scope, “other property” is broadly defined as “any tangible property other than ‘money’ and ‘securities’ that has intrinsic value.” As discussed below in Brightpoint, this definition can provide a wide swath for an insured to contend that the loss at issue falls within the catchall “other property” category.

As noted, the terms “money” and “securities” are relatively limited categories of covered property, and courts should be bound by the specific definitions of those terms. In what is generally considered to be first case involving computer fraud coverage, the court in Royal American Group, Inc. v. ITT Hartford faced the question of whether the computer theft of long distance access codes from a long distance telephone network constituted a covered loss. Royal American, the insured, provided customers with access to its long-distance telephone network for a fee. The network was based on contracts Royal American had with long-distance providers, which permitted Royal American to access these companies’ individual long-distance networks for use by Royal American’s customers. Royal American’s customers connected to this network by using a “1-800” telephone number and security code, which was stored on a computer at Royal American’s facilities. An unknown individual using another computer gained access to Royal American’s computer, stole the security code, and gained unauthorized access to Royal American’s network resulting in $37,489.38 in long-distance charges to Royal American’s accounts with its long distance providers.

Royal American sought to recover the unauthorized long-distance charges under its policy’s computer fraud coverage, which covered loss of “‘Money,’ ‘Securities’ and ‘Property Other than Money and Securities’” resulting directly from computer fraud. The insurer argued that Royal American’s loss was not covered because its contracts with

---

162 ISO CR 00 22 08 13.
165 Id. at *1-2.
166 Id. at *2.
the long distance carriers did not fall within the scope of the policy’s “covered property.”\footnote{Id. at *3-4.} The trial court determined that the contracts to use long distance networks fell within the scope of the definition of “securities,” which the policy defined as “negotiable instruments and nonnegotiable instruments or contracts representing either ‘money’ or other property . . . .”\footnote{Id. at *4-5.} Specifically, the trial court found that Royal American’s contracts were “contracts representing . . . other property” and that “the damage resulting from these contracts which represent [Royal American’s] right to utilize the property of the carriers is clearly Covered Property under the Crime General Provisions definition.”\footnote{Id. at *5.}

The appellate court disagreed with the trial court’s determination. The court cited two dictionary definitions of the term “securities” to support its finding that the plain and ordinary meaning of the term is “a written obligation, evidence, or document of ownership or creditorship (as a stock, bond, note, debenture, or certificate) giving the holder the right to demand and receive property not in his possession” or “evidences of debts or of property” or “evidences of obligations to pay money or of rights to participate in earnings and distribution of corporate, trust, and other property.”\footnote{Id. at *6 (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 2054 (1961) and BLACK’S LAW DICTIONARY 1522 (4th ed. 1968)).} Relying on the plain and ordinary meaning of the term “securities,” the court found that the policy’s definition of “securities” did not vary materially from these definitions and, therefore, refused to stretch the policy’s term to include Royal American’s contractual right to access another company’s long distance network.\footnote{Id. at *6-7.} Moreover, even assuming that the contracts constituted securities under the policy, the policy provided coverage only for “loss of, and loss from damage to, Covered Property.”\footnote{Id. at *7.} The insured could not show how the unauthorized long-distance charges resulted in a loss or damage to its rights under those contracts.\footnote{Id.} Therefore, the court held that Royal American’s contractual liability for the unauthorized long distance charges was not covered property under the policy, reversing the trial court’s decision.\footnote{Id. at *13-14.}

In \textit{Brightpoint}, however, the court found that the insured’s loss of phone cards fell within the broad category of “other property.” The insurer Zurich argued that that the phone cards were not “Covered Property” as defined in the policy as they were not “Money,” “Securities,” or “Property Other than Money and Securities.”\footnote{Id. at *10.} Zurich contended that the loss was purely the economic value of the phone cards and not the cards themselves. Therefore, the cards were not “tangible” property.\footnote{Id.} While the court recognized that to fall within the “Property Other than Money” category the property needed to be “tangible,” have “intrinsic value,” and “not be money, securities or a property specifically listed as not covered,” the court disagreed with Zurich’s contention.

\begin{itemize}
  \item \footnote{Id. at *3-4.}
  \item \footnote{Id. at *4-5.}
  \item \footnote{Id. at *5.}
  \item \footnote{Id. at *6 (quoting WEBSTER’S THIRD NEW INTERNATIONAL DICTIONARY 2054 (1961) and BLACK’S LAW DICTIONARY 1522 (4th ed. 1968)).}
  \item \footnote{Id. at *6-7.}
  \item \footnote{Id. at *7.}
  \item \footnote{Id.}
  \item \footnote{Id. at *13-14.}
\end{itemize}
that the phone cards did not meet those requirements.\textsuperscript{177} In finding the holding in \textit{Peoples Telephone Co., Inc. v. Hartford Fire Insurance Co.},\textsuperscript{178} relied upon by Zurich, that telephone cards were not tangible property to be unpersuasive, the court determined that the prepaid cards were in fact tangible as they could be “physically transferred to another.”\textsuperscript{179} Moreover, the court determined that the prepaid cards had intrinsic value as each had a specific value assigned to it. The court stated: “While a cellular phone is engineered to extract a specific value from each prepaid telephone card, we do not regard that technological feature to detract from the intrinsic monetary values assigned to the cards.”\textsuperscript{180} Therefore, the cards were “covered property” under the policy.

As demonstrated by \textit{Brightpoint}, the third “other property” category grants courts a certain degree of latitude in determining whether a loss is a covered loss. “Intrinsic value” is a nebulous term that depends on facts and circumstances of the particular situation or property at issue.\textsuperscript{181} Therefore, an insurer needs to be cognizant of the fact that an insured will contend that every loss has some form of intrinsic value sufficient to fall within the scope of “covered property.”

F. Standard of Causation - “Resulting Directly From”

The requirement that the insured’s loss result directly from the fraudulent use of a computer is a vital limitation placed on the scope of the Computer Fraud insuring agreement. This requirement evidences a clear intent that there must be a direct and immediate causal link between the computer fraud and the loss, thereby placing an important limit on what losses are recoverable. The intent is to cover only those losses resulting \textit{immediately} from the fraudulent entry of data. This leaves out any losses resulting from a false statement that is sent to an insured by e-mail, and that the insured then acts on voluntarily. When the term “directly” is properly understood, it becomes clear that the only loss that could result \textit{immediately} from the fraudulent entry of data is a loss from hacking. Hacking involves no intermediary steps between the use of a computer and the loss. Scams involving social engineering lack the direct causal link because there is an intervening act between the fraudulent activity and the loss: a knowing decision by the insured’s representative to act on the fraudulent communication. Despite the clear import of the word “directly,” not all courts agree on its meaning in the context of commercial crime policies, including Computer Fraud insuring agreements.

1. History of the Causation Language

\textsuperscript{177} \textit{Id.} at *14-16.
\textsuperscript{178} 36 F. Supp. 2d 1335 (S.D. Fla. 1995).
\textsuperscript{179} 2006 U.S. Dist. LEXIS 26018, at *14-16.
\textsuperscript{180} \textit{Id.} at *16.
\textsuperscript{181} \textit{See In re Northwest Greyhound Lines}, 251 P.2d 607, 612 (Wash. 1952) (stating that the term “intrinsic value” is not self-defining and finding a meaning of the term “require[s] consideration of all the facts and circumstances relevant to a particular case or situation”).
Before 1980, fidelity insurance policies provided coverage for “loss through” a covered event or transaction. Typical language of these earlier policies provided coverage for:

Any loss through any dishonest or fraudulent act of any of the employees including loss of property for any such act of any of the employees.\(^{182}\)

Over time this “through” language was broadly construed by courts by applying tort concepts of causation, essentially turning what was intended to be first-party insurance coverage into liability insurance coverage. Insureds argued, and courts accepted, constructions of this language to find coverage in situations in which coverage was never intended to be afforded.\(^{183}\)

Largely in response to this overly expansive approach to the policy’s language, in the 1980’s, the causation language of fidelity insurance policies underwent a significant change. The industry modified the causation language from “loss through” to “loss resulting directly from.”\(^{184}\) The express intent behind this modification was to refine and provide clarity to courts that fidelity insurance was limited to losses suffered by insureds directly resulting from the covered action and to preclude coverage for an insured’s liability to third parties.\(^{185}\) As explained by the Seventh Circuit in First State Bank of Monticello v. Ohio Casualty Insurance Co.,\(^{186}\) tort causation standards are inappropriate when dealing with the construction of an insurance policy:

[S]ome courts have continued to look to proximate cause and other causation principles borrowed from tort law to decide loss-causation issues under the financial-institution bond. . . . This approach is misdirected; tort-causation concepts like proximate cause, “substantial factor” causation, and intervening cause are inappropriate here. In particular, the concept of proximate cause is problematic in this context; proximate cause is a shifting standard that draws the line of causation “because of convenience, of public policy, of a rough sense of justice . . . . It is practical politics.” . . . Insurance-coverage cases are not concerned with the philosophical social-duty underpinnings of tort law.

\(^{182}\) See Gary J. Valeriano, Direct Loss and Causation, in COMMERCIAL CRIME INSURANCE COVERAGE 351, 354 (Randall I. Marmor & Susan Koehler Sullivan eds., 3d ed. 2015).

\(^{183}\) See Fidelity & Deposit Co. of Md. v. USAFORM Hail Pool, Inc., 523 F.2d 744, 757 (5th Cir. 1975) (stating that “[n]either the bond language itself . . . nor our 1972 opinion requires causation per se as an element of recovery” and that the bond only “requires that there be a fraudulent or dishonest act and a loss to the insured corporation ‘through’ such an act”).


\(^{186}\) First State Bank of Monticello, 555 F.3d at 570; see also Prudential Prop. and Cas. Ins. Co. v. Swindal, 622 So.2d 467, 470 (Fla. 1993) (“Florida law has long followed the general rule that tort law principles do not control judicial construction of insurance contracts.”).
By modifying the “loss through” language, the industry intended to narrow the scope of the causation requirement for coverage. Applying a “but for” standard, or even a “proximate cause” standard, would render the revised “loss resulting directly from” language all but meaningless.

2. General Rules of Construction: The Ordinary Meaning of “Directly” Should Prevail

Insurance policies are subject to the same rules of construction as other contracts. It is well settled that in construing contractual language, a court is to ascertain the intent of the parties at the time of contracting. A basic tenet of that rule is that a court should give the terms used in an insurance policy their plain and ordinary meaning, unless the parties’ intent, as expressed by the policy, indicates that an alternative interpretation was intended. Only when an ambiguity arises will a court examine beyond the policy’s plain meaning to determine what a term means. An ambiguity arises when the words in a policy are susceptible to more than one reasonable interpretation. It does not arise when the insured and insurer merely disagree over the interpretation of the word or provision, nor does it exist because the word or provision at issue is undefined in the policy.

Applying these principles, the ordinary meaning of the word “directly” is clear and should prevail. “Directly” means “immediately,” and without any intervening cause, as evidenced by many dictionary definitions. The American Heritage Dictionary of the English Language defines “directly” as follows:

1. In a direct line or manner, straight

2. Without anyone or anything intervening; immediately

---


189 See, e.g., First State Bank of Monticello, 55 F.3d at 568.


191 See, e.g., Performance Autoplex II. Ltd. v. Mid-Continent Cas. Co., 322 F.3d 847, 854 (5th Cir. 2003).


Webster’s Ninth New Collegiate Dictionary defines the term as “immediately after.” The Collins English Dictionary defines “directly” as:

1. In a direct manner
2. At one; without delay
3. Immediately; just

The Collins English Thesaurus lists the following words as synonyms of “directly”:

1. Straight, unswervingly, without deviation, by the shortest route, in a bee line.
2. Immediately, promptly, instantly, right away, straightaway, speedily, instantaneously, pronto.

Black’s Law Dictionary defines “directly” as:

1. In a straightforward manner.
2. In a straight line or course.
3. Immediately.

Black’s Law Dictionary further defines “direct” as “straight, and undeviating . . . immediate.” And finally, online dictionary sources define “directly” in a similar manner:

1. In a direct way
2. In a straight or direct line from a particular position
3. Without delay

Dictionary.com defines “directly” as:

1. In a direct line, way, or manner; straight
2. At once; without delay; immediately

---

195 MERRIAM WEBSTER (1986).
196 10th Ed. 2009 William Collins Sons & Co. Ltd.
198 BLACK’S LAW DICTIONARY 527 (9th ed. 2009).
199 Id. at 525.
As can be seen from these various definitions, the plain and ordinary meaning of “directly” is “immediately.” In the context of the Computer Fraud insuring agreement, the phrase “resulting directly from” should be commonly understood to mean that there can be no intervening agent or action between the computer fraud and the covered loss. Therefore, because the use of a computer must immediately cause the loss, the insuring agreement is intended to cover only the unauthorized entry into an insured’s computer system or, in other words, hacking. When an insured follows the instructions in a fraudulently created e-mail or some other phishing scam, the fraudulent use of a computer is not the immediate cause of any ensuing loss. Instead, it is the insured’s conscious decision to follow the instructions, and the insuring agreement is not intended to cover such situations because the fraud did not immediately result in the loss.

3. Direct Means Direct

The phrase “direct means direct” has become a commonly used maxim among insurers to explain to courts the requisite casual connection between an insured’s loss and the covered event. The Ninth Circuit decision in Vons Companies, Inc. v. Federal Insurance Co. is generally regarded as the first case to use the “direct means direct” terminology. In Vons, the court rejected the insured’s argument that the policy covered losses paid by the insured to third parties for which the insured was liable. In RBC Mortgage Co. v. National Union Fire Insurance Co. of Pittsburgh, the court found that the phrase “resulting directly from” was clear and unambiguous and that it did not provide coverage for losses incurred as part of a settlement agreement with a third party. In reaching that conclusion, the court expressly rejected the insured’s contention that a “proximate cause” standard was the proper standard to apply in determining whether a loss was direct or indirect. The court stated:

[The proximate cause analysis simply is too broad to capture accurately the intent behind the phrase “loss resulting directly from.” . . . To equate “loss resulting directly from” with “loss proximately caused by” requires a strained reading of “direct loss,” which is a much narrower concept than “proximately caused loss.” This is because a proximate cause “need not be the sole cause nor the last or nearest cause. It is sufficient if it concurs with some other cause acting at the same time, which, in combination with it, causes the injury.”]

This reasoning is in line with the traditional nature of fidelity bonds to provide first-party insurance as well as the “direct” language of the policy. As the RBC Mortgage Co. court noted, adopting a proximate cause standard would widen the potentially covered losses to include losses stemming from a covered event that are only tangentially related to that event, effectively ignoring and rendering inconsequential

202 212 F.3d 489, 492-93 (9th Cir. 2000).
204 Id. at 736-37.
205 See Lynch Props. Inc. v. Potomac Ins. Co., 962 F. Supp. 956, 964 (N.D. Tex. 1996), aff’d, 140 F.3d 622 (5th Cir. 1998) (fidelity coverage is “meant to insure . . . only against immediate harm from employee dishonesty”).
the use of the word “direct.”\textsuperscript{206} The “resulting directly from” language requires an immediate causal connection between the dishonest or fraudulent conduct and the loss.\textsuperscript{207}

The majority of courts have adopted the common-sense “direct means direct” approach. In 2012, the Sixth Circuit put forth an analysis of relevant cases across the country discussing the “resulting directly from” language. While acknowledging that there is a split in authority in its interpretation, the court recognized that the “direct means direct” interpretation was the most commonly held:

The weight of the authorities define “directly” as meaning “immediate” – known by some as the “direct is direct” approach – although other jurisdictions espouse a “proximate cause” approach. . . . The debate over the “directly” language first began when the Surety Association revised its standard fidelity-contract form to replace the term “loss resulting through” with “directly resulting from.” . . . But regardless of the impetus for the “directly resulting from” language within employee fidelity policies, it remains the case that state courts and federal courts interpreting state law are split on how to interpret the provision. The policies these courts have interpreted—although differing in industry, content, and specific conduct covered—share two fundamental features: (1) they are fidelity contracts to protect against employee theft, fraud, destruction of property, or other misfeasance against the insured; and (2) they protect against a loss “directly resulting from,” “resulting directly from,” “resulting solely and directly from,” or “directly caused by” said fraud, theft, or other misfeasance. They are not liability policies, which protect the insured against liability for losses incurred by third parties due to actions by the insured’s employees.\textsuperscript{208}

Under the “direct means direct” approach, the inevitable conclusion is that the insured’s loss must immediately flow from the covered act, without any intervening agent or event. This is the correct intent and interpretation of the phrase.

4. Proximate Cause

Notwithstanding the clear meaning of the word “directly,” a number of courts have incorrectly interpreted the phrase “resulting directly from” as requiring application of the proximate-causation concept found in the tort context. \textit{Jefferson Bank v. Progressive Casualty Insurance Co.}\textsuperscript{209} is a case often cited by insureds for the proposition that “resulting directly from” equates to proximate cause. In that case, the


\textsuperscript{209} 965 F.2d 1274 (3d Cir. 1992).
insured bank sought to recover losses on loans secured by encumbered collateral. The perpetrator had presented title documents that were signed by his co-conspirator and not an actual notary. Insuring Agreement E of the policy provided coverage for loan losses “resulting directly from” the insured extending credit on the basis of certain enumerated loan documents used in transacting the loan that were stolen or contained forgeries or alterations.210

In construing the “resulting directly from” language, the court initially recognized that it suggested a stricter standard of causation than mere proximate cause, stating that “the words ‘resulting directly from’ suggest a requirement beyond that the cause be substantial, for the words imply that the loss must flow ‘immediately,' either in time or space from the forged signature.”211 Nonetheless, the court found that, under Pennsylvania law, proximate cause was the proper standard and that requiring “immediacy” was inappropriate.212 The court based its conclusion on two factors. First, the court examined cases construing “direct cause of loss” to mean “proximate cause of loss.” Strangely, the cases relied the court relied on dealt with whether direct losses as a result of windstorms equated with proximate losses that would be covered under the respective policies. Believing the analyses presented by those courts to be analogous, the court predicted that “resulting directly from” would mean “proximately caused by” under Pennsylvania law.213 Even more interesting is the court’s second reason for applying the proximate-cause standard. Despite its earlier acknowledgment that the phrase “resulting directly from” implied flowing immediately, the court stated that “‘direct cause’ or ‘immediate cause’ is a nebulous and largely indeterminate concept” that did “not enjoy favor under Pennsylvania law.”214 The court then explained that, in negligence cases, the courts of Pennsylvania examined “substantiality,” rather than “immediacy” in determining proximate cause.215 The court summarized its holding as:

Given the difficulty and confusion that results from applying a “nearest cause” or “immediate cause” standard, we do not believe that the parties intended to contract for it. Instead, we believe that in this contract “resulting directly from” means “proximately caused by.”216

Although the case involved Insuring Agreement E, and not the Computer Fraud insuring agreement, to the extent an insured relies on this opinion in a computer fraud coverage dispute, the court’s decision can be criticized in several respects. First, completely disregarding the very terms of the policy, the court incorrectly imports torts concepts into its analysis. In doing so, the court essentially rewrites the very terms of the contract that it initially recognized imposed a stricter and narrower standard than proximate cause. Second, the court’s reliance on cases involving storm damage, and what attendant damages may have resulted from the storms, is misplaced. Contrary to

210 Id. at 1277.
211 Id. at 1281.
212 Id.
213 Id. at 1281.
214 Id.
215 Id.
216 Id. at 1282.
what the court espouses, those cases are not analogous as they involve large natural-occurring events that can lead to damage in a multitude of ways and differentiating between what damages were directly caused by wind as opposed to rain, or some other storm-related phenomena, is incredibly difficult, if not impossible. In Jefferson Bank, such similar overlapping elements were not present to justify relying on those cases. Lastly, the court’s suggestion that a “direct cause” standard is too nebulous a concept to apply is bizarre, given that the court adopts an even more indeterminate concept in its place. The idea of identifying whether a loss resulted immediately from some specific action is much more ascertainable than determining whether there was some attenuated casual connection between the two. Rather than clarify what the policy would cover, the court only exacerbated the issue. It is easy to see why decisions like First State Bank of Monticello are highly critical of the proximate-cause approach to causation. Unfortunately, some courts have continued to apply this misguided standard.  

First National Bank of Louisville v. Lustig is an important case that interprets the phrase “resulting directly from.” The case is not well reasoned, but its holding is narrow. There, the insured claimed coverage under Insuring Agreement A for over $20 million in losses from eight failed loans caused by the dishonest acts of one of its loan officers. The loan officer falsified the credit records of borrowers and guarantors to enable them to obtain loans which they could not afford. When the loans defaulted, the insured bank suffered those losses and sought recovery, which the insurer denied. The insurer argued, among other things, that the bank’s losses did not result directly from the loan officer’s fraudulent conduct, but, rather, resulted from the decline in the general real estate market and the borrower’s poor financial decisions. The court disagreed, stating:

The Sureties would have us read the requirement that the loss be directly caused by the dishonest or fraudulent act narrowly. Such a reading would, however, all but eliminate coverage for loans made because of dishonest or fraudulent acts. There will always be some intervening cause for the failure of these loans to be repaid; otherwise the bank would suffer no loss.

In this context, the court noted that a “[a] loss is directly caused by the dishonest or fraudulent act within the meaning of the Bond where the bank can demonstrate that it would not have made the loan in the absence of the fraud.”

Essentially, the court articulated a “but-for” causation test in determining whether the losses were directly related to the employee’s fraud: A loss is “direct” if “but for” the

\[\text{\textsuperscript{217}}\text{See, e.g., Resolution Trust Corp. v. Fidelity & Deposit Co. of Maryland, 205 F.3d 615, 655 (3d Cir. 2000); Mid-America Bank of Chaska v. American Casualty Co., 745 F. Supp. 1480 (D. Minn. 1990).}\]
\[\text{\textsuperscript{218}}961 F.2d 1162 (5th Cir. 1992).\]
\[\text{\textsuperscript{219}}\textit{Id.} at 1164.\]
\[\text{\textsuperscript{220}}\textit{Id.} at 1167.\]
\[\text{\textsuperscript{221}}\textit{Id.} at 1167-68.\]
\[\text{\textsuperscript{222}}\textit{Id.} at 1168.\]
employee’s fraud, the insured would not have made the loans. Although it is disastrous—and dead wrong—to interpret “resulting directly from” as requiring mere but-for causation, ultimately, Lustig’s holding is narrow. It holds only that a bank’s loss from nonpayment of loans is covered if the bank makes the loan because of employee dishonesty, even though there will always, without fail, be an intervening factor causing the loss: the borrower’s default. Had the court required that there be no intervening factors between the employee dishonesty and the bank’s loss, then there would never be coverage.

Further suggesting the narrowness of the Lustig holding are subsequent decisions from the Fifth Circuit that have construed the phrase “resulting directly from” much more narrowly than the court did in Lustig. In Lynch Properties v. Potomac Insurance Co.,223 for example, the court held that an employee’s embezzlement of a customer’s funds resulted in a direct loss to the customer, but only an indirect loss to the insured when it replaced the embezzled funds. Importantly, the court found the policy’s “resulting directly from” language to be unambiguous and that its intent was clear to only provide coverage for losses directly incurred by the insured.224 Similarly, in BJ Services S.R.L. v. Great American Insurance Co.,225 the court refused to find coverage for losses incurred when the insured was liable to repay funds taken from third parties by its employees. The court stated that the policy made clear that only a loss resulting directly from employee dishonesty was covered. “[W]hen an insured incurs liability to a third party – whether in contract or tort – as a result of employee misconduct, financial loss resulting from that liability is not ‘directly’ caused by the employee misconduct and therefore is not covered by fidelity bonds containing direct-loss language.”226 The BJ Services case is also important in that it approvingly cites to Vons in its analysis. In each of these cases, the employee theft played a substantial role in the insured’s eventual loss. Seemingly under Lustig’s “but for” approach, the losses would be covered. But the courts were clear that the employee’s actions were not sufficient to demonstrate that the insureds’ losses directly resulted from those dishonest acts. Therefore, Lustig is limited to its specific facts.

Even though the majority of courts have adopted the “direct means direct” approach, precluding coverage for losses that do not immediately result from the covered event, there are enough cases mistakenly utilizing a “proximate cause” or similar tort analysis in construing the phrase “resulting directly from” that insurers need to be made aware of the possibility that a court will mischaracterize the intent of the policy language.

5. Cases Interpreting the Phrase “Resulting Directly From” in the Context of Computer Fraud

Unfortunately, the lack of unanimity on the meaning of “directly” is present in cases interpreting Computer Fraud insuring agreements, as well. True to the overall

---

224 Id. at 962.
225 539 Fed. Appx. 545, 549-50 (5th Cir. 2013).
226 Id. at 549.
tendencies discussed above, the majority of courts interpret the phrase “resulting directly from” in the Computer Fraud insuring agreement to preclude coverage for losses that do not flow immediately from the fraudulent use of a computer. But there are exceptions, with a minority of courts continuing to apply a “proximate cause” standard of causation.

Pestmaster Services is a case correctly applying the causation requirement. In Pestmaster, the court held that the payroll company’s use of a computer was merely incidental to, and not directly related to, the payroll company’s misuse of the insured’s funds, reasoning that that the insured’s loss did not “flow immediately” and “directly” from the payroll company’s use of a computer.227 Although the payroll company accessed the insured’s account via a computer, the court determined that there was no loss when the funds were initially transferred to the payroll company because the payroll company was authorized to make such transfers. The losses did not occur until after the authorized transfers had taken place when the payroll company decided to use those funds for its own benefit rather than pay the insured’s payroll taxes.228 Thus, there was no coverage.

In Methodist Health System Foundation, Inc. v. Hartford Fire Insurance Co.,229 the insured sought to recover losses from its investment portfolio as a result of the Bernie Madoff Ponzi scheme. Over the course of two separate purchases, the insured invested $6.7 million worth of shares in Meridian Diversified Fund, Ltd., a mutual fund that invested in hedge funds. Meridian, in turn invested a portion of its holdings in Tremont Hedge Fund, which in turn invested a portion of its holdings in a fund managed by Madoff.230 While the insured’s shares had risen substantially in value over four consecutive years, those investments soon soured. In late 2008, amidst the widespread economic recession, the value of the insured’s shares decreased substantially due at least in part to the discovery of the Madoff scam, which caused Tremont to suffer losses that ultimately affected the insured via its investment with Meridian.231 The insured filed a claim under the Computer Fraud insuring agreement of its commercial crime policy, contending that the insuring agreement covered the losses because Madoff had used a computer to generate false documents that misled investors and gave the appearance of a legitimate investment operation.232 The insurer denied coverage on the grounds that there was no covered computer fraud loss and that the losses were indirectly related to the Madoff scheme.233 The insurer subsequently moved for summary judgment.

The policy’s computer fraud provision read, in relevant, part: “We will pay for loss of and loss from damage to ‘money,’ ‘securities’ and ‘other property’ following and directly related to the use of any computer to fraudulently cause a transfer of that

228 Id. at *23.
230 Id.
231 Id. at 494-95.
232 Id. at 495
233 Id.
property from the inside ‘premises’ . . .” to a person or place outside those premises.234 Relying upon Louisiana law and persuasive authority from the Northern District of Texas, the court focused on the “directly related to” language in the policy to find that the insured’s losses were too far removed from the Madoff scam to be covered.235 While the Ponzi scheme was a contributing factor to the insured’s losses, it was not the direct cause of the loss. The court held that “only Tremont suffered losses ‘resulting directly from’ the Madoff Ponzi scheme; Plaintiff was too far removed from the Madoff scheme in order to recover under a ‘direct loss’ provision because Plaintiff invested in Meridian, who invested in Tremont.”236 The policy’s use of the words “directly related to” indicated an intent to provide coverage only for direct losses to the insured. Thus, the insured’s losses were not covered “because Plaintiff’s investment in Meridian was too many steps removed from Madoff’s fraud.”237

Similarly, in Brightpoint, the insured argued that all that was required for coverage was the use of a computer followed by a theft that was in some way connected to the use of the computer.238 The court rejected the insured’s argument, finding its interpretation of the term “directly related” to “represent[] a distortion of the policy terms” and holding that the insured’s loss did not flow immediately from the use of the facsimile.239 The court noted that, taken to extremes, coverage could apply if a fraudster sent an e-mail indicating that he was coming to the insured’s offices to buy phone cards, and he then showed up in person to complete the transaction with counterfeit money.240 The court found it “obvious” that coverage was not meant to apply in that “contrived example” or in the circumstances presented to the court because, in both cases, “intervening events or circumstances became the direct, proximate, predominate and immediate cause of” the insured’s loss.241

Pinnacle Processing Group, Inc. v. Hartford Casualty Insurance Co.242 concerned an insured’s claim that its obligation to replace funds paid by a bank as a result of fraudulent credit card transactions was an event covered by its policy’s computer fraud provision. The insured, an independent sales organization, was in the business of processing credit card transactions, and it contracted with a merchant bank, Merrick Bank, whereby it was responsible for marketing credit card processing services to merchants and assisting them in obtaining the equipment and software necessary to access those services.243 The insured also entered into individual agreements with merchants, authorizing the individual merchants to use credit-card terminals at which customers could swipe cards. When a customer swiped a credit card at the merchant’s terminal, data passed through the terminal to the bank that issued the card, which, in

---

234 Id. at 496.
235 Id. at 496-97.
236 Id. at 496.
237 Id. at 497.
239 Id.
240 Id. at *21.
241 Id. at *22.
243 Id. at *1-2.
turn, returned an electronic message indicating whether there were sufficient funds or sufficient credit available to cover the cost of the transaction. At the end of each day, Merrick would deposit funds into the merchant’s bank account in an amount equal to the sum of all of the credit card transactions processed that day, and Merrick would then be reimbursed by the banks that issued the credit cards.

In some instances, money would have to be refunded from the merchant to the customer. This “chargeback” could occur when the customer returned an item, when there was an error in the transaction or in processing the transaction, or as a result of fraud. The funds would be either returned to the customer’s issuing bank or the charged amount was simply not posted against the customer’s account at the issuing bank. The merchant nonetheless still had to enable the same amount of funds to be debited from its account, and, if the merchant could not cover the amount of the refund, the insured would cover the loss. Merrick Bank required the insured to establish a reserve account to act as security for the satisfaction of any chargebacks not reimbursed by the merchants. Pursuant to their agreement, Merrick Bank was the sole and exclusive owner of the reserve account and was authorized to withdraw amounts from the account to cover its losses incurred through reimbursed chargebacks.

The insured suffered chargeback losses as a result of fraudulent credit card transactions processed through the insured’s computer system by several retail merchants with whom the insured had established business relationships. The insured’s staff had verified the transactions through telephone conversations with the merchants, the customers, and the issuing banks, and each transaction was processed only after the legitimacy and capacity of the cardholder customer was established. When the chargebacks were initiated, the insured attempted to freeze the refund requests, but ultimately processed them when the cardholders, who it is believed were in on the fraud, submitted written requests to the issuing banks for the refunds. When the insured’s attempts to electronically recover these refund credits from the merchants were dishonored, Merrick Bank deducted the amounts from the insured’s reserve account to cover the cost of refunding the issuing banks, which the insured then replaced.

The insured sought coverage for the fraudulent credit card transactions under its Financial Services Stretch Endorsement, which provided coverage “for physical loss of or physical damage to ‘money,’ ‘securities, and other property having intrinsic value resulting directly from computer fraud.” “Computer fraud” was itself defined as “any act of stealing property following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside your premises or from a banking institution or similar safe depository, to a person . . . outside those premises or to a place outside those premises.”

Focusing on the word “directly” and noting Washington precedent that “[d]irect means without any intervening agency or step,” the

---

244 Id. at *2.
245 Id. at *3-4.
246 Id. at *4.
247 Id. at *5-6.
248 Id. at *7-8.
court found that the insured’s loss was not direct because it did not suffer a loss until “(1) Merrick Bank was unable to recover the chargeback funds from the merchant banks; (2) Merrick Bank deducted funds from [the insured’s] Reserve Account; and, finally, (3) [the insured] fulfilled its contractual obligations to replace those deducted funds.”

The court held that to hold that the term “directly” applied to such an attenuated chain of events would create an ambiguity where none existed and would further render the policy’s use of “directly” superfluous: “there would no difference between the phrase ‘resulting from computer fraud,’ and ‘resulting directly from computer fraud.’”

Additionally, in Kraft Chemical Co., the court held that there was no “direct nexus” between the fraudster’s e-mails and the insured’s loss. The court stated: “The undisputed record indicates that while [the insured’s] claim is premised on the receipt of fraudulent e-mails, the e-mails did not cause the transfer of funds; rather, the transfer was knowingly effectuated by [the insured’s] employees.” The court rejected the contention that the policy’s provision that a loss must be a “direct loss . . . sustained by an Insured resulting from Computer Fraud committed by a Third Part” still provided coverage if the loss was proximately caused by computer fraud: “To equate ‘loss resulting directly from’ with ‘loss proximately caused by’ requires a strained reading of ‘direct loss,’ which is a much narrower concept than ‘proximately caused loss.’”

Because the insured’s employees “eight days after receiving the e-mails, affirmatively logged onto its bank’s website and created, processed, reviewed, authorized and released the wire transfer,” the loss did not “result immediately from the alleged hacking.”

As these cases demonstrate, there is more than ample support for the “direct means direct” causation standard in the context of computer fraud claims. But, unfortunately, there are also a few cases in this context that apply the proximate-causation standard. In Retail Ventures, Inc. v. National Union Fire Insurance Co., the insurer appealed a final judgment in favor of the insured’s claim for coverage under a computer fraud rider to a Blanket Crime Policy for losses resulting from a computer hacking scheme that compromised consumer credit card and checking account information. Hackers used a local wireless network at one of the insured’s stores to gain unauthorized access to the insured’s main computer system and download credit card and checking account information pertaining to more than 1.4 million customers. In the wake of the data breach, the insureds incurred expenses for customer communications, public relations, customer claims and lawsuits, and attorney fees in connection with governmental investigations. The largest share of the insured’s losses stemmed from the compromised credit card information in the form of costs.

---

249 Id. at *12-13.
250 Id. at *13.
251 Id. at *23.
252 Id. at *24.
253 Id. at *25-27.
254 691 F.3d 821, 824 (6th Cir. 2012).
255 Id.
256 Id.
associated with charge backs, card reissuance, account monitoring, and fines imposed by VISA/MasterCard. In denying the subsequent claim, the insurers argued, among other things, that the insureds had not sustained a loss “resulting directly from” the theft of customer information.

Endorsement 17 of the policy provided coverage for “Loss which the Insured shall sustain resulting directly from [. . . ] [t]he theft of any Insured property by Computer Fraud.” “Computer Fraud,” in turn, was defined as “the wrongful conversion of assets under the direct or indirect control of a Computer System by means of: (1) [t]he fraudulent accessing of such Computer Systems; (2) [t]he insertion of fraudulent data or instructions into such Computer System; or (3) [t]he fraudulent alteration of data, programs, or routines in such Computer System.” The insureds argued that the district court incorrectly concluded that the loss sustained was a loss resulting directly from the theft of insured property by computer fraud. The district court had predicted that the Ohio Supreme Court would follow those cases interpreting “resulting directly from” as imposing a traditional proximate cause standard in this context. The insurers argued that the commercial crime policy was a fidelity bond and therefore had to be interpreted to provide only first party coverage. The district court had found that it was not a fidelity bond in toto because the endorsement made no mention of employee dishonesty and its terms indicated that it covered losses to third-party assets. The Sixth Circuit found that the insurers’ reliance on the determination that the policy was fidelity bond was overstated because “even in the context of fidelity or dishonest employee coverage, there is no universal agreement among the courts concerning the meaning of the phrase ‘resulting directly from.’”

The insureds urged the court to interpret the “resulting directly from” language as unambiguously requiring that the theft by computer fraud be the sole or immediate cause of the insured’s loss. The court, however, was not convinced by the insurers’ argument, finding the phrase to be ambiguous. The court noted that the endorsement provided coverage for loss that the insured sustained “resulting directly from” the “theft of any Insured property by Computer Fraud,” which included the “wrongful conversion of assets under the direct or indirect control of a Computer System by means of . . . fraudulent accessing of such Computer System.” Recognizing that Ohio courts had not decided whether to apply proximate cause in the context of a fidelity bond or a commercial crime policy, the court agreed with the district court’s determination that the proximate cause standard was the correct standard to determine whether the insureds’ loss “result[ed] directly from” the “theft of Insured property by Computer Fraud.”

---

257 Id.
258 Id. at 825.
259 Id. at 828.
260 Id.
261 Id.
262 Id.
263 Id. at 831.
264 Id.
265 Id. at 831-32.
In *Apache Corp. v. Great American Insurance Co.*, the insured sought to recover under the computer fraud section of a crime protection policy for losses resulting from the remittance of payments to a fraudulent bank account. The insured, an oil company, received an e-mail from an individual purporting to be an employee of one of the insured’s vendors, Petrofac Facilities Management Limited ("Petrofac"). The e-mail requested that Petrofac be allowed to change its account information so that future invoices would be paid to the new account. An employee of the insured’s verified the information in the e-mail and entered the new account information into the insured’s computer system where it was then approved by the insured’s accounting manager. Thereafter, $2.4 million were directed to the “new” fraudulent account, and the insured sought coverage under the policy 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.”

In a very short and poorly reasoned decision, the court began its analysis by citing to *Lustig* in which, as previously discussed, the Fifth Circuit held that “[a] loss is directly caused by the dishonest or fraudulent act within the meaning of [the policy] where the [insured] can demonstrate that it would not have [disbursed the funds] in the absence of fraud.” Turning to the facts before it, the court agreed with the insured’s position that despite the intervening steps that took place after the receipt of the fraudulent e-mail – the insured’s confirmation and subsequent supervisor clearance – the fraudulent e-mail was still a “substantial factor” in bringing about the insured’s loss. The court found: “These potentially intervening acts do not remove the loss from the protection afforded by the computer fraud coverage of the Policy. That is to say, despite human involvement that followed the fraud, the loss still resulted directly from computer fraud, i.e., the e-mail directing [the insured] to disburse payments to a fraudulent account.”

The court disagreed with the insurer’s argument that because of the insured’s human intervention between the fraudulent e-mail and loss, the policy’s “resulting directly from” language precluded coverage. The court stated that to accept the insurer’s reading of the policy’s language would limit the scope of coverage “to the point of non-existence,” further explaining: “That is, if anytime some employee interaction took place between the fraud and the loss, or anytime fraud was perpetrated anyway other than a direct ‘hacking,’ the insurance company could be relieved of paying under the Policy. Such a policy or provision would be rendered almost pointless.” According to the court, if the insured had intended to cover only hacking, the policy could have

---

267 *Id.* at *2.*
268 *Id.* at *3.*
269 *Id.* at *2-3.*
270 *Id.* at *5-6.*
271 *Id.*
272 *Id.* at *6-7.*
273 *Id.* at *7.*
274 *Id.*
been written to do so, but that as it was written, the policy was not that narrow.\textsuperscript{275} Therefore, the court determined that the e-mail was a cause in fact or a “substantial factor,” which, under \textit{Lustig}, was sufficient to allow coverage under the “directly resulting from” policy language.\textsuperscript{276}

At the time of writing this paper, the \textit{Apache} decision is on appeal to the Fifth Circuit. The court’s decision to uphold or overturn the trial court’s ruling will obviously be of significant importance to the industry.

Another case to be aware of is \textit{Owens, Schine}, but, as previously noted, its opinion has been vacated. There, the insurer argued that there was no evidence of direct causation as the insured’s loss was not caused by a computer, but rather, was caused by the insured’s own initiative to wire funds to South Korea after receiving the purported Wachovia check.\textsuperscript{277} The insured’s receipt of the check constituted an intervening cause between the e-mails and transfer of money. The insurer contended that the possibility that a computer was used to create a fraudulent check did not mean that the transfer of money was directly caused by the use of a computer.\textsuperscript{278} The court, however, disagreed with the insurer, holding that under Connecticut law the “direct causation requirement in a crime policy . . . is synonymous with proximate cause.”\textsuperscript{279} The court further held that the e-mails were “the proximate cause and ‘efficient cause’ of the insured’s loss because the e-mails ‘set the chain of events in motion that led to the entire loss.’”\textsuperscript{280} Thus, the court denied the insurer’s summary judgment.

As with other cases applying a proximate cause standard to the “resulting directly from” language in other insuring agreements, these courts have incorrectly interpreted the plain and ordinary meaning of the insuring agreement. Nonetheless, because there are enough cases doing so in the context of computer fraud claims, it is imperative that insurers recognize that an insured will have some support, no matter how incorrectly decided or weak the position is, to contend for a much broader interpretation of the policy’s terms.

G. Direct Loss

Not only must the alleged loss result directly from computer fraud, but the loss itself must be a loss directly incurred by the insured. Computer crime can take many different forms, but, when it comes to the topic of loss, it can be divided into two broad categories, the first of which is covered while the second is not. The first general category of loss involves theft from the insured itself. Imagine the scenario where a hacker gains access to an insured’s computer system and fraudulently instructs the insured to send funds to an off-shore account. Here, the bank has suffered a loss directly resulting from the fraudster’s use of a computer, and such loss would be

\textsuperscript{275} \textit{Id.} at *7-8.
\textsuperscript{276} \textit{Id.} at *8.
\textsuperscript{277} \textit{Id.} at *20.
\textsuperscript{278} \textit{Id.}
\textsuperscript{279} \textit{Id.} at *22.
\textsuperscript{280} \textit{Id.}
covered under the insuring agreement. The second category involves losses suffered by third parties where the insured is merely a conduit through which that loss is incurred. The most publicized examples of this type of loss involve credit or payment cards transactions between consumers, merchants, and banks. The typical scenario involves hackers gaining access to the network of a payment or credit card company and obtaining consumers’ account or personal identification numbers. With this information in hand, the hackers make purchases, and the corresponding banks debit and credit the merchants’ and consumers’ accounts. Here, the bank is merely a party through which the fraud was perpetrated. The actual losses of the fraud are those suffered by consumers or merchants whose accounts were negatively affected by the fraudulent breach of the card infrastructure. Claims arising from these types of losses are not covered as it is a third party who has suffered the loss. Even if that third party institutes litigation against the insured financial institution and seeks to hold it liable for these losses, the insuring agreement does not provide coverage.

This distinction is important. As noted above, the express language of the Computer Fraud insuring agreement provides that it will cover losses to covered property “directly resulting from” computer fraud. In other words, coverage is limited to a direct loss. To interpret the insuring agreement to cover losses to third-parties would be to alter the very nature of its coverage, turning what has always been intended to be first-party insurance into liability insurance.

This principal was recently espoused in *Taylor and Lieberman v. Federal Insurance Co.* 281 in which the court refused to extend coverage for losses the insured incurred to repay its client for overseas transfers made after receiving fraudulent e-mail instructions. The insured, an accounting firm, had power of attorney to issue payments and transfer funds from a client’s account. The insured received an initial e-mail, purportedly from its client’s e-mail account, instructing the firm to wire funds to a bank in Malaysia. The insured received a second e-mail from the same account instructing the firm to wire funds to a bank in Singapore. Believing the e-mails to have come from the client, the transfers were made and confirmation e-mails were sent to the client’s e-mail address. When a third e-mail requested the wiring of funds to a different Malaysian bank, the insured discovered the fraudulent scheme. The insured was able to recover most of the first transfer, but nothing from the second transfer, and the client soon thereafter withdrew its funds from the insured. The insured tendered its loss under its crime coverage policy, but the insurer denied coverage.282

The insured attempted to recover under its policy’s Forgery, Computer Fraud, and Funds Transfer Fraud coverages, each of which only applied to “direct loss sustained by an Insured.” 283 The insurer argued that there was no “direct loss” because the e-mails did not immediately and without intervening cause result in a loss, and that the insured’s loss only occurred after the client demanded repayment for the lost

---

282 Id. at *2-4.
283 Id. at *6-7.
Essentially, the insurer argued that the insured was attempting to recover for a third-party loss.

The court agreed that the loss was not a direct loss. The court stated that “[a] common use interpretation of direct loss provides that a loss is not direct unless it follows immediately and without intervening space, time, agency, or instrumentality.” The coverage provisions contemplated coverage for fraudulent actions against the insured that directly resulted in the loss of the insured’s own money, not fraudulent actions upon which the insured relied to disburse its client’s money. The court’s reasoning is of particular interest in that it shows that the purpose of these provisions was to guard against loss resulting from hacking:

If the funds had been held in an account owned or attributed to Plaintiff, such as an escrow account . . . and a hacker had entered into Plaintiff’s computer system and been able to withdraw funds such that Plaintiff’s accounts were immediately depleted, then Plaintiff would be correct in asserting coverage from the Policy. Here, however, a series of far more remote circumstances occurred: Client gave Plaintiff power of attorney over Client’s money held in Client’s own account; a perpetrator of fraud motivated Plaintiff’s agent to use the power of attorney to transfer funds out of Client’s account; Plaintiff discovered this fraud and attempted to recover the funds; Client requested repayment of the lost funds and Plaintiff obliged; Plaintiff now requests Defendant indemnify it for the losses that were transferred from Client to Plaintiff. These are not the circumstances . . . [that] appear to be within the contemplation of the Policy.

Similar to other insuring agreements, coverage for computer fraud is intended solely to provide first-party coverage to the insured. The computer fraud must have caused a direct loss to the insured for the coverage afforded by the Computer Fraud insuring agreement to be implicated. Losses to third parties, which the insured may be liable for, however, are not covered, even if the third parties’ losses resulted from the use of a computer. In those cases, such as Taylor, the third party has suffered the direct loss, not the insured. Any loss suffered by the insured is a resulting indirect loss, thereby falling outside the scope of coverage.

H. Other Cases Interpreting the Computer Fraud Insuring Agreement

In addition to the cases discussed above, there are a handful of other decisions that analyze whether a loss is covered by a Computer Fraud insuring agreement. More cases will surely follow as time continues to pass. Each of the most relevant cases is discussed below.

---

284 Id. at *7.
285 Id. at *7-8.
286 Id. at *9.
287 Id. at *10-11.
1. **Southern California Counseling Center v. Great American Insurance Co.**

In this case, the insured sought to recover $100,000 in loss allegedly caused by computer fraud when a sham payroll company withdrew funds from the insured’s bank accounts and converted those funds to its own use instead of using them to pay the insured’s federal and state payroll taxes as agreed. The insured entered into certain agreements with a payroll company whereby after the insured provided payroll information to the payroll company through the company’s website, the payroll company would initiate debit transfers from the insured’s bank account to the payroll company’s account for the remittance of payroll and payroll taxes. After the payroll company’s CEO was arrested, the insured learned that the payroll company had not paid the insured’s state and federal payroll taxes to the tune of approximately $100,000, leaving the insured to cover those unpaid amounts.

The questions for the court were whether the loss was caused by computer fraud within the meaning of the policy and, if so, whether any exclusion applied. The insurer argued that the authorized representation exclusion precluded coverage, which stated that the policy did not cover “loss resulting from ‘theft’ or any other dishonest act committed by any of your . . . Authorized representatives . . . except when covered under Insuring Agreement A.1.” Relying on Ninth Circuit precedent defining “authorized representative” under a crime insurance policy to cover “those who by authorization of the insured are given access to and permitted to handle the insured’s funds,” the court found that the payroll company was the insured’s authorized representative, thus precluding coverage under the exclusion. The fact that the payroll company did not use the funds it withdrew to pay the payroll taxes as promised did not negate the fact that the insured authorized the payroll company to withdraw and handle the funds in the first place. The court also found the insured’s argument that the authorization it granted to the payroll company was void ab initio because the payroll company had induced the authority by fraud to be unavailing. While there may have been fraud in the inducement of the agreements rendering the agreements merely voidable, there was no fraud in the execution of the agreements which would have rendered them void ab initio. The court found that to hold otherwise would be to rewrite the policy “such that the exclusion would apply not to ‘any’ authorized representative as the Policy states, but only to authorized representatives who did not fraudulently induce their status.”

---

289 Id. at *5.
290 Id. at *5-6.
291 Id. at *9.
292 Id. at *9-12.
293 Id. at *12.
294 Id. at *12-13.
295 Id. at *14-15.
296 Id. at *15.
2. **Great American Insurance Co. v. AFS/IBEX Financial Services, Inc.**

This case concerned whether an insurer’s crime policies provided coverage for losses stemming from checks issued by the insured payable to Charles McMahon Insurance Agency. The insured, AFS/IBEX, provided premium financing in the insurance industry, and entered into an agreement with Charles McMahon, Sr., the owner of CMIA, pursuant to which McMahon, Sr. would create and sign premium finance applications on behalf of insureds. AFS/IBEX would then send a check to the insurance company for the purchase price of the insurance, and the insureds would send regular payments to AFS/IBEX. McMahon Sr.’s son, Charles Owen McMahon, Jr., was an insurance agent and owner of McMahon Insurance Services. He was also the office manager of his father’s agency and had responsibility for submitting applications for premium financing to AFS/IBEX under his father’s contract. The son exploited this business relationship by submitting approximately 122 false applications to get AFS/IBEX to issue checks for the premium financing, and AFS/IBEX issued 127 checks made payable to “Charles McMahon Insurance Agency.” The son then endorsed these checks “Charles McMahon Insurance Agency” and deposited the funds in his own personal bank account. The insured never received payments from the fake customers, and it sought to recover its loss under a Computer Fraud insuring agreement, among other provisions. The insurer denied coverage.

The insurer moved for summary judgment arguing, among other things, that AFS/IBEX’s claims were not covered under the Computer Fraud insuring agreements of its respective policies. Specifically, the insurer argued that the sustained losses did not bear a direct enough connection to the use of a computer to fall within the scope of the computer fraud provisions, contending that no computer actually caused the transfer of any funds from the insured’s bank account. Rather, the loss was caused by checks which the son duped AFS/IBEX into issuing and then endorsed and deposited. Thus, the insurer argued that there was no direct loss resulting from the use of a computer as required by the computer fraud provisions. Noting that the computer fraud provisions provided coverage “for any 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,” the court found that this language was designed “to cover losses directly stemming from fraud perpetrated by use of a computer.” The insured put up virtually no fight in attempting to argue that its loss was covered by the Computer Fraud Insuring Argument. Thus, the

---

298 Hereinafter CMIA.
299 Id. at *4.
300 Id.
301 Id. at *4-5.
302 Id. at *5.
303 Id. at *43-44.
304 Id. at *44.
305 Id.
306 Id. at *44-45 (emphasis in original).
court had little difficulty in finding that the insured failed to raise an issue of fact that a computer caused the transfer of any funds from the insured’s bank account.\(^{307}\)

However, because the insured offered little resistance to rebut the insurer’s argument, the court’s opinion does not delve deeply into the facts on just how much the insurance agency used a computer to carry out its scheme that would shed light on what is required by the “use of a computer” requirement. While the court’s holding that the loss was caused by the son’s duping of AFS/IBEX and his ensuing endorsement and deposit of the checks is not clear on what role the computer itself played in the perpetrated fraud, the court still seemed to conclude that it was the steps taken after the insured received the fraudulent applications for premium financing that were the direct cause of the loss. The creation and submission of the false applications, for the court, were too far removed from the immediate cause of the loss to be the “direct” cause.

3. Vonage Holdings Corp. v. Hartford Fire Insurance Co.\(^ {308}\)

The insured was a telecommunications company that provided voice and messaging services over broadband internet networks. The insured discovered that one or more computer hackers located outside of its premises used a computer to fraudulently access the insured’s gateway servers to transfer the use of those servers to themselves and others.\(^ {309}\) The hacker(s) then routed telephone calls to Cuba through one of the insured’s telecommunications carrier partners which, in turn, billed the insured for those calls.\(^ {310}\) The insured also claimed that during the period the hacker(s) transferred the use of its servers it lost the ability to use the servers’ full capacity, resulting in a loss of over one million dollars.\(^ {311}\) The insured sought to recover this loss under its policy. The policy provided coverage, in relevant part, for the loss of “other property” “following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the ‘premises.’”\(^ {312}\) “Other property” was further defined as “any tangible property other than ‘money’ or ‘securities’ that has intrinsic value,” and “premises” was defined as “the interior of that portion of any building which you occupy in conducting your business.”\(^ {313}\)

The insurer filed a motion to dismiss arguing that the insured had not alleged that tangible property directly related to the use of a computer was transferred outside of the insured’s premises, and that the insured had not alleged that it suffered a “loss of” or “loss from damage to” its tangible property.\(^ {314}\) The insured described its server as “a tangible piece of computer equipment, which connects telecommunications networks with cables, fibers and other electronic devices and apparatus, and has intrinsic value to

---

\(^{307}\) Id. at *45.


\(^{309}\) Id. at *1-2.

\(^{310}\) Id. at *2.

\(^{311}\) Id.

\(^{312}\) Id.

\(^{313}\) Id. at *3.

\(^{314}\) Id. at *6.
the core call processing aspects of [the insured’s] business.” The court found that the servers “unquestionably” met the definition of “other property.” The court focused on the phrase “transfer of that property,” finding it to be ambiguous. The court held that it was plausible that the insuring provision contemplated insuring against the transfer of the use of the servers to a person outside the insured’s premises. By contrast, the insurer’s position would require the physical transfer of the property to outside the premises for the insured to have a valid claim, which, according to the court, would make the policy’s subsection “to a person (other than a ‘messenger’) outside those ‘premises,’” superfluous. The court also dismissed the insured’s argument that the insured had suffered a loss of its property. The court found that the insured’s contention that the loss of its ability to use the servers to full capacity, while temporary, was sufficient under the pleading standards. “At the very least, this (i.e. the alleged loss of use) is a plausible interpretation of what constitutes a loss of property.”

4. **State Bank of Bellingham v. BancInsure, Inc.**

In this case, the insured used the Federal Reserve’s FedLine Advantage Plus system to make wire transfers which were made through a desktop computer connected to a private network device provided by the Federal Reserve. To complete a wire transfer, two of the insured employees had to enter their individual names, insert physical tokens into the computer, and enter individual passwords and passphrases. On one occasion, one of the bank’s employees, after completing a wire transaction, left the tokens in the computer and left the computer running. When the employee returned the next day, she discovered that two unauthorized wire transfers had been made from the insured’s Federal Reserve account to two different banks in Poland. The employee contacted the Federal Reserve to reverse the transfers. The Federal Reserve initially refused, but did eventually contact the intermediary institutions to inform them that the transfers were fraudulent. One of the transfers was able to be reversed, but the insured was unable to recover the other transfer. After notifying its insurer of the loss, it was determined that a “Zeus Trojan horse” virus had infected the computer and permitted access for the fraudulent transfers. The insurer then determined that the loss was not covered based on certain employee-caused loss exclusions, exclusions for theft of confidential information, and exclusions for mechanical breakdown or deterioration of a computer system.

The district court granted summary judgment for the insured, holding “that the computer system fraud was the efficient and proximate cause of [the insured’s] loss,”

---

315 *Id.* at *3-4.
316 *Id.* at *8.
317 *Id.* at *9-10.
318 *Id.* at *10.
319 *Id.*
321 Hereinafter FedLine.
322 *Id.* at *1-2.
323 *Id.* at *2.
324 *Id.* at *2-3.
325 *Id.* at *5.
and “neither the employees’ violations of policies and practices (no matter how numerous), the taking of confidential passwords, nor the failure to update the computer’s antivirus software was the efficient and proximate cause of [the insured’s] loss.”\textsuperscript{326} The district court further found that “it was not then a ‘foreseeable and natural consequence’ that a hacker would make a fraudulent wire transfer. Thus even if those circumstances ‘played an essential role’ in the loss, they were not ‘independent and efficient causes’ of the loss.”\textsuperscript{327} On appeal, the Eighth Circuit affirmed the district court’s ruling.

The Eighth Circuit first noted that Minnesota has adopted the concurrent-causation doctrine, which directs that “[a]n insured is entitled to recover from an insurer when cause of the loss is not excluded under the policy. This is true even though an excluded cause may also have contributed to the loss.”\textsuperscript{328} The insurer argued that that doctrine should not be applied to the policy at issue because financial institution bonds require the insured to show that its loss “directly and immediately resulted from dishonest, criminal, or malicious conduct.”\textsuperscript{329}According to the insurer, application of the concurrent-causation doctrine to these bonds would make it impossible for an insurer to show that a bond’s exclusions were the overriding cause of the loss.\textsuperscript{330} The court rejected the argument, stating that no Minnesota case had precluded the application of the doctrine to financial institution bonds.\textsuperscript{331} Furthermore, the insured “still had to show that its loss was directly caused by the fraudulent transfer, and the application of the concurrent-causation doctrine did not interfere with that requirement.”\textsuperscript{332}

The court further rejected the insurer’s argument that the district court erred in concluding that the fraudulent hacking of the computer system by a criminal third party was the overriding, “or efficient and proximate,” cause of the loss.\textsuperscript{333} The court agreed with the district court’s conclusion that “the efficient and proximate cause” of the loss was the illegal transfer of the money and not the employees’ violations of policies and procedures. The court stated: “[A]n illegal wire transfer is not a ‘foreseeable and natural consequence’ of the bank employees’ failure to follow proper computer security policies, procedures, and protocols. Even if the employees’ negligent actions ‘played an essential role’ in the loss and those actions created a risk of intrusion into [the insured’s] computer system by a malicious and larcenous virus, the intrusion and ensuing loss of bank funds was not ‘certain’ or ‘inevitable.’”\textsuperscript{334} Thus, in affirming the district court’s ruling, the court concluded that the “overriding cause” of the insured’s loss was the criminal activity of a third party.\textsuperscript{335}

\textsuperscript{326} Id. at *6.
\textsuperscript{327} Id. at *6-7.
\textsuperscript{328} Id. at *8.
\textsuperscript{329} Id.
\textsuperscript{330} Id. at *9.
\textsuperscript{331} Id.
\textsuperscript{332} Id. at *10.
\textsuperscript{333} Id. at *11.
\textsuperscript{334} Id. at *13-14.
\textsuperscript{335} Id. at *14.
5. **Northside Bank v. American Casualty Co.**

The insured bank opened an account incident to a merchant services agreement with Dakco PC Product Division, Inc. Dakco proceeded to accept orders for merchandise, and take payment by debit and credit cards. Dakco electronically transmitted the card authorizations to the bank and, upon receipt, the bank transferred money into Dakco’s account. It was eventually discovered that Dakco never delivered the purchased merchandise to its customers who then exercised their rights to rescind their payment obligations. When these customers refused to pay, their creditors either refused to pay or charged back the amounts paid to the bank. When the bank went to pass the chargebacks on to Dakco, it found Dakco’s accounts depleted. The bank, as a result, sustained a loss of about $300,000 and sought to recover those funds, in part, through its policy’s Computer Crime endorsement.

The endorsement provided coverage for a loss that was “the direct result of any fraudulent electronic instruction or advice transmitted to or from the insured.” “Fraudulent electronic instruction or advice” was further defined, in relevant part, as “an electronic instruction or advice which is 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.” In response to the insurer’s motion for summary judgment, the bank argued that the words “modified or altered” were ambiguous. The court characterized the insured’s argument as attempting “to place a square peg in a round hole.” The bank contended that Dakco’s submission of electronic instructions and subsequent failure to ship the merchandise should be viewed as a modification or alteration of the electronic instruction with the intent to deceive. The court, however, found that the instructions themselves were never modified or altered. The bank received unmodified and unaltered instructions directing it to pay a sum to Dakco when they left Dakco’s control. The bank then read the instructions and paid in accordance with the instructions language. The terms “modified” and “altered” “mean exactly what they say,” and the bank’s construction of the policy was “so strained and at odds with the obvious intent of the insurance policy that to accept it would be to distort the meaning of the policy beyond all recognition.” Of import, the court also determined that the intent of the policy, in particular its electronic fund transfer and computer crime coverages, was to protect the insured bank “from someone breaking into the electronic fund transfer system and pretending to be an authorized representative or altering the electronic instructions to divert monies from the rightful recipient.”

---

337 Id. at 97.
338 Id. at 98.
339 Id.
340 Id. at 99.
341 Id. at 100.
342 Id. at 101.
343 Id.
344 Id.
345 Id.
346 Id.
6. **Morgan Stanley Dean Witter & Co. v. Chubb Group of Insurance Cos.**

Morgan Stanley entered into a custodial services agreement with London and Bishopgate International in which Morgan Stanley agreed to safeguard money and property that was owned and held by London. As custodian, Morgan Stanley was to be responsive to London’s instructions. In order to facilitate the receipt of London’s instructions, Morgan Stanley provided it with computer software granting access to Morgan Stanley’s computer programs. Some months later, London entered into another agreement with First Tokyo Index Trust Limited (“First Tokyo”), a Scottish investment trust, pursuant to which London managed First Tokyo’s investments. To effectuate its agreement with First Tokyo, London opened an account with Morgan Stanley.

Subsequently, a third firm, which owned seventy-five percent of London, announced it was making a public offer to purchase First Tokyo. First Tokyo instructed London to cease trading on its behalf. However, Morgan Stanley was never informed of First Tokyo’s instruction. London then instructed Morgan Stanley to liquidate the bulk of First Tokyo’s portfolio through five different transactions, with the sale proceeds being delivered to London-affiliated accounts. The transactions were accomplished through instructions sent via computer, fax, and voice to Morgan Stanley. After discovering the loss, First Tokyo sued Morgan Stanley. After settling, Morgan Stanley sought to recover its defense costs and its settlement amount against several insurers under an Electronic Computer Crime Policy. Morgan Stanley argued that it was entitled to coverage under the policy’s insuring agreements covering “computer systems,” “customer voice initiated transfers,” and “facsimile transfer instructions.”

The facsimile policy covered “fraudulent FAX transfer instructions . . . [that] fraudulently purport to have been made by a customer or other authorized representative but which FAX transfer instructions were not made by the customer or other authorized person.” The court found that this agreement unambiguously limited coverage to situations where an authorized person posed as a customer or other authorized person to issue the fraudulent transfer instructions. The court referred to it as “so-called ‘impostor’ coverage.” As there was no dispute that the instructions to Morgan Stanley were from persons authorized to act for London, there was no coverage under this agreement.

348 Hereinafter London.
349 Id. at *3.
350 Id. at *3-4.
351 Id. at *4-5.
352 Id. at *5.
353 Id. at *6.
354 Id. at *7-8.
355 Id. at *8.
The computer system insuring agreement was subject to an exclusion which provided that there was no coverage for "loss by reason of the input of Electronic Data at an authorized electronic terminal . . . or a Customer Communication System by a customer or other person who had authorized access to the customer’s authentication mechanism."\(^{356}\) The court held that this exclusion clearly excluded coverage for fraud committed by customers or other authorized persons. Nonetheless, Morgan Stanley argued that the exclusion was not applicable because its customer was not London, but, rather, First Tokyo, as it owned the funds or the property transferred as a result of the fraudulent computer instructions.\(^{357}\) While the computer services insuring agreement did not define “customer,” the term was defined in the voice initiated insuring agreement as that "business entity which has a written customer agreement with the Assured."\(^{358}\) Morgan Stanley’s custodial agreement with London stated that London was the customer, not First Tokyo or any other entities for which London maintained accounts with Morgan Stanley. Therefore, London was the only customer for purposes of the insuring agreement.\(^{359}\) Furthermore, London was the only entity that had access to Morgan Stanley’s computer system. Therefore, coverage was also precluded by the computer system insuring agreement’s exclusion.\(^{360}\)

III. Conclusion

Given the advancements in technology, today’s businesses face a constant and ever-changing battle against cybercriminals. New technologies present new means for criminals to steal from insureds, often times resulting in significant losses. As a result, the number of claims made against insurers under Computer Fraud insuring agreements will surely climb over the next several years. But as the language of the insuring agreements themselves make clear, and as several cases demonstrate, these agreements are meant to cover only true hacking. The key phrases “fraudulently cause” and “resulting directly from” signify that insurers should only be liable for losses that immediately flow from a hacker's unsanctioned entry into an insured's computing system. By the same token, losses stemming from social-engineering scams, no matter their complexity, are simply not covered under Computer Fraud insuring agreements. These risks are intended to be addressed by entirely separate policies aimed specifically at social engineering. But insureds that do not purchase that coverage cannot shoehorn their social-engineering losses into a Computer Fraud insuring agreement. Hacking is a distinct risk from social engineering, and insurers are much better able to calculate proper premiums for each risk separately. Insurers cannot afford to cover two of the most serious risks that businesses face today with one lump insuring agreement that covers any fraud involving a computer in even a tangential way. The author therefore urges courts to be thorough and careful in their interpretation of Computer Fraud insuring agreements. These policies are designed to cover hacking, and it is in insureds’ best interests that they be interpreted as such. Otherwise, insurers

\(^{356}\) Id.
\(^{357}\) Id. at *9.
\(^{358}\) Id.
\(^{359}\) Id.
\(^{360}\) Id. at *10.
will be forced to charge premiums for hacking policies that are so high, they will become untenable.