4

"THE POINT OF NO RETURN": COMPUTER FRAUD INSURANCE AND DEFINING CYBERCRIME

On December 11, 2008, investor Bernie Madoff was arrested for perpetrating the largest private Ponzi scheme in history, amounting to nearly $65 billion in fraud. Thousands of individuals and organizations who had invested their money with Madoff lost massive sums of money in the scandal, including Nobel laureate author Elie Wiesel and former Dodgers pitcher Sandy Koufax. The Methodist Health System Foundation Inc. (MHSFI), a nonprofit based in Slidell, Louisiana, focused on improving access to primary health care in East New Orleans, lost the full value of its investment with Madoff's firm, which it estimated at $439,467. On September 3, 2009, less than a year after Madoff's arrest, the nonprofit filed a claim for that loss with its insurer, Hartford, under its Crime Shield Insurance policy with the carrier. MHSFI's policy had a $500,000 limit per loss, which the Louisiana foundation hoped would cover its entire Madoff investment, less a $5,000 deductible.

In its claim, MHSFI pointed to the Computer and Funds Transfer Fraud portion of the Crime Shield policy, which defined computer fraud as the loss of money or other property "following and directly related to the use of any computer to fraudulently cause a transfer of that property from inside the 'premises'" to a person or place outside those premises. Since the fraudulent trading slips and month-end account statements that Madoff had provided to account holders were created on computers and "central to Madoff's scheme," the Ponzi scheme was an act of computer fraud and therefore should be covered under its policy, MHSFI argued. The organization explained its reasoning for labeling the financial fraud a computer crime:

> But for Madoff's use of a computer to obtain and manipulate data that made its trading slips and month-end account statements appear accurate, and created a false perception of a successful history of investment and trading, MHSFI's money would not have been transferred to Madoff. MHSFI's loss was therefore

> "directly related" to Madoff's use of computers to fraudulently cause the transfer of MHSFI's money from banking premises and/or financial institutions to Madoff, and Hartford is therefore obligated to cover that loss under its Crime Policy.[1]

As further evidence of the essential role computers had played in Madoff's scheme, MHSFI pointed to the fact that federal prosecutors had filed charges against two computer programmers working for Madoff who had written programs that generated fictitious trading data for his client accounts.

On October 20, 2009, Hartford sent MHSFI a letter denying their claim on the grounds that Madoff's Ponzi scheme, despite involving computers, was not an act of computer fraud. Hartford pointed out that MHSFI had voluntarily given its money to a fund called Meridian that later invested it with Madoff's firm. "Madoff did not use computers to fraudulently cause a transfer of Methodist's funds," Hartford pointed out. The insurer continued:

> At no point did the transferors open their online statements and learn in shock that transfers had occurred without their knowledge. Rather, the transfers flowed from decisions made by the transferors to speculate in the stock market. . . . These decisions were informed by a hope that its investments would increase in value and did not "flow immediately" from any use of a computer by Madoff. Any role played by a computer in Methodist's loss theory is, at most, incidental. . . . This is not computer fraud within the meaning of the Hartford Policy.[2]

MHSFI sued Hartford, contesting the claim denial, but US district judge Helen Berrigan granted summary judgment to the insurer on July 1, 2011. Berrigan dismissed the case because MHSFI's investment decision was "too many steps removed from Madoff's fraud" to qualify for coverage under the Hartford policy. Since MHSFI had voluntarily made those investments, "the Madoff Ponzi scheme was not a direct cause" of MHSFI's losses, Berrigan explained. Because of that, she did not even address in her ruling the question of whether Madoff's actions constituted computer fraud, but almost certainly the answer would have been that it did not.

In March 2009, years before the MHSFI suit was resolved, Madoff pleaded guilty to eleven counts of fraud, money laundering, perjury, and theft, and he was later sentenced to 150 years in prison, but at no point was he charged with any computer crimes. Of course, he had used computers in the course of operating his Ponzi scheme—by the early 2000s, it would have been nearly impossible to operate a Ponzi scheme or really any form of white-collar crime

without the use of a computer—but that, in itself, did not make him a cybercriminal. And yet, as the MHSFI case hinted, defining what, precisely, was and was not computer fraud was not an entirely straightforward undertaking when so many crimes involved computers in at least some capacity. As computers became increasingly involved in financial transactions, computer fraud transformed from something that had initially seemed like a very specific type of crime to a much broader and murkier class of crimes that relied on or involved computers in a range of capacities, from sending fraudulent emails to initiating unauthorized financial transfers. Because insurers were selling policies geared specifically toward covering computer and electronic crimes, this evolution of the nature of cybercrime and its variations prompted significant disputes about what those policies covered and, more fundamentally, what constituted a computer crime, as opposed to a crime that just happened to involve computers. Canonical examples of computer crimes included someone stealing or guessing an employee's password and using it to transfer funds to themselves from another account or a hacker exploiting a vulnerability in a company's software to initiate an unauthorized transfer—the types of crimes that were executed entirely, or almost entirely, through computers. On the other end of the spectrum, Madoff's Ponzi scheme seemed to be a fairly clear example of a crime where computers played a peripheral, supporting role, but other incidents would prove to be much murkier. As computers became increasingly embedded in both business and criminal activity during the late 1990s and early 2000s, insurers and policyholders repeatedly scuffled over what exactly constituted computer fraud as carriers experimented with different definitions and language in their coverage.

While insurers were largely successful in their efforts to deny any cyber-related claims under CGL policies, they met with much more mixed success in court when it came to denying coverage under computer fraud policies for crimes they deemed insufficiently computer-centric, in part due to the fact the language in these policies defining computer fraud varied much more than the language defining personal and advertising injuries in standard-form CGL policies. Different policies offered different definitions of what counted as computer fraud and courts, in turn, had very different opinions about just how clear that language was, what it meant, and how directly a crime had to be executed via computer for it to count as computer fraud. Some courts took a fairly narrow view that for a crime to qualify as

computer fraud it could not involve any human intervention on the victim's part. Other courts were more open to the idea that something like phishing emails containing faked invoices might play an enabling role in computer fraud even if the victims themselves were responsible for ultimately acting on the fraudulent information in those emails to initiate financial transfers. These disputes often centered on the question of whether computers had to *directly* cause financial fraud for an incident to be considered an act of computer fraud or whether it was sufficient for the perpetrators to use computers to mislead employees into initiating fraudulent financial transfers through spoofed emails or other forms of computer-enabled manipulation. This requirement for the computers to directly cause the fraud stemmed from insurance policy language that often defined computer fraud in similar terms to the MHSFI policy as losses "directly related to the use of any computer to fraudulently cause a transfer." But the specific language varied from policy to policy as the threat landscape evolved and insurers' understanding of computer fraud shifted. For policyholders, these different definitions and interpretations of computer fraud coverage led to significant uncertainty about what such policies actually applied to, especially as computer crimes continued to evolve and change, and carriers continued to experiment with new language in their computer fraud policies.

INTERVENING EVENTS AND IMMEDIATE CAUSES: *BRIGHTPOINT V. ZURICH*

On January 23, 2003, the wireless device company Brightpoint received a purchase order for 200,000 prepaid telephone cards at its branch in the Philippines. The fax appeared to come from long-time Brightpoint customer Enrico Genato, who ran a business that regularly purchased large numbers of prepaid phone cards from Brightpoint. Because Genato purchased such large volumes of phone cards, Brightpoint required him to include postdated checks with his purchase orders, as well as bank guaranties certifying that his accounts held sufficient funds to cover those checks. Genato would fax Brightpoint copies of the checks and guaranties along with his purchase orders, and Brightpoint would then pick up the original checks, guaranties, and purchase orders when they delivered the phone cards, which they purchased directly from telecom companies. Everything appeared to be in

order for the purchase order that arrived on January 23, 2003; it included both the postdated check and bank guaranties, as did the fax from Genato that arrived the following day, January 24, which contained a purchase order for another 150,000 phone cards.[3]

On both January 23 and 24, Brightpoint employee Jay-Jay Moralde went to the office of Globe Telecom, a major Philippines telecom provider, and purchased enough prepaid phone cards for each of Genato's orders. In the parking area just outside the Globe office where he made the purchases, Moralde then turned them over to Reena Aldeguer, who had received orders for Genato in the past, and who gave Moralde the original postdated checks and bank guaranties for the orders. But the checks, totaling 82,350,000 Philippine pesos, or roughly $1.5 million, turned out to be forged. So, on April 11, 2003, Brightpoint submitted a claim for the money they had spent on the stolen prepaid phone cards to its insurer, Zurich, citing Form F of its Crime Policy which covered computer fraud and wire transfer crimes and defined computer fraud as "theft of property following and directly related to the use of any computer to fraudulently cause a transfer of that property." Brightpoint's policy explicitly stated that fraudulent transfers falling under this definition could be initiated via "written, telephonic, telegraphic, telefacsimile, electronic, cable, or teletype instructions."[4]

On October 16, 2003, Zurich denied Brightpoint's claim, writing that "there is nothing . . . that proves that a computer was used to fraudulently cause a transfer of the phone cards." Brightpoint sued Zurich, looking to the *American Heritage Dictionary* to help prove that it had, in fact been the victim of computer fraud. Form F of the Zurich coverage defined computer fraud as theft "directly related" to the use of a computer, so Brightpoint looked up both words in the fourth edition of the *American Heritage Dictionary*, which defined "related" as meaning "connected" or "associated" with something, and "direct" as meaning "characterized by close logical, causal, or consequential relationship." Thus, Brightpoint argued, "the theft of the phone cards had a 'close logical, causal, or consequential' connection or relationship to the use of a computer" because "the first step taken in the scheme each day was to fax purchase orders to Brightpoint for approval. . . . And the only means by which Brightpoint received the fraudulent purchase orders was by fax. So the use of the fax here was not a 'remote cause' . . . it was an integral part of the theft."

Zurich did not dispute that the fax machine played a role in the scam or the dictionary definitions Brightpoint had looked up, but it contended that the faxes, central though they may have been to the fraud, could not be considered the "efficient proximate cause" of Brightpoint's losses, that is "the risk that sets others in motion." Zurich maintained that it was the physical checks and bank guaranties that Aldeguer had handed to Moralde in the Globe parking lot—not the faxed copies of them—that were the true "predominating cause" of the fraud. In its response to Brightpoint's suit, Zurich argued that Aldeguer's and Moralde's "'face-to-face' event of physically exchanging the cards for original checks and guaranties was the cause of Brightpoint's loss. . . . As such, Brightpoint's alleged loss was not 'directly related' to the receipt of faxed purchase orders, checks and Bank Guaranties."

On March 10, 2006, Indiana district judge Sara Evans Barker ruled in favor of Zurich. She was not just skeptical about designating the Brightpoint incident as an act of computer fraud, she was even skeptical about calling a fax machine a computer, writing in her ruling that "the common and 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 machine." But her decision to support Zurich's denial of the Brightpoint claim ultimately stemmed from the argument Zurich had made that Moralde's and Aldeguer's face-to-face exchange of the physical phone cards for the paper checks and bank guaranties was the true direct cause of Brightpoint's losses. "The facsimile transmission caused Brightpoint to purchase the cards from its supplier, not to transfer them to its purchaser, and the use of the fax thus cannot be viewed as having directly or proximately caused the theft," Barker wrote in the ruling.

Brightpoint had argued that just because there were multiple different causes of the fraud didn't mean that the faxes weren't every bit as central as the hand-off of the physical copies. The faxes containing copies of the forged purchase orders, checks, and guaranties could be viewed as a proximate cause of the fraud, even if the actual hard copies of those documents were also a proximate cause, Brightpoint contended. Since many crimes, including Madoff's Ponzi scheme, have some computer-based component, Brightpoint's reasoning, in which a computer could be one of many different causes of a crime, had the potential to significantly expand the scope of what kinds of incidents were considered computer fraud.

But Barker was not convinced by this argument. She pointed to the language in Brightpoint's Form F coverage requiring that a covered theft be "directly related to the use of any computer" and, eschewing the *American Heritage Dictionary* definitions that Brightpoint had cited, looked to the definition of the word "directly" in *Black's Law Dictionary* as meaning "in a straight line or course" or "immediately." Even if there were multiple causes of the Brightpoint fraud, "the loss to Brightpoint that occurred here did not flow immediately from the use of the facsimile," Barker concluded. Underlying the logic of her decision was a clear concern that broad interpretations of the meaning of computer fraud could quickly spiral out of control and allow policyholders to label every crime that involved even the slightest technological component—from counterfeiting to Ponzi schemes—as computer fraud. Barker highlighted this risk in her ruling:

> Brightpoint's approach in isolating words and relying upon dictionary definitions of terms such as "following" and "directly related," leads to bizarre constructions of the contract. For example, applying this approach, Form F could be read to provide coverage where a customer sends an e-mail indicating that he is coming over to Brightpoint's offices to make a cash purchase of 50 mobile phone units and completes the transaction by using counterfeit money. If coverage were permitted, it would reflect an interpretation other than a plain and ordinary interpretation of the policy at issue; any reasonable person would not give the Form F provisions regarding coverage for computer fraud or wire transfer that "spin." Obviously, in both the contrived example and in this case, intervening events or circumstances became the direct, proximate, predominate and immediate cause of Brightpoint's loss.

The most significant element of the *Brightpoint* ruling for influencing future cases over computer fraud insurance disputes was Barker's contention that, in order to be considered the result of computer fraud, a loss must "flow immediately" from the use of a computer, without any "intervening events or circumstances." But the nature of those intervening events would change significantly as computer crimes evolved. And, adding to the confusion, different insurers would define computer fraud in different ways, further complicating the question of what kinds of crime each different policy applied to. For instance, the rise of social engineering techniques like phishing would lead to many crimes that were not entirely automated but did not rely on the face-to-face exchange of physical forged documents either.

Some insurers created specific social engineering coverage under cyber risk policies for such incidents, but not all customers purchased those more specialized policies, and many of those who didn't continued to feel that their computer fraud coverage should provide them with some protection from computer-based manipulation—a sentiment that some courts turned out to share, as well. Barker's reference to what "any reasonable person" would consider to be computer fraud would be important for these cases as well since computer spoofing schemes would be understood by many reasonable people as falling within that category.

HACKING, UNAUTHORIZED ACCESS, AND *PESTMASTER V. TRAVELERS*

In August 2009, a pest control company headquartered in California called Pestmaster Services hired a contractor to administer its payroll services. The contractor, Priority 1 Resource Group, was owned by a woman named Dawn Branzuela, who agreed to pay payroll taxes and prepare and deliver payroll checks on Pestmaster's behalf. So that Priority 1 could perform these services, Pestmaster authorized Priority 1 to initiate automated clearing house (ACH) transfers from Pestmaster's bank accounts in order to cover employee paychecks. Each payroll period, Priority 1 would send Pestmaster invoices for the amounts owed for employee salaries and taxes, and after Pestmaster approved the invoices Priority 1 would then initiate ACH transfers to move the approved amounts from Pestmaster's account to their own. In June 2011, Pestmaster CEO Jeffrey Van Diepen was notified by the IRS that five quarters of the company's federal payroll taxes, totaling $335,304.87, had gone unpaid. Instead of actually paying Pestmaster's payroll taxes, it turned out Branzuela had been spending that money on her own expenses. As a result, the IRS told Van Diepen, the company now owed the government $373,136.[5]

On June 13, 2011, Pestmaster filed a claim under its crime liability policy with insurer Travelers for the losses it suffered as a result of Priority 1's fraud, citing specifically the policy's Computer Crime Insuring Agreement, which provided coverage for losses "directly caused by Computer Fraud," where computer fraud was defined as "the use of any computer to fraudulently cause a transfer of money, securities or other property." On January 4, 2013, Travelers denied the claim, and on June 11, 2013, Pestmaster filed a

complaint against Travelers in Los Angeles Superior Court. The California district judge who presided over the case, John Walter, was unconvinced by Pestmaster's argument that it had been the victim of computer fraud. In particular, he was struck by the fact that nothing Branzuela had done resembled computer hacking. "'Computer Fraud' occurs when someone 'hacks' or obtains unauthorized access or entry to a computer in order to make an unauthorized transfer," Walter wrote in his July 17, 2014, ruling in favor of Travelers. He continued, "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. . . . 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 unauthorized entry into a computer system."[6] The most striking thing about the language Walter used to describe computer fraud as hacking is how closely it echoes the CFAA, especially in its emphasis on authorization. The CFAA, commonly regarded as the US anti-hacking law, makes it illegal to access computers without authorization or in excess of authorization. Although Pestmaster's policy with Travelers made no mention of access, authorization, or hacking in its definition of computer fraud, Walter seized on the idea that computer fraud was synonymous with hacking which, in turn, required unauthorized access to a computer.

The *Pestmaster* ruling extended Barker's logic in the *Brightpoint* case about "intervening events" to apply even to incidents of fraud that didn't involve any physical copies of forged materials but relied entirely on electronic transfers and invoices. Those transfers, so long as they had been approved by the policyholder and not through unauthorized hacking, were still sufficient intervening events to show that "Pestmaster's claimed losses did not 'flow immediately' and 'directly' from Priority 1's use of a computer," Walter wrote in the ruling, quoting Barker's language from *Brightpoint*. Once again, the crucial question was how directly the computer fraud—and, by extension, the computers—had caused these losses because of the language in the policy limiting coverage to losses "directly caused" by computer fraud. It was a significant victory for Travelers, not least because the actual definition of computer fraud in the policy it had issued to Pestmaster made no mention of hackers of unauthorized access, a point Pestmaster emphasized in its appeal. But on July 29, 2016, the Ninth Circuit affirmed

Walter's analysis of the policy's computer fraud provision and his contention that computer fraud was inextricably linked to the issue of authorization. The Ninth Circuit explained its reasoning:

> We interpret the phrase "fraudulently cause a transfer" to require an unauthorized transfer of funds. When Priority 1 transferred funds pursuant to authorization from Pestmaster, the transfer was not fraudulently caused. Because computers are used in almost every business transaction, reading this provision to cover all transfers that involve both a computer and fraud at some point in the transaction would convert this Crime Policy into a "General Fraud" Policy. While Travelers could have drafted this language more narrowly, we believe protection against all fraud is not what was intended by this provision, and not what Pestmaster could reasonably have expected this provision to cover.[7]

However, the Ninth Circuit's willingness to overlook the broad language in the policy Travelers sold to Pestmaster and construe the coverage narrowly, on behalf of the carrier, would not be shared by all courts.

PHISHING, AMBIGUOUS DEFINITIONS, AND *AMERICAN TOOLING V. TRAVELERS*

On March 18, 2015, Gary Gizinski, the vice president and treasurer of Michigan-based company American Tooling Center, sent an email to one of American Tooling's vendors in China, Shanghai YiFeng Automotive Die Manufacture Co. Ltd, asking a YiFeng employee named Jessie Chen to provide any outstanding invoices. American Tooling manufactures metalworking machinery as well as equipment for welding and die cutting and, at the time of the incident, it subcontracted some of its manufacturing work to YiFeng. After completing its orders for American Tooling, YiFeng, and other international vendors, would submit invoices via email to Gizinski, who would then review a spreadsheet of the outstanding accounts payable each week and initiate wire transfers through an online banking portal. For each of these transfers, Gizinski would manually enter the recipient's name, banking information, and the amount to be wired, at which point the assistant comptroller for American Tooling would have to log into the same portal and approve the transfer.[8]

It's unclear what exactly happened to the 2015 email Gizinski sent to Chen, but American Tooling later alleged that "an unidentified third party,

through means unknown, intercepted this email" and then responded to it, impersonating Chen by using a spoofed "from" address and submitting invoices that purported to be from YiFeng. On March 27, 2015, the impersonator emailed Gizinski that YiFeng had changed its banking information and American Tooling should send the payments to the new account. Gizinski complied with the request and wired money to the new account, only to receive an email on April 3 informing him that the transfer had not gone through "due to some new bank rules in the province." YiFeng would return the payment, the email said, and American Tooling would need to wire the money to yet another new bank account. On April 8, 2015, Gizinski wired the same sum of money to this new account, before the previous transfer had been returned. On April 9, 2015, he wired an additional payment of $1,575 at the impersonator's request, and then on May 8, 2015, he sent an additional payment of $482,640.41 to yet another account that he had been instructed to use. Overall, American Tooling transferred approximately $834,000 to the impostor's accounts through these four wire transfers before learning from YiFeng that the company had not received any of these payments.[9]

American Tooling's business insurance policy at the time was provided by Travelers, which promptly denied American Tooling's claim. American Tooling sued Travelers for breach of contract, arguing that the incident was covered under the "computer fraud" provisions of the policy's computer crime section, which stated: "The Company will pay the Insured for the Insured's direct loss of, or direct loss from damage to, Money, Securities and Other Property directly caused by Computer Fraud." This was yet another variation on the definition of covered computer fraud—one that relied on the terms "direct" and "directly" even more heavily than Pestmaster's policy.

Travelers argued that the computer fraud clause did not apply to the YiFeng incident because "the loss was not directly caused by Computer Fraud."[10] The circumstances of the American Tooling incident were slightly more complicated than the Pestmaster fraud had been—there was a "hacker" of sorts involved, whoever was sending spoofed emails from Chen. But other courts had already looked to the *Pestmaster* ruling as the basis for not requiring insurers to cover scams triggered by phishing emails. For instance, a 2016 ruling by the Fifth Circuit had vacated a judgment against Great American Insurance Company (GAIC) in a case that closely resembled the American

Tooling incident. One of GAIC's policyholders, a Houston oil company called Apache Corporation, had changed the bank account information it had on file for a vendor, Petrofac, after receiving phone calls and emails from someone purporting to represent Petrofac. The emails had been sent from the domain petrofacltd.com, instead of the actual Petrofac domain, petrofac.com, but by the time Apache realized its mistake it had already transferred approximately $7 million to the fraudulent account. Apache filed a claim under its crime insurance policy with GAIC. When GAIC denied Apache's claim, Apache sued its insurer and a Texas district judge, Alfred H. Bennett, ruled in Apache's favor in 2015, finding that the scam qualified as an act of computer fraud and GAIC was obligated to cover it.[11] But the following year, in October 2016, Bennett's ruling was overturned by the Fifth Circuit Court of Appeals, which cited the Ninth Circuit's recent ruling in the *Pestmaster* case.[12]

John Corbett O'Meara, the Michigan district judge who authored the first ruling in the *American Tooling* case, relied on both the narrow interpretations of computer fraud set out in the *Pestmaster* and *Apache* cases, and also Barker's earlier reasoning in *Brightpoint*, that "intervening events" separating the use of a computer from an actual act of fraud invalidated computer fraud coverage. In his August 2017 ruling that Travelers was not obligated to cover American Tooling's losses under their computer fraud policy, O'Meara wrote:

> Here, the fraudulent emails did not "directly" or immediately cause the transfer of funds from ATC's bank account. Rather, intervening events between ATC's receipt of the fraudulent emails and the transfer of funds (ATC verified production milestones, authorized the transfers, and initiated the transfers without verifying bank account information) preclude a finding of "direct" loss "directly caused" by the use of any computer.[13]

In other words, because of all the intermediate steps involved in the firm's invoicing process that occurred between receiving the spoofed emails and issuing the wire transfers—Gizinski manually entering account information and initiating transfers, for instance, and the assistant comptroller signing off on those transfers—the fake emails could not be said to have "directly" caused the wire transfers, O'Meara found.

He also referenced the *Pestmaster* precedent that computer fraud required "hacking," and O'Meara clearly did not view spoofed emails as meeting that bar. "Although fraudulent emails were used to impersonate a vendor

and dupe ATC [American Tooling Center] into making a transfer of funds, such emails do not constitute the 'use of any computer to fraudulently cause a transfer.' There was no infiltration or 'hacking' of ATC's computer system," O'Meara wrote. He concluded: "The emails themselves did not directly cause the transfer of funds; rather, ATC authorized the transfer based upon the information received in the emails."[14]

At the heart of O'Meara's initial ruling in favor of Travelers was that same sentiment the Ninth Circuit had put forward the previous year, arguing against construing "computer fraud" to mean any act of fraud involving computers. Both O'Meara and the Ninth Circuit seemed to be getting at the idea that computer fraud occurs when a fraudulent act is carried out *entirely* through a computer system, not just using a computer peripherally. It's a distinction that Walter also made in his ruling in the *Pestmaster* case, when he wrote that the "use of a computer was merely incidental to, and not directly related to, the misuse of Pestmaster's funds."[15] In *Apache*, the Fifth Circuit had made a similar distinction, finding that "the [fake Petrofac] email was part of the scheme; but, the email was merely incidental to the occurrence of the authorized transfer of money."[16] But distinguishing between when computers are "merely incidental" to acts of fraud and when they are "directly related" to or "directly cause" fraud can be complicated.

Adding to the growing consensus that computer fraud should be construed narrowly, the Eleventh Circuit issued an opinion on a computer fraud insurance claim in May 2018 for a case in which a company called Interactive Communications International Inc. (InComm) was suing its insurer, GAIC. InComm sold reloadable debit card credits and had lost $11.4 million in 2013 and 2014 when fraudsters figured out how to redeem individual InComm credits multiple times. The company sought coverage for the losses under its computer fraud policy, issued by GAIC, but the Eleventh Circuit ruled that their losses were not covered because "although the fraudsters' manipulation of InComm's computers set into motion the chain of events that ultimately led to InComm's loss, their use of the computers did not 'directly'—which is to say immediately and without intervention or interruption—cause that loss."[17]

To justify this analysis, the Eleventh Circuit outlined four distinct steps in the InComm fraud scheme: (1) the fraudsters manipulated InComm's computer system to enable duplicate redemption, (2) InComm received a call to redeem a credit and transferred money to a bank that issued the

reloaded debit card with the appropriate credits, (3) the debit card user made a purchase and paid using the reloaded card, and finally, (4) the bank that had received money from InComm in step 2 transferred money to the merchant to cover the purchase made by the cardholder. "InComm insists that its loss occurred at Step 2—and is thus 'directly' the result of the Step-1 fraud. . . . But the facts of the case demonstrate otherwise," the Eleventh Circuit ruled. "InComm retained at least some control over the funds . . . even after the Step-2 transfer, and could prevent their loss by intervening to halt the disbursement of money . . . to merchants at Step 4." Based on that analysis, the Eleventh Circuit concluded:

> the loss did not occur until—at Step 4—Bancorp [the bank] actually disbursed money from the InComm-earmarked account to pay merchants for purchases made by cardholders. That was the point at which InComm could not recover its money. That was the point of no return. That being the case, it seems clear to us that InComm's loss did not "[result] directly" from the initial computer fraud.[18]

It is a striking conclusion partly because the perpetrators in this case did, in fact, "hack" into InComm's computer systems without authorization to allow them to redeem credits multiple times—that was the first step the Eleventh Circuit identified in their breakdown of the fraud. But because it occurred too many steps before the actual fraud was carried out, even the unauthorized hacking in this case was not considered sufficient to rise to the level of computer fraud.

There had clearly been several intermediate steps between American Tooling's receipt of the fraudulent invoices and their issuing the payments (Gizinski entering account information into the system, Gizinski initiating the transfers to those account, the assistant comptroller signing off on those transfers) and at no point had anyone actually hacked into American Tooling's computer systems. If the Sixth Circuit had upheld O'Meara's ruling that the fake emails sent to Gizinski by someone impersonating Chen had not "directly" caused the fraud, and were instead merely incidental to it, such a ruling would have been entirely consistent with other courts' decisions. Instead, just two months after the Eleventh Circuit issued its opinion for *Interactive Communications*, the Sixth Circuit reversed O'Meara's decision in a ruling filed on July 13, 2018, that found that American Tooling had in fact been the victim of computer fraud. The Sixth Circuit did cite the

Pestmaster decision, but rather than focusing on the section of the decision about the risk of converting computer crime policies into general fraud policies through overbroad definitions of computer fraud, the Sixth Circuit instead highlighted the immediately following clause in the *Pestmaster* ruling, which acknowledged that "Travelers could have drafted this language more narrowly," returning to the principal that ambiguities in insurance policies must be interpreted against the insurer.[19]

The Sixth Circuit disagreed with the idea that, absent that narrower definition being spelled out in the insurance policy itself, computer fraud should be restricted to instances of unauthorized hacking of computer systems. The court explained in its *American Tooling* decision, "Travelers' attempt to limit the definition of 'Computer Fraud' to hacking and similar behaviors in which a nefarious party somehow gains access to and/or controls the insured's computer is not well-founded. If Travelers had wished to limit the definition of computer fraud to such criminal behavior it could have done so."[20] The fraudulent emails sent to American Tooling from a spoofed address were enough to render the incident a case of computer fraud, the Sixth Circuit decided, because those "emails fraudulently caused ATC to transfer the money to the impersonator."[21]

As for whether the spoofed emails *directly* caused American Tooling to transfer the money, the Sixth Circuit adopted the approach of the Eleventh Circuit in the *Interactive Communications* case, sketching out a series of steps to the fraud. But the Sixth Circuit identified only two such steps "when framed at the same level of generality as the Eleventh Circuit used." The Sixth Circuit explained:

> ATC received the fraudulent email at step one. ATC employees then conducted a series of internal actions, all induced by the fraudulent email, which led to the transfer of the money to the impersonator at step two. This was "the point of no return," because the loss occurred once ATC transferred the money in response to the fraudulent emails. Thus, the computer fraud "directly caused" ATC's "direct loss."

It is an astonishing twisting of the Eleventh Circuit's logic—it conflates the steps in which American Tooling employees "conducted a series of internal actions" (i.e., checking that the work for which they were being invoiced had been completed, entering the new bank account information into their systems, submitting the transfer, approving the transfer), as well as the electronic

transfer itself, into a single step so that the fake emails can be presented as the direct cause of the fraudulent transfer.

The Sixth Circuit went to great lengths to explain how its ruling was consistent with those issued by the Ninth and Eleventh Circuits, arguing that the spoofed emails distinguished *American Tooling* from *Pestmaster* and that there were fewer intermediate steps between the computer action and the subsequent fraud in *American Tooling* than in *Interactive Communications*. But what was really different about *American Tooling* was the Sixth Circuit's willingness to go after the ambiguity of the language in the Travelers policy defining computer fraud. *American Tooling* complicated the growing consensus around what computer fraud meant in the context of insurance policies, but it also made clear that the burden of appropriately scoping those definitions fell to insurers. That shifting of responsibility was in line with the principle that any ambiguity in the terms of an insurance policy should be interpreted in favor of the policyholders. In some ways, what is most surprising about *American Tooling* is not that the court departed from the decisions of so many other courts but rather that it had taken until 2018 for a circuit court to place the onus on insurers to narrowly define computer fraud in their policies. That so many courts had previously given the benefit of the doubt to insurers when it came to interpreting computer fraud policies suggests how concerned judges had been about the scale of computer fraud claims that might result from broader interpretations. But it also speaks to the inability—or unwillingness—of both courts and insurers to think through more specific, narrow definitions and descriptions of the different roles computers could play in financial fraud and what it meant for them to play a "direct" role.

"ARMED WITH A COMPUTER CODE": *MEDIDATA SOLUTIONS V. FEDERAL INSURANCE COMPANY*

In July 2018, the same month that the Sixth Circuit issued its ruling in *American Tooling*, the Second Circuit decided a very similar case between a company called Medidata Solutions and its insurer, Federal Insurance Company. In September 2014, Medidata had made a $4,770,226 transfer to someone claiming to be an attorney named Michael Meyer, after a series of forged emails that appeared to come from Medidata's president had authorized the

transfer. Federal Insurance denied Medidata's claim under its computer fraud policy, but a New York court ruled in July 2017 that Medidata's losses were covered by the policy because the spoofed emails constituted an act of hacking. Federal Insurance had argued "that the emails did not directly cause Medidata's loss, because no loss would have taken place if Medidata employees had not acted on the instructions contained in those emails." They had also tried to persuade the court that spoofed emails did not fall under the definition of computer fraud in Medidata's policy, which specified that such an incident must involve the "direct loss" of money resulting from "the fraudulent: (a) entry of Data into or deletion of Data from a Computer System or (b) change to Data elements or program logic of a Computer System, which is kept in machine readable format."[22] Here was yet another variation on the definition of computer fraud, using different policy language that was less predicated on how directly a computer caused the fraud and more focused on how exactly the computer and the data stored on it were being manipulated.

The New York district judge who ruled on the case, Andrew L. Carter Jr., considered an email with a spoofed "from" address to be a kind of hacking because that email "accessed" Medidata's email system by landing in an employee's inbox. "The fraud on Medidata was achieved by entry into Medidata's email system with spoofed emails armed with a computer code that masked the thief's true identity," Carter wrote in his ruling. He referenced the Medidata insurance policy's language about "entering" and "changing" data, adding that "the thief's computer code also changed data from the true email address to Medidata's president's address to achieve the email spoof."[23] Carter's language, particularly his reference to "spoofed emails armed with computer code"—a phrase he used twice in the ruling—hints at just how important judges' technical understandings of computers and the Internet were to their decisions about what was and was not computer fraud.

Going by the definition of computer violations in Medidata's insurance policy, the fake email would have involved the "entry of data into . . . a computer system"—but so does everything done using a computer. It's a very broad definition, in some sense, for an insurer to be relying on to delimit computer fraud. Carter's lengthy description of how email works made the process of spoofing a from address sound considerably more complicated than it actually was. Carter explained:

> The thief constructed messages in Internet Message Format ("IMF") which the parties compare to a physical letter containing a return address. The IMF message was transmitted to Gmail in an electronic envelope called a Simple Mail Transfer Protocol ("SMTP"). Much like a physical envelope, the SMTP Envelope contained a recipient and a return address. To mask the true origin of the spoofed emails, the thief embedded a computer code. The computer code caused the SMTP Envelope and the IMF Letter to display different email addresses in the "From" field. The spoofed emails showed the thief's true email address in the SMTP "From" field, and Medidata's president's email address in the IMF "From" field. When Gmail received the spoof emails, the system compared the address in the IMF "From" field with a list of contacts and populated Medidata's president's name and picture. The recipients of the Gmail messages only saw the information in the IMF "From" field.[24]

As for the idea that the intervening steps of Medidata employees authorizing the transfer, after they received the forged emails, would disqualify the incident from being directly caused by computers, Carter rejected that as well. "Medidata employees only initiated the transfer as a direct cause of the thief sending spoof emails posing as Medidata's president," he wrote. Here, the particular language in Medidata policy was especially relevant since it did not emphasize the directness of a computer's link to fraudulent activity to the same extent as the American Tooling or Pestmaster policies, requiring only that the policyholder suffer a "direct loss . . . resulting from computer fraud" rather than a loss "directly related" to the use of a computer.

The next year, just days before the Sixth Circuit's decision reversing the lower court's *American Tooling* ruling, the Second Circuit affirmed Carter's opinion that the Medidata email scam was covered by its computer fraud policy with Federal Insurance. "The chain of events was initiated by the spoofed emails, and unfolded rapidly following their receipt," the Second Circuit wrote, dismissing Federal Insurance's appeal that the emails themselves did not cause the fraudulent transfer. "While it is true that the Medidata employees themselves had to take action to effectuate the transfer, we do not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred," the ruling continued. Like Carter, the Second Circuit viewed email spoofing as sufficient to render the incident an act of computer fraud, writing that "the attack represented a fraudulent entry of data into the computer system, as the spoofing code was introduced into the email system."[25]

At the heart of these disputes between insurers and their customers over what constitutes computer fraud is the question of how directly linked to a computer the actual act of fraud must be. Part of what makes these definitional issues about computer fraud and unauthorized access to computers difficult to resolve is the variety of different ways that computers feature in everyday life—and crime—as well as the large spectrum of technical skills and manipulations required to use and exploit them. The ubiquity of computers in business settings makes it easy to understand the Ninth Circuit's concern in *Pestmaster* that a broad interpretation of the meaning of computer fraud might allow companies to transform these into "general fraud" policies. These concerns have been exacerbated by how confused and, in many cases, nonspecific policy language defining computer fraud has been, contributing to continuing legal disputes and uncertainty for both insurers and their customers about what those policies actually cover.

OVERLAPPING COVERAGE AND *NATIONAL BANK OF BLACKSBURG V. EVEREST*

On Saturday, May 28, 2016, hundreds of ATMs across North America began dispensing cash from National Bank of Blacksburg accounts without the account owners' knowledge or authorization. The unauthorized withdrawals continued through the weekend, ending early in the morning of Monday, May 30. All told, the fraudulent disbursements, including related fees, amounted to $569,648.24. National Bank couldn't figure out what had happened—how someone had gotten access to so many of its customers' accounts or why all of its automatic safeguards, such as daily withdrawal limits to prevent individuals from taking out large sums of cash at once and blocks on withdrawals for overdrawn accounts, had been overridden.

National Bank hired digital forensics and security firm Foregenix to investigate the theft. Foregenix determined that the incident had likely originated with a phishing email sent to National Bank employees, which enabled the criminals to install malware onto a computer within National Bank's network. From that initial toehold in National Bank's system, the attackers were then able to access and install malware on another machine, Foregenix believed, and that second server had access to the STAR Network, a debit payment network that National Bank used to provide "bank card processing services" to its customers so that they could use their bank

cards at ATMs and retailers. Certain National Bank employees were able to access the STAR Network through a web portal that allowed them to change several parameters and security settings for their customers' accounts. For instance, it was possible for National Bank to block or activate customer accounts as well as to "remove or alter anti-theft and antifraud protections such as 4-digit personal identification numbers (PINs), daily withdrawal limits, daily debit card usage limits, and fraud score protections" through their access to the STAR Network.[26] By stealing credentials for the National Bank employees who had administrator-level access to the STAR Network, the perpetrators of the 2016 breach were then able to "actively monitor customer accounts and remove or modify numerous security measures on accounts belonging to National Bank customers." So, during the last weekend of May 2016, when the theft occurred, the perpetrators had been able to continue dispensing funds past the standard limits by logging into the STAR Network and removing blocks on overdrawn accounts and returning customer accounts to active status even after they had been maxed out, Foregenix reported to National Bank. But how exactly the criminals had managed to initiate so many withdrawals across the continent or collect the cash they stole without attracting attention remained a mystery. Even following the investigation by Foregenix, National Bank concluded that "the exact mechanics of this criminal enterprise are still not fully known."[27]

Then, in January 2017, National Bank suffered another, nearly identical intrusion, likely perpetrated by the same group in Russia that had been accused of breaching their systems in 2016. National Bank hired Verizon to investigate this second incident. Verizon determined that the 2017 breach, like the 2016 one, had begun with a phishing email sent to National Bank employees. This time, the phishing email that initiated the theft included an attached Word document that contained malware, in the form of a macro, which the intruders used to steal more employee credentials. As in 2016, the intruders were able to leverage this malware to gain access to other computers at National Bank, including one that had access to the STAR Network as well as to the bank's Navigator software, which was used to manage customer banking transactions. With their access to Navigator, the perpetrators were able to fraudulently credit $2,070,000 to National Bank customer accounts. Then, returning to their previous pattern, at the beginning of the first full weekend in January 2017, the intruders used their access to the STAR Network to disburse funds from these accounts to hundreds of

ATMs beginning on Saturday, January 7, 2017, and continuing through the morning of Monday, January 9, 2017, when National Bank was alerted to the withdrawals. This time, the fraudulent disbursements and related fees totaled $1,833,984.58—thanks to the fraudulent deposits of more than $2 million, the perpetrators had managed to significantly increase how much money they were able to withdraw from the targeted accounts.

On July 27, 2017, National Bank filed a claim with Everest National Insurance Co. for the 2016 and 2017 incidents, which had cost the bank $2.4 million, under its Computer and Electronic (C&E) Crime Rider. National Bank's C&E Crime Rider, which had a single loss limit of liability totaling $8 million and a $125,000 deductible, covered losses "resulting directly from an unauthorized party (other than an Employee) acting alone or in collusion with others, entering or changing Electronic Data or Computer Programs within any Computer System . . . operated by the Insured . . . provided that the entry or change causes: (1) property to be transferred, paid or delivered, (2) an account of the Insured, or of its customer, to be added, deleted, debited or credited, or (3) an unauthorized account or a fictitious account to be debited or credited." The May 2016 theft, as described by National Bank in its complaint, certainly seemed to fit these criteria—it did involve changing electronic data in such a way as to cause money to be paid from National Bank accounts. On June 13, 2018, almost a year after National Bank filed its claim, Everest denied coverage for both incidents under the C&E Crime Rider. Instead, Everest said, the losses associated with the two incidents were covered exclusively under the Debit Card Rider in National Bank's policy, which had a single loss limit of liability totaling $50,000 and a $25,000 deductible. The Debit Card Rider covered losses "resulting directly from Debit Transactions, or automated mechanical device transactions, due to the fraudulent use of a lost, stolen or altered Debit Card or Counterfeit Debit Card used to access a cardholder's deposit account through an electronic payment device or automated mechanical device."

In its coverage determination, Everest raised two exclusions in National Bank's policy that they argued made clear there was no coverage for the incidents other than that provided by the Debit Card Rider. The first relevant exclusion, Exclusion K, excluded coverage for losses "resulting directly or indirectly from the use or purported use, of credit, debit, charge, access, convenience, or other cards . . . (1) in obtaining credit or funds, or (2) in gaining access to automated mechanical devices which, on behalf of

the Insured, disburse Money, accept deposits, cash checks, drafts or similar Written instruments or make credit card loans." The second exclusion Everest cited, Exclusion L, excluded coverage for losses "involving automated mechanical devices which, on behalf of the Insured, disburse Money, accept deposits, cash checks, drafts or similar Written instruments or make credit card loans." The lack of clarity around the specific circumstances of the theft made it difficult to parse exactly how relevant these exclusions were to the 2016 and 2017 incidents. It did not appear from Foregenix's account of what happened that there was necessarily any use of "credit, debit, charge, access, convenience, or other cards," as required for Exclusion K to apply, though clearly there were automated mechanical devices—ATMs—involved in disbursing money on behalf of National Bank.

National Bank sued Everest, and it seemed, at first, like exactly the kind of incident that would fit even the narrowest definition of computer fraud. When Judge Berrigan had dismissed MHSFI's claim that its losses in the Madoff Ponzi scheme were the consequence of computer fraud, she had pointed out, "At no point did the transferors open their online statements and learn in shock that transfers had occurred without their knowledge." But in the case of the National Bank scam, people actually had opened their online statements and learned in shock that withdrawals had occurred without their knowledge. The lawsuit was complicated, however, by the differences in the relevant policy language and the fact that neither party seemed to be entirely certain exactly how the theft was perpetrated. In their complaint, National Bank described the incident as follows:

> The hacking allowed unidentified criminal actors, through coordinated unauthorized intrusions into National Bank's computer systems and network, to change customer account balances, monitor network communications, remove critical security measures such as anti-theft and anti-fraud protections, conduct keystroke tracking, and otherwise enter or change electronic data and computer programs on National Bank's computer systems, which allowed them to illegally withdraw funds from the accounts of National Bank customers, post fake deposits, and remove illegal transactions from customer accounts. . . . Critical to this Court's analysis of National Bank's claims, none of the losses arise from a National Bank customer's debit card being stolen, or from their debit card information being stolen directly from a National Bank customer's possession without their knowledge or permission (e.g. use of a "skimmer" or of a counterfeit or fraudulently obtained debit card).

The relatively vague description of what actually happened offered by National Bank—"unauthorized intrusions" that enabled the perpetrator to "change customer account balances" and "enter or change electronic data and computer programs"—suggested that the bank was not entirely clear how the stolen credentials were used to steal $2.4 million. This is not unusual in the aftermath of cybersecurity incidents. Depending on how carefully companies log changes in their networks and computer systems, how long those logs are stored, and how quickly a breach is noticed, it may not always be possible for them to completely reconstruct every step of an intrusion and how it happened. In the case of National Bank, however, this uncertainty about the mechanics of the breach also contributed to the controversy over which of the two riders in its crime coverage was most directly applicable to the incident in question.

The two riders appeared to cover distinct threats—stolen, lost, or counterfeit debit cards, on the one hand, and malicious manipulation of the bank's computer systems, on the other—but, in fact, there was considerable potential for overlap between the two as the National Bank incidents demonstrated. Even if fraudulent or stolen debit cards were used to make the withdrawals, and it is not clear that they were, it was quite possible—probable, even—that the information for manufacturing those cards came from the perpetrators' access to the bank's computer network. And certainly, the perpetrators' ability to withdraw large sums of money from those accounts using ATMs was directly caused by the fraudulent deposits that the intruders had made using their remote access to the computer network. Conceivably, both riders could have been applicable to the National Bank incidents, assuming it was possible to show that stolen or fraudulent debit cards played some role in the theft. However, only the Debit Card Rider—and not the C&E Crime Rider—referenced coverage of losses that involved an "automated mechanical device," such as an ATM. That appeared to be Everest's rationale for determining that the Debit Card Rider was the sole relevant coverage for National Bank's claim since ATMs, unlike debit cards, were indisputably involved in the theft.

On January 23, 2019, National Bank and Everest settled their case at a closed meeting overseen by a magistrate judge.[28] The terms of the settlement were confidential and therefore offered little insight into a central challenge of cybercrime-related claims that the case had raised, namely that many cybersecurity incidents fall under multiple types of coverage because

computers and cyber risk can be tied to so many different types of losses. In the case of National Bank, Everest was able to use these overlapping policies against its customer to try to significantly reduce how much the bank would be reimbursed under its policy by classifying the incident—which combined elements of computer crime and debit card fraud—solely under the portion of National Bank's insurance with the lowest coverage. The confusion around cybercrime coverage arose not just from disagreements over how computer fraud should be defined, but also, in part, from situations like the one National Bank found itself in where an incident of computer fraud overlapped with other potential kinds of fraud and therefore with other coverage.

Computer fraud, and cybercrime more generally, has proven a challenging category of risks for insurers to define clearly, both because there is a wide variety of mechanisms for executing fraud through computers, and these mechanisms are constantly changing, and because cybercrimes often overlap with other types of theft. Adding to these challenges, the victims of cybercrimes aren't always able to retrace every detail of how these crimes were committed, making it even more difficult to know how exactly computers were involved. Many of the policies governing computer fraud have relied on language about fraud resulting "directly" from the use of computers but the variations on that language, and the different interpretations of it by different courts, suggest a need for much greater specificity and clarity in defining what types of crime carriers view as resulting directly from computers and how cybercrimes that overlap with other types of fraud are covered. Policyholders—and insurers—would benefit from more standardization of the language used to define computer fraud in these policies and perhaps even from breaking down computer fraud into several different, more specific types of cybercrime instead of trying to find language broad enough to encompass the diversity of computer uses and crimes but still narrow enough so as not to include every crime involving a computer in any way.

Cyberinsurance Policy

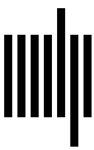
Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks

By: Josephine Wolff

Citation:

Cyberinsurance Policy: Rethinking Risk in an Age of Ransomware, Computer Fraud, Data Breaches, and Cyberattacks
By: Josephine Wolff
DOI: 10.7551/mitpress/13665.001.0001
ISBN (electronic): 9780262370752
Publisher: The MIT Press
Published: 2022

The open access edition of this book was made possible by generous funding and support from MIT Press Direct to Open



The MIT Press

The MIT Press would like to thank the anonymous peer reviewers who provided comments on drafts of this book. The generous work of academic experts is essential for establishing the authority and quality of our publications. We acknowledge with gratitude the contributions of these otherwise uncredited readers.

This book was set in Bembo by Westchester Publishing Services.

Library of Congress Cataloging-in-Publication Data

Names: Wolff, Josephine, author.
Title: Cyberinsurance policy : rethinking risk in an age of ransomware, computer fraud, data breaches, and cyberattacks / Josephine Wolff.
Description: Cambridge, Massachusetts : The MIT Press, [2022] | Series: Information policy series | Includes bibliographical references and index.
Identifiers: LCCN 2021045988 | ISBN 9780262544184 (paperback)
Subjects: LCSH: Computer insurance. | Computer security—Management. | Cyberspace—Security measures—Management. | Computer crimes—Prevention. | Risk management.
Classification: LCC HG9963.5 .W65 2022 | DDC 658.4/78—dc23/eng/20220114
LC record available at https://lccn.loc.gov/2021045988