CYBER-CRIMES: How Have Courts Dealt with the Insurance Implications of this Emerging Risk?

By Alan Rutkin

Insurance coverage law has one firm rule: *when a new risk emerges, new coverage issues follow.* There are roughly forty cases addressing insurance coverage for cyber-crime liability. *W*e have seen three interesting questions recurring:

(1) Does the policy apply to acts by this person?

(2) Does the policy apply to this type of conduct?

(3) Was the problem *caused* by computer activity?

1) Does the policy apply to acts by this person?

A common coverage question in cyber-crime claims is whether the policy applies to the acts of the *person* who used the computer to cause the injury.

The issue is authorization. Computer-specific policies often limit coverage to the bad acts of persons who are *not* authorized. Acts by employees are often excluded.

In *Apps Communication, Inc. v. Hartford Casualty Insurance Co.*,[1] a Computers and Media Endorsement excluded dishonest or criminal acts by employees. A virus damaged the policyholder's computers. The policyholder alleged that a "virus was introduced" into its computer system, but the policyholder did not allege who introduced the virus. The court held that the policyholder needed to allege who introduced the virus to make it clear that the employee exclusion did not apply.[2]

---

[1] No. 11C3994, 2011 U.S. Dist. LEXIS 118906 (N.D. Ill. Oct. 14, 2011); *see also Palm Hills Properties v. Continental Ins. Co.*, No. 07-668-RET-SCR, 2008 WL 4303817 (M.D. La. July 23, 2008)(court applied employee exclusion to bar coverage).

[2] This decision is very favorable to insurers. Generally, insurers have the burden to establish exclusions. But here, the court found that the policyholder's complaint effectively needed to allege that the exclusion did not apply. *But see NMS Services, Inc. v. Hartford*, 62 F. App'x 511, 2003 U.S. App. LEXIS 7442 (4th

Like the employee exclusion, several courts have considered and enforced exclusions for acts of authorized representatives. In *Stop & Shop v. Federal Insurance Co.*,[3] the First Circuit applied an "authorized representatives" exclusion when a tax payment service stole $13 million from a supermarket. In *Milwaukee Area Technical College v. Frontier Adjusters*,[4] the court applied an "authorized representatives" exclusion when a college's claim adjuster stole $1.6 million.

Other courts faced more nuanced versions of the authorized person issue.

In *Universal American Corp. v. Union Fire Insurance Co*.,[5] a "Computer Systems Fraud" policy covered "[l]oss resulting directly from a fraudulent … entry of Electronic Data." The policyholder, a health insurer, suffered $18 million in losses from fraudulent claims. Most of these claims were submitted by providers. The providers entered fraudulent information. The case hinged on the meaning of "fraudulent entry." Did it extend to the entry of information that was fraudulent? Or, was it limited to instances where it was fraudulent to enter any information at all. The court found that "entry" focused on the act of entering data; the data was fraudulent, but the act of entering it was legitimate. The court found for the insurer.

In *Morgan Stanley Dean Witter & Co. v. Chubb*,[6] an authorized person made unauthorized transfers causing about $100 million in losses. The policy, an "Electronic Computer Crime Policy," focused on how the transfers were made. If the transfer was

---

Cir. Sept. 24, 2003) (applying "acts of destruction" exception to exclusion where bad actor was an employee).

[3] 136 F.3d 71 (1st Cir. 1998).

[4] 312 Wis. 2d 360 (Wis. App. 2008).

[5] 38 Misc. 3d 859, 959 N.Y.S.2d 849 (N.Y. Sup. Ct. 2013), ***aff'd,*** 25 N.Y. 3d 675 (2015).

[6] No. A-4124-03T2, 2005 N.J. Super. Unpub. LEXIS 798 (App. Div. Dec. 2, 2005).

made by fax, coverage only applied if the person giving the fax instructions was not authorized to do so. The voice coverage, however, extended to unauthorized instructions by authorized persons. Consequently, the court found that the fax coverage did not apply, but the voice coverage did apply.

In *Pestmaster Services v. Travelers Casualty and Surety Co.,*[7] a payroll company was authorized to electronically transfer funds from the insured's account into its own as part of its payroll services. The payroll company failed to pay the insured's payroll taxes as required by the contract, and instead used the money to pay its own obligations. The insured made a claim under its Computer Crime policy, which covered losses directly caused by "Computer Fraud." The court held that the payroll company's acts did not constitute "Computer Fraud" because the funds transfer was authorized and did not involve hacking or any unauthorized entry into a computer system.[8] The fraud took place only after the authorized transfer.

1. <u>Does the policy cover this act?</u>

In claims arising from cyber-crimes, many cases focus on whether the policy applies to the *act* that caused the injury.

Generally, computer fraud policies cover hacking. Nearly *all* criminals *use* computers. Only *some* criminals *hack* computers. Consequently, a common issue in the "act" cases is distinguishing *hacking* a computer from *using* a computer.

[7] No. CV-13-5039-JFW(MRWx), 2014 U.S. Dist. LEXIS 108416 (C.D. Cal. July 17, 2014).

[8] The court observed that "Computer Fraud" 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." *Id.* at *19.

Hacking is "to gain access to a computer illegally."[9] Policyholders have tried to extend hacking coverage to instances in which criminals give bad information that is then legally entered into the policyholder's computer. At least two courts have distinguished giving bad information from actually breaking into a computer. Both courts found that the hacking coverage did not apply.[10]

Similarly, another court recently distinguished a data *refusal* from a data *error*. The policy covered errors, not intentional refusals. The court upheld the insurer's disclaimer.[11]

Just a few weeks ago, the Supreme Court of New Hampshire found that "hacking" is not an occurrence because it is "inherently injurious."[12]

Finally, we're seeing talk about whether coverage can be subject to policyholders following "best practices." In 2013, an insurer sought a declaratory judgment of no coverage based upon an exclusion for "Failure to Follow Minimum Required Practices." The case was dismissed on procedural grounds. But, we will surely see more of the "best practices" issue.[13]

---

[9] Merriam-Webster.com definition of "hack," *available at* http://www.merriam-webster.com/dictionary/hack.

[10] *Hudson United Bank v. Progressive Cas. Ins. Co*., 112 F. App'x 170, 2004 U.S. App. LEXIS 21335 (3d Cir. Oct. 14, 2004) (fraudulent data entry was not recoverable because data was not entered into the covered computer (*i.e.,* the policyholder's computer); *Northside Bank v. American Cas. Co*., 60 Pa. D. & C. 4th 95 (Ct. Common Pleas Jan. 10, 2001), ***aff'd,*** 792 A.2d 625 (Pa. Super. Ct. 2001) (coverage protecting a bank against hackers did not apply to the introduction of information that was fraudulent when received). *See also Metro Brokers v. Transportation Ins. Co.*, No. 1:12-cv-3010, 2013 U.S. Dist. LEXIS 184638 (N.D. Ga. Nov. 21, 2013), ***aff'd,*** 603 Fed. App'x. 833 (11th Cir. 2015) (policyholder conceded that malicious code and system penetration exclusion applied to virus).

[11] *Travelers Property Cas. Co. v. Federal Recovery Services, Inc.,* 103 F. Supp. 3d 1297 D. Utah 2015).

[12] *Todd v. Vermont Mutual Insurance Co.*, No. 2015-0233 (N.H. Apr. 7, 2016).

[13] *Columbia Casualty Co. v. Cottage Health System,* No. 2:15-cv-03432 (C.D. Cal. 2015).

2. Does the policy limit coverage to losses that computer activity caused "directly"?

Claims under computer policies frequently involve a causation issue. Coverage is typically limited to losses "directly related" to some type of bad act on a computer.

Insurers often maintain that direct means immediate, without an intervening cause.[14] Policyholders, on the other hand, argue for a "proximate cause" approach.

In *Retail Ventures*,[15] criminals used computers to gain access to their victims. The criminals used computers to steal credit card information, and then stole from the accounts. The computers set up the crimes, but the computers were not used to carry out the crimes. The court found the losses resulted directly from computers.

Similarly, in *Apache Corp. v. Great American Insurance Co.,*[16] a federal district court held that a computer fraud policy covered wire transfers to a phony account because a fraudulent email was a substantial factor in bringing about the injury. There, the insured's employee received a phone call from an imposter posing as one of the insured's vendors. The imposter claimed to be providing new account information for future wire payments. The employee asked for a written request on the vendor's official letterhead. The imposter sent the letter by email. Another employee of the insured called the number on the letter to verify the request and obtained supervisor clearance before wiring the funds.

After learning that the account was fraudulent, the insured sought recovery under the computer fraud section of its crime protection policy. The policy covered loss

---

[14] *See, e.g., Retail Ventures, Inc.,* 691 F.3d at 824.

[15] 691 F.3d 821.

[16] No. 4:14-CV-237, 2015 U.S. Dist. LEXIS 161683 (S.D. Tex. Aug. 7, 2015).

"resulting directly from the use of any computer to fraudulently cause a transfer of" property to another. The insurer declined coverage on the basis that the scheme's success hinged on the telephone calls and related acts. It did not result directly from the use of a computer. The court disagreed and held "despite the human involvement that followed the fraud, the loss still resulted directly from computer fraud, i.e. the email directing [the insured] to disburse payments to a fraudulent account."[17]

In contrast to these decisions, several courts have found that the use of a computer was merely incidental to the loss. In *Pinnacle Processing Group v. Hartford Casualty Insurance Co.*,[18] the court held that "direct" means "without any intervening cause." In *Brightpoint, Inc. v. Zurich American Insurance Co.,*[19] the court cited Black's Law Dictionary to state that direct means "in a straight line or course" and "immediately."[20] In *Pestmaster*, the court stated that "direct means direct," and held that losses must "flow immediately and directly" from computer use.[21]

[17] *Id.* at *6-7. The case is currently on appeal before the Fifth Circuit.

[18] No. C10-1126-RSM, 2011 U.S. Dist. LEXIS 128203 (W.D. Wash. Nov. 4, 2011).

[19] 2006 U.S. Dist. LEXIS 26018.

[20] *Id. at *20.*

[21] *Pestmaster,* 2014 U.S. Dist. LEXIS 108416 at *23-24 (computer was merely incidental to misuse of funds where fraud occurred after an authorized electronic transfer).