

Cybercrimes

How Courts Are Dealing
with Insurance
Implications
of This Emerging Risk

By Alan Rutkin and Robert Tugander



To say that cybercrime is an emerging risk is an understatement. The headlines tell it all. It seems like every few weeks a story breaks about another major hacking. Whether it is a large retailer like Target or Home Depot, a financial giant like J.P. Morgan, a major Hollywood studio like Sony, or even the United States Post Office, any institution or person can become a victim of cybercrime.

Advancement in computer technology has immeasurable benefits. But with it comes new kinds of risks. After all, criminals use computers too. Sometimes the crimes are new and different, like stealing customer lists, credit card data, or trade secrets. Other times, cybercrimes are just new versions of old deeds. Today, bank robbers can use laptops and Wi-Fi instead of masks and guns.

Perhaps statistics tell the story best. In 2013, there were 62 percent more data breaches than in 2012.¹ In 2014, there were 27.5 percent more data breaches than in 2013, and the 2015 numbers are likely to have been even higher.² Without question, a new risk—cybercrime—has emerged.

Insurance coverage law has one firm rule: *when a new risk emerges, new coverage issues follow*. There are roughly 40 cases addressing insurance coverage for cybercrime liability. Several factors complicate this new body of coverage law.

First, cybercrimes require courts to fit new technologies into old categories. Is data “physical”? Is a data breach a “publication”? How do “intentional act” exclusions apply to computer activity? Courts are wrestling with many of these issues.

Second, cybercrime claims implicate new and different policy forms. For the last two decades of the twentieth century, pollution presented difficult coverage questions. But, these questions generally focused on a few common policy terms. Cybercrime claims, on the other hand, involve different forms and terms.

Third, computer-specific policies involve factually intensive questions. These policies provide specific grants of coverage. Coverage is limited to defined persons, acts, and injuries. These limitations lead to factual disputes.

Given these three factors, as well as the complexity inherent in new technology, difficult coverage issues arise. The cases are too few to identify trends or majority views, but five questions help organize and understand the existing law.

Does the Policy Apply to Acts by This Person?

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

The issue is authorization. Both *authorized* persons and *unauthorized* persons present risks. But the risks

are different, and policies treat them differently. 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.*,³ 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.⁴

Like the employee exclusion, several courts have considered and enforced exclusions for acts of authorized representatives. In *Stop & Shop Cos. v. Federal Insurance Co.*,⁵ 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 of Milwaukee*,⁶ 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. National Union Fire Insurance Co. of Pittsburgh, PA*,⁷ 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 Group of Insurance Cos.*,⁸ 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 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, Inc. v. Travelers Casualty & Surety Co. of America*,⁹ a payroll company was authorized to electronically transfer funds from the insured’s



TIP

To keep track of cyber coverage issues, remember the berry ACAI. Most issues involve Authorization, Causation, Act, or Injury.

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.¹⁰ The fraud took place only after the authorized transfer.

Does the Policy Cover This Act?

In claims arising from cybercrimes, many cases focus on whether the policy applies to the *act* that caused the injury. The cases address different policy forms with different coverage grants, and the grants are applied to different factual circumstances. Given the many variables, it is impossible to boil the cases down to a few rules or trends, and draw clear lessons. That said, a few points should be noted.

Alan Rutkin is a partner at Rivkin Radler LLP in New York City, where he often serves on the firm's management committee. He has represented insurance companies in insurance coverage matters for 30 years. Among a number of TIPS leadership positions, Rutkin is a past chair of TIPS's Insurance Coverage Litigation Committee and currently serves on the TIPS Council. **Robert Tugander** is a partner at Rivkin Radler LLP in Uniondale, New York, where he counsels insurers in complex coverage disputes. He has handled a wide array of insurance matters relating to environmental, toxic torts, intellectual property, and business tort claims. They can be reached, respectively, at alan.rutkin@rivkin.com and robert.tugander@rivkin.com.

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.

Hacking is "to gain access to a computer illegally."¹¹ 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.¹²

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.¹³

Another issue is that computer fraud policies often require a specific "transfer." Two courts have focused on this issue. In one case, the court found that the transfer need not be "physical."¹⁴ In the other case, the court found that the transfer must take place from inside the specified premises.¹⁵

Finally, a court recently addressed whether coverage can be subject to policyholders following "best practices." An insurer sought a declaratory judgment of no coverage based upon an exclusion for "failure to follow minimum required practices."¹⁶ The case was dismissed on procedural grounds. But, we will surely see more of the "best practices" issue.

Does the Policy Bar Coverage Because of This Person's Intent?

Crime involves bad intent. So, courts have been faced with questions concerning whether intentional act exclusions apply to claims arising from wrongdoing with computers.¹⁷

Courts seem willing to enforce intentional act exclusions in claims

arising from computer crime.¹⁸ But questions of intent inevitably lead to questions of perspective: from whose perspective is intent considered?

This question arose in *Lambrecht & Associates, Inc. v. State Farm Lloyds*.¹⁹ The policy covered "accidental direct physical loss." The insured's business was disrupted by a hacker. The hacker surely acted intentionally. The court found that although the injury was intended by the hacker, the injury was not intended by the policyholder. The incident needed to be considered from the policyholder's perspective. Thus, the incident was covered.

Also, intentional act exclusions require substantial evidence. In *Eye-blasters, Inc. v. Federal Insurance Co.*,²⁰ the policyholder was accused of maintaining an Internet-based advertising program that disrupted users' computers. The insurer invoked the intentional act exclusion. The Eighth Circuit found for the policyholder. It held that the insurer needed to submit evidence specifically showing that the acts were intentionally wrongful.

Does the Policy Cover This Injury?

Another dispute concerns whether the policy covers the *injury*. This question has often concerned whether the injuries are within the definition of "property damage." More specifically, the issue concerns whether data is "physical" or "tangible." Now, most commercial general liability (CGL) policies specifically exclude data.²¹ But, these decisions are still worth reviewing.

Even though digital data differs from our view of "physical," policyholders have often succeeded in arguing that data is "physical." Several policyholders established physical damage by tying data to hardware.²² Courts adopting this argument have focused on the computer itself to find something physical.

In *Lambrecht*,²³ the insurer argued that loss of information was not "physical" because it did not exist in a physical form. But, the court found that it was "physical" because it affected the server and the server had a hard drive that could not be used.²⁴

Not all courts focus on the hardware. Some focus on the data. In *Landmark American Insurance Co. v. Gulf Coast Analytical Laboratories, Inc.*, the court found that electronic data "has physical existence, takes up space on the tape, disc, or hard drive, makes physical things happen, and can be perceived by the senses."²⁵

In *State Auto Property & Casualty Insurance Co. v. Midwest Comput-*

does publication require something more?

Again, courts disagree. At least one court found that the acquiring of information is not in itself a publication.²⁹ But in *Netscape Communications Corp. v. Federal Insurance Co.*, the Ninth Circuit interpreted a policy that required "making known" the information (as opposed to "publication") and held that intercepting and internally disseminating messages is "making known" the information.³⁰ The policyholder also convinced the court that breaches in seclusion are invasions of privacy within the meaning of personal injury.³¹

Many cybercrime cases focus on whether the policy applies to the act that caused the injury.

ers & More, the court reached the opposite conclusion: "[C]omputer data cannot be touched, held, or sensed by the human mind; it has no physical substance. It is not tangible property."²⁶

Landmark is very favorable to policyholders, but whether it will gain broad acceptance is uncertain. It was rational for the court to consider physicality as being "perceived by the senses." In fact, the dictionary defines "physical" as "existing in a form that you can touch or see."²⁷ But, you cannot "touch or see" digital data. The data focus should have favored the insurer, but the policyholder still won.²⁸

Another subissue on injury is whether it is "personal injury" within the meaning of the policy. Liability policies often define this term to include the "publication" of material. In the computer crime context, "publication" is complicated. Is there publication once the thief acquires the information, or

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.³² Policyholders, on the other hand, argue for a proximate cause approach.

In *Retail Ventures, Inc. v. National Union Fire Insurance Co. of Pittsburgh, PA*,³³ 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 Sixth Circuit found the losses resulted directly from computers.

Similarly, in *Apache Corp. v. Great American Insurance Co.*,³⁴ a federal district court held that a computer fraud policy covered wire transfers to a phony account because a fraudulent e-mail 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 e-mail. 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 "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."³⁵

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, Inc. v. Hartford Casualty Insurance Co.*,³⁶ the court held that "direct" means "without any intervening cause." In *Brightpoint, Inc. v. Zurich American Insurance Co.*, the court cited *Black's Law Dictionary* to state that "direct" means "in a straight line or course" and "immediately."³⁷ In *Pestmaster*, the court stated that "direct means direct," and held that losses must "flow immediately and

Computer fraud coverage requires more than a criminal using a computer.

directly" from computer use.³⁸

The court in *Metro Brokers, Inc. v. Transportation Insurance Co.*³⁹ adopted a different, broader view of causation, but this view was grounded on policy language. Thieves used a computer virus to steal a bank password. Then, the thieves stole money. A dispute arose as to whether a virus exclusion applied. The policyholder argued that the exclusion did not apply because the virus did not, in itself, steal money. Humans needed to act after the virus. The key here was the causation language in the exclusion. The exclusion applied to any loss that a virus "caused directly or indirectly." "Indirectly" relaxed the causation requirement. What's more, the exclusion relaxed causation further by stating that it applied "regardless of any other cause or event that contributes concurrently or in any sequence to the loss."⁴⁰ So, *Metro Brokers* took a relaxed view of causation, but that view interpreted an exclusion, not the grant of coverage in computer fraud policies, and the exclusion language supported the relaxed view.

Insurers won two other causation cases, but both cases show that computer fraud coverage requires more than a criminal using a computer; the criminal must use the computer to cause the fraud. In *Great American Insurance Co. v. AFS/IBEX Financial Services, Inc.*,⁴¹ the court held that even though a person filing false applications used a computer, the loss was not a direct result of the computer use. Similarly, in *Methodist Health System Foundation, Inc. v. Hartford Fire Insurance Co.*, the court rejected a claim by an investor in a fund that invested with Bernard Madoff; the investment was "too many steps removed from Madoff's fraud."⁴²

Conclusion

Because relatively few cases have addressed insurance coverage for criminal conduct, it is too soon to draw firm conclusions. But the five issues discussed here seem likely to reoccur. The coverage disputes may extend to other issues. In fact, the cases concerning cybercrime do address a few other issues. Some of these issues are specific to computers.⁴³ Other coverage cases involving cybercrime seem to hinge on insurance issues that are not specific to computers.⁴⁴ Ultimately, because these claims are brought under specifically tailored policy provisions, we will continue to see factually intensive coverage disputes. ■

Notes

1. SYMANTEC CORP., INTERNET SECURITY THREAT REPORT 2014, at 5 (2014).

2. ROBERT P. HARTWIG & CLAIRE WILKINSON, INS. INFO. INST., CYBER RISK: THREAT AND OPPORTUNITY 3 (2015).

3. No. 11C3994, 2011 U.S. Dist. LEXIS 118906 (N.D. Ill. Oct. 14, 2011); see also *Palm Hills Props., L.L.C. v. Cont'l Ins. Co.*, No. 07-668-RET-SCR, 2008 WL 4303817 (M.D. La. July 23, 2008) (applying employee exclusion to bar coverage).

4. 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 Servs., Inc. v. Hartford*, 62 F. App'x 511 (4th Cir. 2003) (applying "acts of destruction" exception to exclusion where bad actor was an employee).

5. 136 F.3d 71 (1st Cir. 1998).

6. 752 N.W.2d 396 (Wis. Ct. App. 2008).

7. 37 N.E.3d 78 (N.Y. 2015).

8. No. A-4124-03T2, 2005 N.J. Super. Unpub. LEXIS 798 (Dec. 2, 2005).

9. No. CV-13-5039-JFW(MRWx),

2014 U.S. Dist. LEXIS 108416 (C.D. Cal. July 17, 2014).

10. 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.

11. *Hack Definition*, MERRIAM-WEBSTER.COM, www.merriam-webster.com/dictionary/hack (last visited May 4, 2016).

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

13. *Travelers Prop. Cas. Co. of Am. v. Fed. Recovery Servs., Inc.*, 103 F. Supp. 3d 1297 (D. Utah 2015).

14. *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, No. 11-6187, 2012 U.S. Dist. LEXIS 44401 (D.N.J. Mar. 28, 2012).

15. *Brightpoint, Inc. v. Zurich Am. Ins. Co.*, No. 1:04-cv-2085-SEB-JPG, 2006 U.S. Dist. LEXIS 26018 (S.D. Ind. Mar. 10, 2006) (holding that fraudulent transfers were not covered because transfer did not move property from inside the premises to outside of those premises).

16. *Columbia Cas. Co. v. Cottage Health Sys.*, No. 2:15-cv-03432, 2015 U.S. Dist. LEXIS 93456 (C.D. Cal. July 17, 2015).

17. Many courts have held that "lack of intentionality" is an implicit part of insurance contracts. See, e.g., *K&L Homes, Inc. v. Am. Family Mut. Ins. Co.*,

829 N.W.2d 724, 734 (N.D. 2013).

18. See, e.g., *i-Frontier v. Gulf Underwriters Ins. Co.*, No. 04-5797, 2005 U.S. Dist. LEXIS 19149 (E.D. Pa. June 3, 2005) (applying exclusion for “any act, error, or omission intentionally committed while knowing it was wrongful” in policy covering cyberspace activities, where employee used computer to steal manual); *Compaq Computer Corp. v. St. Paul Fire & Marine Ins. Co.*, No. C3-02-2222, 2003 Minn. App. LEXIS 1078, at *16 (Sept. 2, 2003) (applying exclusion for “intentionally wrongful acts” where policyholder was accused of intentionally and knowingly selling defective computer drives).

19. 119 S.W.3d 16 (Tex. App. 2003).

20. 613 F.3d 797 (8th Cir. 2010).

21. See, e.g., *Liberty Corporate Capital Ltd. v. Sec. Safe Outlet, Inc.*, 937 F. Supp. 2d 891 (E.D. Ky. 2013), *aff’d*, 577 F. App’x 399 (6th Cir. 2014).

22. See, e.g., *Eyeblaster*, 613 F.3d at 802 (holding that a frozen computer constituted a loss of use of tangible property); *Vonage Holdings Corp. v. Hartford Fire Ins. Co.*, No. 11-6187, 2012 U.S. Dist. LEXIS 44401, at *9 (D.N.J. Mar. 28, 2012) (finding an insured loss by focusing on the lost ability to use full capacity servers).

23. 119 S.W.3d 16.

24. Outside of the crime context, courts have reached different conclusions about whether data is tangible. For example, in *Am. Online, Inc. v. St. Paul Mercury Ins. Co.*, 347 F.3d 89, 95 (4th Cir. 2003), the court held that lost data is not “physical damage to tangible property,” but that “if a hard drive were physically scarred or scratched so that it could no longer properly record data . . . then the damage would be physical.” On the other hand, another court found that “‘physical damage’ is not restricted to the physical destruction or harm of computer circuitry but includes loss of access, loss of use, and loss of functionality.” *Am. Guar. & Liab. Ins. Co. v. Ingram Micro, Inc.*, No. 99-185, 2000 U.S. Dist. LEXIS 7299, at *6 (D. Ariz. Apr. 18, 2000).

25. No. 10-809, 2012 U.S. Dist. LEXIS 45184, at *9–10 (M.D. La. Mar. 26, 2012) (emphasis added).

26. 147 F. Supp. 2d 1113, 1116 (W.D. Okla. 2001).

27. *Physical Definition*, MERRIAM-WEBSTER.COM, www.merriam-webster.com/dictionary/physical (last visited May 4, 2016).

28. An insurer prevailed on a related issue in *Carlson Co. v. Delaget, LLC*, No. 11-cv-477-JPS, 2012 U.S. Dist. LEXIS 70836 (W.D. Wis. May 21, 2012). There, the policyholder was sued for negligence in safeguarding a bank passcode. The court held that money is not “tangible property.”

29. *Recall Total Info. Mgmt., Inc. v. Fed. Ins. Co.*, 83 A.3d 664 (Conn. App. Ct. 2014), *aff’d*, 115 A.3d 458 (Conn. 2015); see also *Zurich Am. Ins. Co. v. Sony Corp. of Am.*, No. 651982/2011, 2014 N.Y. Misc. LEXIS 5141 (Sup. Ct. Feb. 21, 2014) (finding that theft of data was a publication but that coverage did not apply to publication by someone other than the policyholder).

30. 343 F. App’x 271, 272 (9th Cir. 2009); see also *Tamm v. Hartford Fire Ins. Co.*, 16 Mass. L. Rep. 535 (Super. Ct. 2003) (finding that e-mail to outside counsel constituted publication).

31. *Netscape Commc’ns*, 343 F. App’x at 272. Beyond the cases concerning “physical” and “personal injury,” a few injury cases address issues related to characterizing an injury. See, e.g., *Retail Ventures, Inc. v. Nat’l Union Fire Ins. Co. of Pittsburgh, PA*, 691 F.3d 821 (6th Cir. 2012) (rejecting an insurer’s effort to treat credit card information as “trade secrets,” thereby applying a trade secrets exclusion); *Royal Am. Grp., Inc. v. ITT Hartford*, No. 16246, 1994 Ohio App. LEXIS 104 (Jan. 12, 1994) (rejecting a policyholder’s effort to treat long distance telephone services as “securities,” and finding that these services were not “covered property”—a term defined to include “securities”).

32. See, e.g., *Retail Ventures*, 691 F.3d at 824.

33. 691 F.3d 821.

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

35. *Id.* at *6–7. The case is currently on appeal before the Fifth Circuit. 36. No. C10-1126-RSM, 2011 U.S. Dist.

LEXIS 128203 (W.D. Wash. Nov. 4, 2011).

37. No. 1:04-cv-2085-SEB-JPG, 2006 U.S. Dist. LEXIS 26018, at *20 (S.D. Ind. Mar. 10, 2006).

38. *Pestmaster Servs., Inc. v. Travelers Cas. & Sur. Co. of Am.*, No. CV-13-5039-JFW(MRWx), 2014 U.S. Dist. LEXIS 108416, at *23–24 (C.D. Cal. July 17, 2014) (finding that computer was merely incidental to misuse of funds where fraud occurred after an authorized electronic transfer).

39. No. 1:12-cv-3010-ODE, 2013 U.S. Dist. LEXIS 184638 (N.D. Ga. Nov. 21, 2013), *aff’d*, 603 F. App’x 833 (11th Cir. 2015).

40. *Id.* at *18.

41. No. 3:07-cv-924-O, 2008 U.S. Dist. LEXIS 55532 (N.D. Tex. July 21, 2008).

42. 834 F. Supp. 2d 493, 496–97 (E.D. La. 2011).

43. See, e.g., *Eyeblaster, Inc. v. Fed. Ins. Co.*, 613 F.3d 797 (8th Cir. 2010) (applying intellectual property exclusion); *Nationwide Ins. Co. v. Hentz*, No. 11-cv-618-JPG-PMF, 2012 U.S. Dist. LEXIS 29181 (S.D. Ill. Mar. 6, 2012) (applying care and custody exclusion to stolen laptop), *aff’d*, 704 F.3d 522 (7th Cir. 2013); *Hewlett-Packard Co. v. Factory Mut. Ins. Co.*, No. 04 Civ. 2791, 2007 U.S. Dist. LEXIS 24146 (S.D.N.Y. Mar. 30, 2007) (excusing delay caused by a sabotaged investigation); *i-Frontier, Inc. v. Gulf Underwriters Ins. Co.*, No. 04-5797, 2005 U.S. Dist. LEXIS 19149 (E.D. Pa. June 3, 2005) (noting but not interpreting the meaning of “cyberspace”).

44. See, e.g., *Freedom Banc Mortg. Servs., Inc. v. Cincinnati Ins. Co.*, No. 13AP-400, 2014 Ohio App. LEXIS 204 (Jan. 23, 2014) (addressing time limit on suit); *Pollak v. Fed. Ins. Co.*, No. 13-12114-FDS, 2013 U.S. Dist. LEXIS 165650 (D. Mass. Nov. 21, 2013) (determining that the plaintiff was not the “intended beneficiary”); *Saint Consulting Grp., Inc. v. Endurance Am. Specialty Ins. Co.*, No. 11-11279-GAO, 2012 U.S. Dist. LEXIS 45474 (D. Mass. Mar. 30, 2012) (applying exclusion for statutory violations), *aff’d*, 699 F.3d 544 (1st Cir. 2012).