RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY

Justin D. Wear, Robert Flowers, Kyle D. Black, Lauren D. Godfrey, and Roberta D. Anderson

This survey reviews recent regulatory developments and court decisions addressing cybersecurity issues from October 1, 2016, through September 30, 2017. The first part will discuss statutory and regulatory developments particularly related to breach notification. The second part will discuss standing to sue under Article III, section 2 of the U.S. Constitution, in light of the U.S. Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins.*

Justin D. Wear (jwear@manierherod.com) is a partner with Manier & Herod in Nashville. Robert Flowers (rflowers@travelers.com) is with The Travelers Companies in Hartford. Kyle D. Black (kyle.black@lewisbrisbois.com) is an associate in the Pittsburgh office of Lewis Brisbois. Roberta D. Anderson (randerson@cohenlaw.com) is a director in the Pittsburgh office of Cohen & Grigsby, P.C. Lauren D. Godfrey (lauren.godfrey@lewisbrisbois.com) is a partner in the Pittsburgh office of Lewis Brisbois.

Finally, the third part will discuss notable cases involving fraud-related cybercrimes.

I. STATUTORY AND REGULATORY BREACH NOTIFICATION DEVELOPMENTS

Data breach notification requirements received particular attention in 2017. Following the massive Equifax breach, which exposed names, Social Security numbers, and other private information on more than 145 million people, legislators across the country, as well as the general public as a whole, have become more cognizant of the need for and enforcement of breach notification. Below are the statutory and regulatory breach notification requirements that were recently passed across the country.

A. *Arkansas*

Arkansas enacted the State Insurance Department General Omnibus Bill on March 1, 2017.[1] Effective July 31, 2017, the bill amended Arkansas Code § 23-61-113, which governs certain regulated entities' disclosure of nonpublic personal information. Specifically, the state Insurance Commissioner adopts "rules governing the treatment of consumer financial and protected health information . . . by all licensed insurers, health maintenance organizations, or other insuring health entities" regulated by the Insurance Commissioner.[2] The amendment now adds that these regulated entities include "legal entities engaged in the business of insurance. . . ."[3] Furthermore, these regulated entities are also required to notify the Insurance Commissioner of a data breach.[4] Notice to the Insurance Commissioner must be "in the same time and manner as required" under Arkansas' breach notification statutes.[5] In other words, notice to the Insurance Commissioner must be in the most expedient time and manner possible and without unreasonable delay.[6]

B. *New York*

New York enacted a new regulation from the New York Department of Financial Services that adds a new breach notification requirement for financial service institutions on March 1, 2017.[7] In the event of a data breach, businesses are already generally required to notify the New York Attorney General, the New York Department of State, the New York State Police,

1. S.B. 247, 91st Gen. Assemb., Reg. Sess. (Ark. 2017); also known as Act 283.
2. ARK. CODE § 23-61-113(b)(1).
3. *Id.* § 23-61-113(b)(2)(A).
4. *Id.* § 23-61-113(b)(2)(A)(i)–(ii).
5. *Id.*
6. *See* Arkansas Personal Information Protection Act, ARK. CODE § 4-110-105(2).
7. *See* N.Y. COMP. CODES R. & REGS. tit. 23, § 500.

and the affected New York residents.[8] Now, under the new regulation, entities licensed under New York's Banking Law, Insurance Law, or Financial Services Law will also be required to notify the Department of Financial Services' Superintendent of Financial Services.

C. *Virginia*

On March 13, 2017, Virginia enacted House Bill 2113. Effective July 1, 2017, the bill amends Virginia Code § 18.2-186.6, which governs notification requirements for breach of payroll data. The amendment imposes special regulatory notification requirements on employers and payroll service providers when tax information is affected.[9] An employer or payroll service provider must now notify the Virginia Attorney General after discovering a breach of computerized data containing a resident's taxpayer identification number (TIN), combined with income tax withheld from that resident.[10] An employer or payroll service provider must notify the Virginia Attorney General without unreasonable delay.[11] In its notification to the Virginia Attorney General, the employer or payroll service provider must include the name and TIN of the affected residents as well as the employer's name and federal employer identification number.[12] However, notification to the attorney general is not required when the employer or payroll service provider reasonably believes that the breach has not and will not cause identity theft or some other fraud.[13] For an employer, the amendment applies only to information concerning its employees.[14]

D. *Utah*

On March 23, 2017, Utah enacted Senate Bill 99, which became effective on May 9, 2017, amending Utah Code §§ 13-44-301 and 13-45-401. The amendments expand the ability of the Utah Attorney General to enforce Utah's Protection of Personal Information Act. Specifically, the attorney general may now enter into a confidentiality agreement with an individual to obtain information if there is reasonable cause to believe the individual has information relevant to enforcing Utah's breach notification law.[15] Likewise, a court may issue a similar confidentiality order in a civil suit brought under the statute.[16]

8. *See* N.Y. Gen. Bus. Law § 899-aa.
9. Va. Code § 18.2-186.6(M).
10. *Id.* § 18.2-186.6(M).
11. *Id.* § 18.2-186.6(M).
12. *Id.* § 18.2-186.6(M).
13. *Id.* § 18.2-186.6(M).
14. *Id.* § 18.2-186.6(M).
15. Utah Code §§ 13-44-301(7)(a); 13-45-401(5)(a).
16. *Id.* §§ 13-44-301(7)(b); 13-45-401(5)(b).

The attorney general may also use any testimony, documents, or materials obtained by a confidentiality agreement or order in an enforcement action taken under the statute.[17] The amendments also compel the attorney general to keep all procedures, testimony, documents, or materials produced by a confidentiality notice or order confidential unless the individual at issue waives confidentiality.[18] The attorney general may disclose materials obtained via a confidentiality agreement or order with a grand jury, or with a federal or state law enforcement officer, if the individual from whom the information is obtained is notified at least twenty days before disclosure, and the law enforcement officer certifies that he or she will keep the material confidential and use it only for law enforcement purposes.[19] The amendments also permit the attorney general to seek attorney fees and costs associated with enforcing the statute.[20]

E. *Tennessee*

On April 4, 2017, Tennessee enacted Senate Bill 457, which amended Tennessee Code § 47-18-2107, Tennessee's breach notification statute. The amendment makes clear that entities are no longer required to give personal notification of a data breach if the data was encrypted. Specifically, the amendment now defines a "breach of system security" as the acquisition of "unencrypted computerized data; or encrypted computerized data and the encryption key."[21] The amendment further defines "encrypted" as "computerized data that is rendered unusable, unreadable, or indecipherable without the use of a decryption process or key and in accordance with the current version of the Federal Information Processing Standard (FIPS) 140-2."[22] In other words, entities will not need to give notice of a breach of encrypted data as long as the encryption key is not compromised.

Furthermore, the amendment extends Tennessee's forty-five-day time limit for providing notice after a data breach has been discovered. According to the amendment, if "the legitimate needs of law enforcement" require an extension, an additional forty-five days may be taken for supplying notification.[23]

F. *New Mexico*

New Mexico enacted its own Data Breach Notification Act on April 16, 2017, thereby becoming the forty-eighth state to require notification to

17. *Id.* §§ 13-44-301(11); 13-45-401(6).
18. *Id.* §§ 13-44-301(11)(a); 13-45-401(6)(a).
19. *Id.* §§ 13-44-301(11)(d); 13-45-401(6)(d).
20. *Id.* §§ 13-44-301(4)(a); 13-45-401(3)(a).
21. Tenn. Code Ann. § 47-18-2107(a)(1)(A).
22. *Id.* § 47-18-2107(a)(2).
23. *Id.* § 47-18-2107(d).

consumers following a data breach.[24] The Data Breach Notification Act bears similarities to many other state breach notification statutes. For example, like most state breach notification statutes, New Mexico only covers electronic data that contains personal information.[25] New Mexico also requires consumer notification to be made within forty-five days after discovery of a breach.[26] An entity must also notify the New Mexico Attorney General if more than 1,000 residents have to be notified of a breach.[27] Importantly, an entity must also notify the New Mexico Attorney General if it provides notification to residents via substitute notice, regardless of the number of residents notified.[28] However, "notification to affected New Mexico residents is not required if, after an appropriate investigation, the person determines that the security breach does not give rise to a significant risk of identity theft or fraud."[29]

G. *Maryland*

On May 4, 2017, Maryland enacted House Bill 974, which takes effect on June 1, 2018.[30] The bill makes several changes to Maryland's Personal Information Protection Act. Most notably, the bill expands the definition of "personal information" to include, when combined with an individual's first name or first initial and last name: (1) a passport number, or other identification number issued by the federal government; (2) a state identification card number; (3) health information, including information about an individual's mental health; (4) a health insurance policy or certificate number, or health insurance subscriber identification number, in combination with a unique identifier that permits access to an individual's health information; and (5) biometric data that can be used to uniquely authenticate an individual's identity when accessing a system or account.[31]

The amendment also adds an individual's username or email address in combination with a password or security question and answer permitting access to the individual's email account to the definition of "personal information." Unlike the other "personal information" mentioned above, a username or email address does not need to be linked to an individual's name to qualify as "personal information." If only a username or email address (and password or security question permitting access to the compromised email account) and no other personal information is affected, however, an entity can notify affected individuals by providing directions on

24. 2017 New Mexico House Bill No. 15.
25. *Id.* § 2(C).
26. *Id.* § 6(A).
27. *Id.* § 10.
28. *Id.*
29. *Id.* § 6(C).
30. 2017 Maryland House Bill No. 974.
31. *Id.*

how to change the account's password or security question and answer, or providing additional steps to protect the compromised email account.[32]

An entity must provide notice to affected Maryland residents of a data breach within forty-five days of discovery. If notification is subject to a law enforcement delay under the statute, notice to affected residents must be no later than thirty days after the law enforcement agency determines notification will not impede a criminal investigation, or will not jeopardize homeland or national security.

The amendment further revised the statute's definition of "encryption" to mean the protection of data using an encryption technology that renders it indecipherable without an associated encryption key.[33]

H. *Washington*

Washington State enacted Substitute House Bill 1717, which amended Washington's breach notification statute for state agencies, on May 16, 2017.[34] The amendment particularly imposes restrictions on state agencies' ability to collect and otherwise use an individual's "biometric identifiers." First, the amendment notably points out that "[a]dvances in technology have given rise to new forms of data. . . . One new form of personally identifiable information is biometric identifiers. The unique nature of this new type of personal data calls for additional guidance regarding its use by state agencies."[35] The amendment defines "biometric identifiers" as "any information . . . based on an individual's retina or iris scan, fingerprint, voiceprint, or scan of the hand or face geometry," subject to certain exceptions.[36]

Pursuant to the amendment, an agency may not "collect, capture, purchase, or otherwise obtain a biometric identifier" without first notifying and obtaining an individual's consent.[37] The notice must clearly specify the purpose and use of the individual's biometric identifier, and the consent must be specific to the notice's terms and maintained by the agency for as long as it retains the individual's biometric identifier.[38] Furthermore, the amendment prohibits an agency from selling an individual's biometric identifier and limits its use to the terms of the notice and consent.[39] The agency must, among other things, establish security policies to protect the integrity and confidentiality of biometric identifiers it ob-

32. *Id.*
33. *Id.*
34. *See* WASH. REV. CODE § 42.56.590.
35. Substitute H.B. 1717 § 1.
36. *Id.* § 2(7)(b).
37. *Id.* § 2(1).
38. *Id.* § 2(1)(a).
39. *Id.* § 2(2)(a)–(b).

tains.[40] The agency must also address biometric identifiers in its privacy policy, adhere to records retention requirements, and minimize the amount of biometric identifiers to that necessary to fulfill the notice and consent obtained from the individual.[41]

I. *Delaware*

Delaware enacted House Bill 180 on August 17, 2017.[42] Effective April 18, 2018, the bill makes several significant revisions to Delaware's breach notification statute. The bill will require that entities that conduct business in Delaware and own, license, or maintain personal information must now implement and maintain "reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business." The bill will also expand the definition of "personal information" to include, when combined with an individual's first name or first initial and last name: (1) passport number; (2) taxpayer identification number (TIN); (3) state or federal identification card numbers; (3) a username or email address, when combined with a password or security question and answer permitting access to an online account; (4) medical history, DNA profile, medical treatment, or medical treatment or diagnosis by a health care professional; (5) health insurance policy numbers; (6) other health insurance identifiers; or (7) unique biometric data.

The bill further redefines when a breach is discovered. The revised law states that "determination of the breach of security" means the point in time when an entity that owns, licenses, or maintains computerized data "has sufficient evidence to conclude that a breach of security of such computerized data has taken place."

The bill now requires entities to provide notice to affected Delaware residents within sixty days of determining a breach occurred. The bill also contains a provision that accounts for the fact that an entity may not be able to, through reasonable diligence, identify all affected state residents within the sixty-day notification timeline. If more affected residents are found, the entity has to notify those newly discovered residents "as soon as practicable" after determining they too were affected, unless the entity has already provided substitute notice.

Under the revised law, breach notification can now be made electronically if the entity's "primary means of communication with the resident is by electronic means." Furthermore, under the amended statute, entities must notify the Delaware Attorney General if more than five hundred res-

40. *Id.* § 2(3)(a).
41. *Id.* § 2(3)(b), (d), (f).
42. 2017 Delaware House Bill No. 180.

idents are notified. Moreover, the notification to the attorney general must be made no later than when state residents are notified. However, the bill further adds that notification is not required if, after an appropriate investigation, the entity reasonably determines the breach "is unlikely to result in harm" to the affected residents.

An entity is also required under the revised Delaware statute to provide one year's worth of credit monitoring services at no cost to state residents when Social Security numbers are reasonably believed to have been breached.

II. STANDING

Recent decisions from around the country show how courts are grappling with whether an individual has "standing" to assert cybersecurity claims. By way of background, standing "is a threshold jurisdictional question" that ensures a suit is "appropriate for the exercise of the [federal] courts" judicial powers.[43] The United States' standing requirement stems from Article III, section 2 of the U.S. Constitution, which provides that the "judicial Power shall extend to all Cases [and] Controversies."[44] In other words, a federal court's jurisdiction is limited to actual cases or controversies.[45] In order to determine whether a party has standing, the party invoking federal jurisdiction must show that the party "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision."[46]

In pertinent part, in order to establish an injury-in-fact, "a plaintiff must show that he or she suffered 'an invasion of a legally protected interest' that is 'concrete and particularized.'"[47] In 2016, the Supreme Court elaborated more on the "concreteness" requirement. The Court in *Spokeo, Inc. v. Robins*[48] explained that concreteness "is quite different from particularization."[49] The Court explained that a concrete injury is one that "actually exist[s]" and is "real, not an abstract."[50]

The Court clarified that "concreteness" is not necessarily synonymous with "tangible."[51] An "intangible injury" can be concrete to constitute an

43. Pye v. United States, 269 F.3d 459, 466 (4th Cir. 2011) (citing Steel Co. v. Citizens for a Better Env't, 523 U.S. 83 (1998)).
44. U.S. CONST. art. III § 2, cl. 1.
45. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
46. *Id.* at 1547 (citing Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992)).
47. *Id.* at 1548 (quoting *Lujan*, 504 U.S. at 560).
48. *Id.* at 1548 n.2.
49. *Id.* at 1548.
50. *Id.*
51. *Id.* at 1549.

injury-in-fact.[52] In order to determine whether an intangible harm constitutes an injury-in-fact, "history and the judgment of Congress play important roles."[53] The Court did note, however, that a plaintiff cannot automatically satisfy the injury-in-fact requirement just because "a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[54] That is, one cannot "allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement."[55] In other words, a technical violation of a statute may not rise to the level of an injury-in-fact for constitutional purposes.

Recent federal court cases have had the opportunity to apply *Spokeo's* elaborated standing analysis. The Fourth Circuit held that an individual does not have Article III standing when he fails to allege a concrete injury stemming from inaccurate information in a credit report. In *Dreher v. Experian Information Solutions, Inc.*,[56] the plaintiff, Michael Dreher, was undergoing a background check when he learned that his name was associated with a delinquent credit card account.[57] To address this matter, the plaintiff requested his credit report from Experian.[58] The Experian credit report listed a delinquent account under the names "Advanta Bank" or "Advanta Credit Cards."[59] The plaintiff sent letters to the Advanta address listed on the report, asking Advanta to delete the inaccurate information in the Experian credit reports.[60] After receiving no response from Advanta, he contacted Experian about the issue, but Experian's credit reports continued to show the delinquent account.[61]

Unbeknown to the plaintiff, Advanta closed during the 2008 financial crisis.[62] CardWorks Inc., and CardWorks Servicing LLC (collectively, CardWorks) was subsequently appointed as servicer of Advanta's portfolio, meaning that CardWorks was ultimately in charge of handling all Advanta credit card disputes.[63] CardWorks decided to do business using Advanta's name, phone, number and website.[64] CardWorks was also in charge of deciding

52. *Id.*
53. *Id.*
54. *Id.*
55. *Id.*
56. 856 F.3d 337 (4th Cir. 2017).
57. *Id.* at 340.
58. *Id.* The plaintiff also received credit reports from two other agencies, although it is unclear if these other agencies also listed the alleged inaccurate information.
59. *Id.*
60. *Id.*
61. *Id.* at 340–41. This process of fixing his credit report did not affect his security clearance. The Advanta account was deleted from the plaintiff's credit report two years later. The plaintiff alleged that this process caused additional stress and wasted time.
62. *Id.* at 341.
63. *Id.*
64. *Id.*

how to list Advanta accounts, or tradelines, on consumer reports.[65] CardWorks decided that all accounts on Experian credit reports would bear the Advanta name.[66]

The plaintiff filed a class action lawsuit, asserting, in pertinent part, that Experian violated 15 U.S.C. § 1681g(a)(2) of the Fair Credit Report Act (FCRA), which states that a consumer reporting agency "shall, upon request . . . clearly and accurately disclose to the consumer . . . *[t]he sources of the information* [in the consumer's file at the time of the request]."[67] The plaintiff alleged that Experian willfully violated the FCRA by failing to include the name "CardWorks" in the Advanta tradelines on its credit reports.[68] The plaintiff claimed he suffered a cognizable "informational injury" because he was denied "specific information to which [he] w[as] entitled under the FCRA."[69]

The parties eventually filed cross motions for partial summary judgment.[70] Experian argued that the plaintiff and the class members lacked Article III standing.[71] The plaintiff argued that Experian willfully violated the FCRA and that no jury could find Experian's intentional omission of CreditWorks from the credit report was objectionably reasonable.[72] The district court granted the plaintiff's motion and denied Experian's motion.[73] The district court did not analyze whether the plaintiff's alleged injury was particular and concrete.[74] Instead, the district court concluded that *any* violation of the statute sufficed to create an Article III injury-in-fact.[75]

Experian subsequently appealed, and the Fourth Circuit held the case in abeyance pending the Supreme Court's decision in *Spokeo*.[76] Following *Spokeo*, the Fourth Circuit ultimately held that "receiving a creditor's name rather than a servicer's name—without hindering the accuracy of the report or efficiency of the credit report resolution process—worked no real world harm on [the plaintiff]."[77]

The Fourth Circuit acknowledged that an "information injury" is a type of intangible injury that can constitute an Article III injury-in-fact.[78] The

65. *Id*. A tradeline is an account entry on a credit report.
66. *Id.*
67. *Id.* at 344.
68. *Id.* at 342.
69. *Id.* at 345.
70. *Id.* at 342.
71. *Id.*
72. *Id*.
73. *Id.*
74. *Id*.
75. *Id.* (emphasis added).
76. *Id*.
77. *Id.* at 346.
78. *Id.* at 345 (citing Fed. Election Comm'n v. Akins, 524 U.S. 11, 24 (1998); Pub. Citizen v. U.S. Dep't of Justice, 491 U.S. 440, 449 (1989)).

Fourth Circuit explained that a statutory violation alone does not create a concrete informational injury sufficient to support standing, however.[79] The court further explained that a constitutionally cognizable informational injury requires that a person lack access to information to which he is legally entitled *and* that the denial of that information creates a "real" harm with an adverse affect.[80]

To determine whether the plaintiff suffered a "real harm" with adverse effect, the Fourth Circuit examined whether the plaintiff's alleged intangible injury has been similarly protected under common law, or if the intangible injury has been expressly identified by Congress.[81] Neither the plaintiff nor the court could identify any similar interest that has traditionally served as a basis for lawsuit.[82]

The Fourth Circuit further explained that in enacting the FCRA, Congress sought "to ensure fair and accurate credit reporting . . . and protect consumer privacy."[83] The court noted that the plaintiff failed to show how the knowledge that he was corresponding with a CardWorks employee, rather than an Advanta employee, would have made any difference at all in the fairness and accuracy of his credit report, or that it would have made the credit resolution process more efficient.[84] While the plaintiff essentially argued that a company should not be allowed to hide its true identity, the Fourth Circuit found that the plaintiff's argument is primarily a customer services complaint.[85] Thus, the Fourth Circuit held that the harm the plaintiff allegedly suffered is not the harm that Congress sought to prevent when it enacted the FCRA.[86]

The court concluded that the plaintiff failed to demonstrate that he suffered a concrete injury sufficient to satisfy Article III standing.[87] Thus, the Fourth Circuit vacated the district court's decision and dismissed the class action on jurisdictional grounds.[88]

The Eighth Circuit held that a plaintiff had Article III standing to assert his contract-related claims. In *Kuhns v. Scottrade, Inc.*,[89] the plaintiff, Matthew Kuhns, opened a brokerage account with Scottrade, Inc., a securities brokerage firm. When opening the account, Kuhns signed a brokerage agreement and provided Scottrade with his name, Social Security

79. *Id.* (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016)).
80. *Id.* (citing *Spokeo*, 136 S. Ct. at 1548) (emphasis added).
81. *Id.* (citing *Spokeo*, 136 S. Ct. at 1549).
82. *Id.*
83. *Id.* at 346 (quoting Safeco Ins. Co. of Am. v. Burr, 511 U.S. 47, 52 (2007)).
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.* at 347.
88. *Id.*
89. 868 F.3d 711 (8th Cir. 2017).

number, and other personal identifying information (PII).[90] The brokerage agreement provided that Kuhns agreed to pay Scottrade brokerage fees and commissions for purchases and sales of securities.[91] The agreement also stated that Scottrade would protect the PII of all of its customers by maintaining "physical, electronic and procedural safeguards that comply with federal regulations," as well as by using industry leading security technologies.[92]

In 2013, hackers accessed the internal customer database of Scottrade and extracted the PII of more than 4.6 million Scottrade customers, including Kuhns.[93] The hackers ultimately used the information to operate a stock price manipulation scheme, illegal gambling websites, and a Bitcoin exchange.[94]

Kuhns and others affected by the data breach brought a class action lawsuit against Scottrade.[95] The lawsuit asserted claims of breach of contract, breach of implied contract, and unjust enrichment due to Scottrade's deficient cybersecurity protection.[96] Kuhns particularly argued that a portion of the fees paid in connection with his Scottrade account were used to meet Scottrade's contractual obligations to provide data management and security to protect his PII.[97] When Scottrade breached those obligations, Kuhns argued he received brokerage services of lesser value.[98] Thus, Kuhns asserted that the difference between the amount he paid and the value of the services received was actual economic injury establishing injury-in-fact for his contract-related claims.[99]

Scottrade filed motions to dismiss the case for lack of subject matter jurisdiction and for failure to state a claim.[100] The district court granted the motion to dismiss for lack of subject matter jurisdiction, explaining that the plaintiffs did not have standing to bring their claims.[101] The district court did not address the motion to dismiss for failure to state a claim.[102] Kuhns appealed the district court's ruling.[103]

90. *Id.* at 714.
91. *Id.*
92. *Id.*
93. *Id.* at 714–15.
94. *Id.*
95. *Id.* at 713, 715.
96. *Id.* The plaintiffs also sought declaratory judgment and violation of the Missouri Merchandising Practices Act, MO. REV. STAT. § 407.025.
97. *Id.* at 716.
98. *Id.*
99. *Id.*
100. *Id.* at 715.
101. *Id.*
102. *Id.*
103. *Id.* None of the other plaintiffs appealed this ruling.

The Eighth Circuit affirmed the dismissal on the grounds that the plaintiffs failed to state a claim.[104] However, the court found that Kuhns had standing to bring his contract-related claims based on allegations that he did not receive the full benefit of his bargain with Scottrade.[105] The Eighth Circuit explained that "a party to a breached contract has a judicially cognizable interest for standing purposes, regardless of the merits of the breach alleged."[106] Applying this rule of law to the case, the court found that Kuhns alleged that he bargained for and expected protection of his PII; that Scottrade breached the contract when it failed to provide promised reasonable safeguards; and that Kuhns suffered actual injury in the form of the diminished value of his bargain.[107] Regardless of the merits of his contract-related claim, the court held that Kuhns had Article III standing to assert those claims.[108]

The Ninth Circuit examined the extent to which a violation of a statutory right can itself establish an injury sufficiently concrete for purposes of Article III standing upon remand in *Spokeo*. In *Robins v. Spokeo, Inc.*,[109] Spokeo, a website that compiles consumer data and publishes consumer reports on its website, allegedly published inaccurate information about Thomas Robins. In particular, Spokeo published inaccurate information about Robins' age, marital status, wealth, education level, and profession.[110] Robins sued Spokeo for willful violations of the FCRA,[111] alleging that Spokeo failed to "follow reasonable procedures to assure maximum possible accuracy" of the information in his consumer report as required by § 1681e(b).[112] Robins alleged that the inaccurate report harmed his employment prospects, that he continued to be unemployed, and as a result, suffered from emotional distress.[113]

The district court dismissed Robins' complaint, holding that Robins lacked standing to sue under Article III.[114] Specifically, the district court concluded that Robins alleged only a bare violation of the statute and did not adequately plead that such violation caused him to suffer an actual injury-in-fact.[115] The Ninth Circuit reversed and remanded, hold-

104. *Id.* at 716–19.
105. *Id.*
106. *Id.* at 716 (quoting Carlsen v. Gamestop, Inc., 833 F.3d 903, 909 (8th Cir. 2016)).
107. *Id.*
108. *Id.* (citing ABF Freight Sys., Inc. v. Int'l Bhd. of Teamsters, 645 F.3d 954, 960–61 (8th Cir. 2011)).
109. 867 F.3d 1108 (9th Cir. 2017).
110. *Id.* at 1111.
111. 15 U.S.C. §§ 1681–1681(x).
112. *Spokeo*, 867 F.3d at 1111.
113. *Id.*
114. *Id.*
115. *Id.*

ing that Robins' allegations established he suffered a sufficiently concrete and particularized injury.[116]

On certiorari, the Supreme Court vacated the Ninth Circuit's opinion, holding that its standing analysis was incomplete.[117] The Court explained that although the Ninth Circuit properly addressed whether the injury alleged was particularized to Robins, the Ninth Circuit failed to adequately address whether the injury was concrete.[118] The Court remanded the case back to the Ninth Circuit to explain whether Robins' alleged injury satisfied the concreteness requirement imposed by Article III.[119] Back in the Ninth Circuit, Robins argued that Spokeo's violation of the FCRA for failing to reasonably ensure the accuracy of his consumer report, alone, was enough to establish a concrete injury.[120]

On remand, and following the Supreme Court's guidance, the Ninth Circuit explained that a plaintiff does not automatically satisfy Article III's standing requirements whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right.[121] Instead, the court explained that Article III standing requires a concrete injury.[122] To establish a concrete injury, the plaintiff must allege a statutory violation that caused a real injury, as opposed to a purely legal or abstract harm.[123] The court noted that Congress has the power to define some abstract or intangible harm as a concrete injury sufficient to satisfy Article III's standing requirements.[124] "[A]n alleged procedural violation [of a statute] can by itself manifest concrete injury where Congress conferred the procedural right to protect a plaintiff's concrete interests and where the procedural violation presents 'a risk of real harm' to that concrete interest."[125] Thus, the court explained there are some statutory violations that do establish a concrete injury.[126]

With this in mind, to determine whether Robins satisfied Article III's concreteness requirement, the Ninth Circuit evaluated (1) whether the statutory provisions at issue were established to protect a concrete interest; and if so (2) whether the specific procedural violation alleged in this case actually harmed, or presented a material risk of harm, to such concrete interest.[127]

116. *Id.* (citing Robins v. Spokeo, Inc. (*Spokeo I*), 742 F.3d 409, 414 (9th Cir. 2014)).
117. *Id.* (citing Spokeo, Inc. v. Robins (*Spokeo II*), 136 S. Ct. 1540 (2016)).
118. *Id.*
119. *Id.*
120. *Spokeo*, 867 F.3d at 1112.
121. *Id.* (citing *Spokeo II*, 136 S. Ct. at 1549).
122. *Id.* (quoting *Spokeo II*, 136 S. Ct. at 1548–49).
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.* at 1113.

First, the court held that the FCRA provisions at issue, namely § 1681e(b), were created to protect a concrete interest.[128] The court explained that Congress created the FCRA to protect consumers' interest in fair and accurate credit reporting and to protect consumer privacy.[129] To protect this interest, FCRA requires consumer-reporting agencies to follow several procedural requirements concerning the creation and use of consumer reports.[130] In particular, § 1681e(b) requires consumer-reporting agencies to "follow reasonable procedures to assure maximum possible accuracy" of the information contained in an individual's consumer report.[131] The FCRA allows individuals to sue consumer-reporting agencies that are non-compliant with these procedural requirements.[132]

The court further explained that the dissemination of false information in consumer reports can itself constitute an actual injury.[133] The court noted that consumer reports are often used in, among other things, employment decisions, loan applications, and home purchases.[134] The threat to a consumer's livelihood is caused by the existence of inaccurate information in his credit report.[135] Thus, the Ninth Circuit explained that it makes sense that Congress might choose to protect against such harms without requiring any additional showing of injury.[136]

The Ninth Circuit further observed that the interest that FCRA protects also resembles other reputational and privacy interests that have long been protected in common law, such as defamation.[137] Thus, the court recognized that with the FCRA, Congress has chosen to protect against a harm that is similar in kind to other harms that have traditionally served as the basis for a lawsuit.[138] Accordingly, guided by Congress's judgment and historical practice, the Ninth Circuit concluded that the FCRA procedures at issue were created to protect consumers' concrete interest in accurate credit reporting.[139]

Next, the Ninth Circuit determined Robins had alleged FCRA violations that actually harmed, or created a material risk of harm to, his con-

128. *Id.*
129. *Id.* at 1113 (citing Safeco Ins. Co. of Am. v. Burr, 551 U.S. 47, 52 (2007)).
130. *Id.*
131. *Id.* at 1114 (citing 15 U.S.C. § 1681e(b)).
132. *Id.* at 1113–14 (quoting *Spokeo II*, 136 S. Ct. at 1545)).
133. *Id.* at 1114 (citing *Spokeo II*, 136 S. Ct. at 1550)).
134. *Id.*
135. *Id.*
136. *Id.*
137. *Id.* at 1114–15.
138. *Id.* at 1115; *see also In re* Horizon Healthcare Inc. Data Breach Litig., 846 F.3d 625, 638–40 (3d Cir. 2017) (comparing FCRA's privacy protections to common law protection for "a person's right to prevent the dissemination of private information").
139. *Spokeo*, 867 at 1115.

crete interest.[140] The court first noted that a mere procedural violation of the statute alone is not enough to show an actual harm or material risk of harm.[141] In particular, the mere failure to "follow reasonable procedures to assure maximum possible accuracy" of consumer reports may not result in the creation or dissemination of an inaccurate consumer report.[142] The court noted that Robins must allege more than a bare procedural violation of the statute.[143]

The court recognized that Robins alleged more than a mere procedural violation. Robins alleged that Spokeo not only prepared a consumer report with inaccurate information, but also published the report on the Internet.[144] Thus, the court held that Robins' allegations clearly implicate his concrete interest in truthful credit reporting.[145]

The court rejected Robins' argument that any FCRA violation premised on *some* inaccurate disclosure of his information is sufficient to show an actual harm.[146] The Supreme Court explicitly rejected the notion that every minor inaccuracy reported in violation of FCRA will cause actual harm or present a material risk of actual harm.[147] For example, an inaccurately reported zip code, without more, most likely would not create any actual harm or material risk of actual harm.[148] The Supreme Court required some examination of the nature of the specific alleged reporting inaccuracies in order to determine if there is a real risk of harm to the concrete interest that the FCRA protects.[149]

Besides inaccurate zip codes, the Supreme Court gave little guidance on what information would be considered harmless if inaccurately reported.[150] However, in this case, the Ninth Circuit noted that the misinformation of Robins' age, marital status, and educational background were substantially more likely to harm Robins' concrete interest than an incorrect zip code.[151] Spokeo inaccurately reported that Robins was married with children, that he was in his 50s, that he had a graduate degree, and that his wealth level was higher that it really was.[152] Although the

140. *Id.*
141. *Id.*
142. *Id.* (citing *Spokeo II*, 136 S. Ct. at 1550)).
143. *Id.*
144. *Id.*
145. *Id.* at 1116 (citing *Spokeo II*, 136 S. Ct. at 1553–54 (Thomas, J., concurring) (unlike other FCRA procedural requirements, Section 1681e(b) potentially creates a private duty to protect an individual's personal information).
146. *Id.*
147. *Id.* (citing *Spokeo II*, 136 S. Ct. at 1550).
148. *Id.*
149. *Id.*
150. *Id.* at 1116–17.
151. *Id.* at 1117.
152. *Id.*

Ninth Circuit acknowledged that the alleged misinformation could seem worse, the court agreed that this type of information is the type that may be important to employers or others making use of a consumer report.[153] Thus, the Ninth Circuit concluded that the alleged FCRA violations actually harmed, or at least that actually created a material risk of harm, to Robins' concrete interest.[154]

Last, the Ninth Circuit rejected Spokeo's argument that Robins' allegations of harm were too speculative to establish a concrete injury.[155] Spokeo relied on *Clapper v. Amnesty International USA*[156] to argue that Robins failed to demonstrate how the published inaccurate information would expose him to a "certainly impending" injury.[157] Spokeo argued that Robins merely asserted that such inaccuracies *might* hurt his employment prospects, but not that the inaccuracies presented a material or impending risk of doing so.[158]

However, the Ninth Circuit explained that Spokeo's reliance on *Clapper* was misplaced because *Clapper* did not address the concreteness of an intangible injury such as the one Robins asserts.[159] In *Clapper*, the plaintiffs believed that some of the people with whom they exchanged information were likely targets of surveillance under a federal statute.[160] The plaintiffs sought to strike down the statute authorizing the surveillance in order to remove the threat that their communications would eventually be intercepted.[161] In other words, the plaintiffs sought to establish standing on the basis of harm they would supposedly suffer from threatened conduct that had not yet happened.[162]

Thus, the Supreme Court in that case addressed what must be shown to establish standing based on anticipated conduct or anticipated injury.[163] Unlike *Clapper*, where the challenged conduct and alleged injury had not yet occurred, in this case, Spokeo's conduct and Robins' alleged injury had already occurred.[164] Namely, Spokeo already published the in-

153. *Id.* The court further noted that the Consumer Financial Protection Bureau has argued that even seemingly flattering inaccuracies can hurt an individual's employment prospects because such inaccuracies may cause a prospective employer to question the applicant's truthfulness or suggest that he or she is overqualified.

154. *Id.*

155. *Id.*

156. 133 S. Ct. 1138 (2013).

157. *Spokeo*, 867 F.3d at 1117.

158. *Id.*

159. *Id.* at 1118.

160. *Id.* (citing *Clapper*, 133 S. Ct. at 1145) (emphasis added).

161. *Id.* (citing *Clapper*, 133 S. Ct. at 1145–46).

162. *Id.*

163. *Id.* (citing *Clapper*, 133 S. Ct. at 1147–48). The Supreme Court explained that a plaintiff cannot show injury-in-fact unless the "threatened injury [is] *certainly impending*" as opposed to merely speculative.

164. *Id.*

accurate information, and Robins already allegedly suffered harm to his employment prospects due to the inaccurate report.[165] Thus, the Ninth Circuit held that *Clapper* was not controlling.[166] Ultimately, the Ninth Circuit concluded that Robins' alleged injuries were sufficiently concrete to establish standing under Article III.[167]

III. CYBERCRIMES

More and more insurance policies are including "computer fraud" provisions, which generally cover losses arising from fraud conducted through a computer. Coverage for losses from computer fraud may be unpredictable, however, if the fraud is performed in conjunction with social engineering fraud; that is, fraud generally conducted by enlisting the trust of its victims to voluntarily disclose information or perform the fraudulent transaction. Recent decisions have analyzed these computer-fraud provisions in the context of policyholders who are victimized by social engineering fraud.

The Fifth Circuit held that the use of an email as part of a criminal's scheme was merely incidental to the occurrence of a fraudulent money transfer and therefore not sufficient to invoke a computer-fraud provision in an insured's policy. In *Apache Corp. v. Great American Insurance Co.*,[168] wrongdoers impersonated a vendor and contacted the insured by telephone and email requesting a change in the account to which the vendor's payments should be transferred. After calling a number on a document attached to the email, the insured made the change. The email contained a domain address of "petrofacltd.com," but the vendor's authentic email domain name was "petrofac.com."[169] Approximately $7 million was transferred to the new account owned by the wrongdoers.

The insured submitted a claim to its insurer, Great American Insurance Co. (GAIC), asserting coverage under its policy's computer-fraud provision. The computer-fraud provision stated, in pertinent part, that GAIC would "pay for loss of . . . money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that [money]. . . ."[170] GAIC denied the claim, advising the insurer that its "loss did not result directly from the use of a computer, nor did the use of a computer cause the transfer of funds."[171] The insured sued GAIC for denying its

165. *Id.*
166. *Id.*
167. *Id.*
168. 662 F. App'x 252 (5th Cir. 2016).
169. *Id.* at 253.
170. *Id.* at 254.
171. *Id.* at 255.

claim under the computer-fraud provision. On cross motions for summary judgment, the trial court granted the insured's motion and denied GAIC's motion.[172] The trial court concluded that the use of the email placed the loss within the computer-fraud provision. GAIC thereafter appealed.

Applying Texas law, the Fifth Circuit noted the Texas Supreme Court's preference for uniformity when identical insurance provisions are interpreted in other jurisdictions.[173] The court reviewed the case law from other jurisdictions and concluded that "there is cross-jurisdictional uniformity in declining to extend coverage when the fraudulent transfer was the result of other events and not directly by the computer use."[174] The court noted that the use of email was merely incidental to the transfer of money, and that to interpret the policy to cover any loss simply because an email communication was involved would "convert the computer-fraud provision to one for general fraud."[175] The court concluded that the "plain meaning of the policy language," and the uniform interpretations across jurisdictions, dictate that the insured's loss was not covered under the computer-fraud provision. Thus, the Fifth Circuit vacated the judgment of the trial court and rendered judgment in favor of GAIC.

The U.S. District Court for the Northern District of Georgia held that a commercial crime policy covered a fraudulent wire transfer. In *Principle Solutions Group, LLC v. Ironshore Indemnity, Inc.*,[176] an insured was a victim of a social engineering scheme. The insured's controller received a series of emails that tricked the controller into wiring $1.7 million to the fraudster.[177] The insured tendered the loss to its insurer, Ironshore Indemnity, under its "commercial crime policy." The policy at issue provided coverage for losses "resulting directly from a 'fraudulent instruction.'" However, Ironshore Indemnity denied the claim. The insured filed suit, arguing that the loss was covered under the commercial crime policy because the insured's loss resulted directly from a fraudulent email with "fraudulent instruction[s]."[178] Ironshore Indemnity argued that the loss did not result "directly" from the "fraudulent instruction" because there were intervening events, such as additional emails between the fraudster and the

172. *Id.* at 254.
173. *Id.* at 255.
174. *Id.* at 258.
175. *Id.*
176. 2016 WL 4618761 (N.D. Ga. Aug. 30, 2016).
177. *Id.* at *2.
178. Notably, the insured relied upon the district court's ruling in *Apache Corp. v. Great American Insurance Co.*, *see* 2015 WL 7709584, at *5, which the Fifth Circuit subsequently overturned.

insurer, the insurer's employees setting up and approving the wire transfer, and the bank actually performing the wire transfer.

The district court disagreed and held the insuring agreement to be ambiguous.[179] The district court held that an interpretation of "direct loss" as precluding any intervening actions, as well as an interpretation that permitted intervening actions, to both be reasonable.[180] Therefore, the court broadly construed the provision in favor of coverage for the insured.

In another case out of the Northern District of Georgia, the court held that a fraudulent scheme using telephones to exploit a computer coding vulnerability in the insured's system was not covered under an insurance policy's computer-fraud provision. In *InComm Holdings, Inc. v. Great American Insurance Co.*,[181] InComm Holdings, Inc., a debit card processing business, provided services that enabled consumers who had prepaid debit cards to load funds onto the cards. The cardholders purchased "chits" from a retailer and the retailer transferred the funds from the chit purchase to InComm's bank account. The cardholder could redeem the chit only once by calling InComm by telephone to access an "Interactive Voice Response" system (IVR) and providing the pin number on the chit and the account number of the debit card.[182] InComm then would make the funds available for use on the cardholder's debit card. Next, InComm would wire the funds to the bank of the debit card issuer to reimburse it for the purchases made with the debit card.

For approximately six months, there was an error in InComm's IVR system that allowed cardholders to redeem a chit more than once. When the error was discovered, there were over $10 million of unauthorized redemptions.[183] InComm submitted a claim under the computer-fraud provision of its policy with its insurer, GAIC. The policy, in pertinent part, afforded coverage for "loss of, and loss from damage to, money . . . resulting directly from the use of any computer to fraudulently cause a transfer of that [money]. . . ."[184] GAIC denied the claim, and InComm sued GAIC for breach of contract and bad faith.[185] The parties moved for cross summary judgment. GAIC argued that the loss did not result from the "use of any computer" and that there was no direct loss.[186]

The district court agreed with GAIC. As to whether the loss involved the use of a computer, the court rejected InComm's argument that the

179. *Id.* at *5.
180. *Id.*
181. 2017 WL 1021749 (N.D. Ga. Mar. 16, 2017).
182. *Id.* at *2.
183. *Id.* at *3.
184. *Id.*
185. *Id.* at *4.
186. *Id.*

IVR system was the computer that was used by the cardholders. The court examined the dictionary definitions of "computer" and "telephone" and concluded that a telephone was not a computer. In addition, the court examined the dictionary definition of "use" and concluded that the cardholders did not use the IVR system.[187] The court explained that the fact that "a computer was somehow involved in a loss does not establish that the wrongdoer 'used' a computer to cause the loss."[188] The court concluded that such a broad interpretation would "unreasonably expand the scope of the Computer Fraud Provision."[189]

The court further found that even if computers were used to cause InComm's loss, the loss did not result directly from the computer use. The court found that the loss occurred when the card issuer bank paid funds to the seller to settle the cardholder's purchases made with the debit card. The fraudulent redemptions of chits did not directly cause the loss because several other steps took place before the loss was incurred. The court found that the "weight of authority" was consistent with interpreting "directly" to mean "immediately."[190] Thus, the court granted GAIC's motion for summary judgment.

The U.S. District Court for the Southern District of New York recently held that a fraudulent wire transfer was a covered loss under a policy's computer-fraud provision. In *Medidata Solutions, Inc. v. Federal Insurance Co.*,[191] wrongdoers impersonated Medidata Solutions' president and advised accounts payable employees that an attorney would soon be contacting them with payment instructions. The email from the president advised that the matter was strictly confidential. That same day, an employee received a phone call from the purported attorney with wire transfer instructions. The employee explained to the attorney that she needed an email from Medidata's president requesting the wire transfer, and that she also needed approval from Medidata's Vice President and its Director of Revenue.[192] The fraudsters followed-up with an additional email purportedly from the president requesting the requisite approval. The employee subsequently initiated a wire transfer as instructed.[193] Soon thereafter, a second wire was requested by the president. The employee grew suspicious of this request and personally contacted the president, who advised that he had never requested a wire transfer.[194] The insured sought

187. *Id.* at *7–9.
188. *Id.* at *8.
189. *Id.*
190. *Id.* at *10.
191. 2017 WL 3268529 (S.D.N.Y. July 21, 2017).
192. *Id.* at *1.
193. *Id.* at *2.
194. *Id.*

coverage under its insurance policy's computer-fraud provision. The insurer, Federal Insurance Co., denied coverage, and litigation ensued.

The district court held that coverage was implicated and awarded summary judgment to Medidata. The court first held that the insured's system was hacked or breached because it was encrypted with a virus that resulted in Medidata's email server, during processing, changing the fraudster's true email address in the "From" line to the president's email address and picture.[195] The court also held that the emails directly caused the loss. The emails, standing alone, caused no loss. It was only after numerous additional, voluntary steps were performed by Medidata employees that the monies were transferred. Without citing to a case supporting its holding, the court concluded that "[t]he chain of events began" with the fraudulent email, such that the "direct loss" requirement was satisfied.[196]

Under seemingly similar facts as *Medidata Solutions*, in the U.S. District Court for the Eastern District of Michigan reached the opposite conclusion and held that a computer-fraud provision did not cover a fraudulent wire transfer. In *American Tooling Center, Inc. v. Travelers Casualty & Surety Co. of America*,[197] the insured received emails from a fraudster posing as one of its vendors. The emails instructed the insured to send payment for several legitimate invoices to a new bank account. In reality, the bank account did not belong to the legitimate vendor, but was instead controlled by the wrongdoers. The fraudulent emails were transmitted from a "yifeng-**rn**ould" domain, which was confused for the correct domain: "yifeng-**m**ould.com."[198] The insured transferred $800,000 to the fraudster's bank account.

The insured subsequently made a claim under its insurance policy's computer-fraud provision. The provision covered "direct loss" of money "directly caused by Computer Fraud." The insurer denied the claim, however, and the insured sued the insurer for breach of contract. The parties filed cross motions for summary judgment. The insurer argued that the loss was not "directly caused" by the use of a computer.

The district court agreed with the insurer. The district court explained that, "Given the intervening events between the receipt of the fraudulent emails and the (authorized) transfer of funds, it cannot be said that ATC suffered a 'direct' loss 'directly caused' by the use of any computer."[199] The court noted that there was no infiltration or hacking of the insured's computer system, and thus no coverage under the computer fraud insur-

195. *Id.* at *4.
196. *Id.* at *6.
197. 2017 WL 3263356 (E.D. Mich. Aug. 1, 2017).
198. *Id.* at *1.
199. *Id.* at *2.

ing agreement.[200] In a footnote, the court distinguished the holding in *Medidata Solutions*, noting that the language in the computer-fraud provision at issue was different.[201] In particular, the court explained that the policy in *Medidata* did not have language requiring the "direct loss" to be "directly caused by the Computer Fraud." Thus, the court granted the insurer's motion for summary judgment.

200. *Id.* at *3. The *American Tooling* court referenced *Apache Corp. v. Great American Insurance Co.*, 662 F. App'x 252 (5th Cir. 2016), and *Pestmaster Services, Inc. v. Travelers Casualty & Surety Co. of America*, 656 F. App'x 332 (9th Cir. 2016), in support of its holding.

201. *Id.* at *2 n.1.