# RECENT DEVELOPMENTS IN CYBERSECURITY AND DATA PRIVACY

*Lauren D. Godfrey, Matthew Horton, Ericka A. Johnson, Joshua A. Mooney, and Michael C. Zimmermann*



*Lauren D. Godfrey (lauren.godfrey@lewisbrisbois.com), is a Partner at Lewis Brisbois Bisgaard & Smith LLP in Pittsburgh, PA. Matthew Horton (mhorton@foley.com) is Senior Counsel at Foley & Lardner LLP in Washington, D.C. Ericka A. Johnson (Ericka.johnson@squirepb.com) is an Associate at Squire Patton Boggs in Washington, D.C. Joshua A. Mooney (mooneyj@whiteandwilliams.com) is a Partner at White and Williams LLP in Philadelphia, PA. Michael C. Zimmermann (mczimmermann@usfca.edu) is an attorney in San Francisco, CA.*

This survey reviews recent statutory developments and court decisions in the area of cybersecurity and data privacy law from October 1, 2018 through September 30, 2019. The first part discusses significant state data privacy and security statutes that were enacted, became effective, or are the most significant to practitioners during the survey period. Specifically, state legislatures are now focusing on strengthening data security measures in the insurance sector and requiring greater protections of consumers' online data. The second part discusses significant court decisions applying negligence principles, the economic loss doctrine, and the balancing of privacy interests in discovery. The third part highlights certain Federal Trade Commission ("FTC") enforcement actions seen during the survey period. The fourth part discusses court decisions which have interpreted cyber insurance policy provisions in the cybercrimes area.

## I. STATE DATA PRIVACY AND SECURITY STATUTORY DEVELOPMENTS

All fifty states have enacted their own version of a data-breach notification statute. States are now turning to data security statutes, some focusing on the insurance industry, for enacting standards for collecting and protecting consumer data.

### A. *The Insurance Data Security Law—Alabama, Connecticut, Delaware, Mississippi, and New Hampshire*[1]

Five states have enacted an Insurance Data Security Law (the "Acts"), legislation based upon the National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law, which in turn borrowed heavily from the cyber regulations promulgated by the New York Department of Financial Services ("DFS"), 23 NYCRR Part 500.

The Acts establish data security standards and a regulatory framework requiring insurers and other insurance-regulated organizations to "develop, implement, and maintain a comprehensive written information security program based upon a risk assessment" commensurate with the "size

1. Alabama Insurance Data Security Law, Ala. Code §§ 27-62-1 to 27-62-12, 2019 Ala. S.B. 54 (2019) (enacted and effective May 1, 2019) [hereinafter AL]; Connecticut Insurance Data Security Law, P.A. 19-117, § 230, 2019 Conn.. H.B. 7424 (2019) (enacted on June 26, 2019, effective on Oct. 1, 2020) [hereinafter CT], Delaware Insurance Data Security Act, Del. Code Ann. tit. 18, §§ 8601–8611, 2019 Del. H.B. 174 (2019) (enacted and effective July 31, 2019) [hereinafter DE]; Mississippi Insurance Data Security Law, Miss. Code Ann. §§ 83-5-801 to 83-5-825, 2019 Miss. S.B. 2831 (2019) (enacted on June 4, 2019, effective July 1, 2019) [hereinafter, MS]; New Hampshire Insurance Data Security Law, N.H. Rev. Stat. Ann. §§ 420-P:1 to 420-P:14, 2019 N.H. S.B. 194 (2019) (enacted on Aug. 2, 2019, effective on Jan. 1, 2020) [hereinafter NH].

and complexity" of the organization, and which "contains administrative, technical, and physical safeguards" to protect nonpublic information and the organizations' information systems.[2] The organization's information security program must include an incident response plan for cybersecurity events, and a document retention and disposal plan.[3] The Acts generally define "nonpublic information" as "electronic information that is not publicly available" and is either protected health information, or information that can be used to identify a consumer, in combination with one or more of the following data elements (1) Social Security number; (2) driver's license or non-driver identification card number; (3) financial account, credit card, or debit card number; (4) a security code, access code, or password that would permit access to a consumer's financial account; or (5) biometric records.[4]

As part of the information security program, a covered organization must designate an employee or outside vendor to oversee its program, and conduct periodic risk assessments that identify reasonably foreseeable cyber threats, the likelihood and potential damage of such threats, and the sufficiency of the organization's policies, procedures, and safeguards to withstand such threats.[5] Safeguards include employee training and management, appropriate network architecture and software design, detection/monitoring programs, and information classification, governance, and transmission.[6] The Acts expressly require that a covered organization's board of directors and executive management be involved with the development and implementation of the information security program.[7] The Acts also require covered organizations to conduct due diligence to ensure that their thirty-party service providers, such as law firms, have implemented "appropriate" cybersecurity measures.[8]

Covered organizations must notify the insurance commissioner of a "cybersecurity event" as "promptly as possible," but no later than three business days from the determination that a cybersecurity event occurred, where there is reasonable likelihood of material harm to the state resident

2. AL, *supra* note 1, § 54(4); CT, *supra* note 1, § 230(c)(1); DE, *supra* note 1, § 8604(a); MS, *supra* note 1, § 4(a); NH, *supra* note 1, ch. 420-P:4 § I.

3. AL, *supra* note 1, § 54(4); CT, *supra* note 1, § 230(c)(2), (10); DE, *supra* note 1, § 8604(f); MS, *supra* note 1, §§ 4(4), (8); NH, *supra* note 1, ch. 420-P:4 §§ IV(11), VIII.

4. AL, *supra* note 1, § 54(3)(11); CT, *supra* note 1, § 230(b)(9); DE, *supra* note 1, § 8603(12); MS, *supra* note 1, § 3(k); NH, *supra* note 1, ch. 420-P:3 § XI.

5. AL, *supra* note 1, § 54(4)(c); CT, *supra* note 1, § 230(c)(3); DE, *supra* note 1, § 8604(c); MS, *supra* note 1, § 4(3); NH, *supra* note 1, ch. 420-P:4 § III.

6. AL, *supra* note 1, § 54(4)(c); CT, *supra* note 1, § 230(c)(3), (7); DE, *supra* note 1, § 8604(d); MS, *supra* note 1, §§ 4(3), (4); NH, *supra* note 1, ch. 420-P:4 §§ III, IV.

7. AL, *supra* note 1, § 54(4)(e); CT, *supra* note 1, § 230(c)(5); DE, *supra* note 1, § 8604(e); MS, *supra* note 1, § 4(5); NH, *supra* note 1, ch. 420-P:4 § V.

8. AL, *supra* note 1, § 54(14); CT, *supra* note 1, § 230(c)(6); DE, *supra* note 1, § 8604(h); MS, *supra* note 1, § 4(6); NH, *supra* note 1, ch. 420-P:4 § VI.

whose information was compromised or to the organization's operations.[9] The Acts define a "cybersecurity event" as an "event resulting in unauthorized access to, disruption, or misuse of an information system or nonpublic information stored on an information system."[10] "Cybersecurity event" does not include unauthorized acquisition of encrypted data, or an "event" where the organization determines that the information "has not been used or released and has been returned or destroyed."[11]

The Acts empower the state's Department of Insurance to enforce the Act, but there is no private right of action.[12] The Acts also require certification of compliance with the Act every February 15 to the Commissioner of Insurance.[13] The effective dates for (1) implementation of the information security program and (2) implementation of the third-party due diligence are Alabama (May 1, 2020, May 1, 2021); Connecticut (Oct. 1, 2020, Oct. 1, 2021); Delaware (July 31, 2020, July 31, 2021); Mississippi (July 1, 2020, July 1, 2021), and New Hampshire (Jan. 1, 2021, Jan. 21, 2022).[14] Each statute enumerates certain exceptions to its requirements based on the organization's size.[15]

### B. *California*

Effective on January 1, 2020, the California Consumer Privacy Act ("CCPA") represents a fundamental change in privacy law in California, if not the whole United States, because of the broad reach of the statute and California's large economy.[16] CCPA regulates "personal information" of "consumers" and definies "consumer" as a California resident under the state tax code.[17] The CCPA broadly defines "personal information" as "information that identifies, relates to, describes, is reasonably capable of being

9. AL, *supra* note 1, § 54(6); CT, *supra* note 1, § 230(e)(1); DE, *supra* note 1, § 8606(a); MS, *supra* note 1, § 6(1); NH, *supra* note 1, ch. 420-P:6 § I.

10. AL, *supra* note 1, § 54(3)(4); CT, *supra* note 1, § 230(b)(3); DE, *supra* note 1, § 8603(4); MS, *supra* note 1, § 3(d); NH, *supra* note 1, ch. 420-P:3 § IV. Notably, the definition is narrower than New York's DFS cyber regulations definition for "cybersecurity event."

11. AL, *supra* note 1, § 54(3)(4); CT *supra* note 1, § 230(b)(3); DE, *supra* note 1, § 8603(4); MS, *supra* note 1, § 3(d); NH, *supra* note 1, ch. 420-P:3 § IV.

12. AL, *supra* note 1, §§ 54(2), (7), (10); CT, *supra* note 1, § 230(f), (h); DE, *supra* note 1, §§ 8602(b), 8607; MS, *supra* note 1, §§ 2(2), 7; NH, *supra* note 1, ch. 420-P:2 § II, 420-P:7.

13. AL, *supra* note 1, § 54(2); CT, *supra* note 1, § 230(c)(9); DE, *supra* note 1, § 8604(i); MS, *supra* note 1, § 4(9); NH, *supra* note 1, ch. 420-P:4 § IX. The date for the New Hampshire statute is March 1.

14. AL, *supra* note 1, § 54(14); CT, *supra* note 1, § 230(c)(1),(6); 2019 DE, *supra* note 1, H.B. 174 § 2 (2019); NH, *supra* note 1, ch. 420-P, § 2 (Implementation by Licensees).

15. AL, *supra* note 1, § 54(9)(a)(1); CT, *supra* note 1, § 230(c)(10); DE, *supra* note 1, § 8609(a); MS, *supra* note 1, § 9(1)(a); NH, *supra* note 1, ch. 420-P:9 § I.

16. The CCPA was originally enacted on June 28, 2018. It is included within the survey period because it has been one of the most important regulatory changes that practitioners and their clients have had to address during the survey period leading up to its effective date on January 1, 2020.

17. Cal. Civ. Code § 1798.140(g).

associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including names, addresses, commercial information, biometric information, internet-based information, including IP addresses and browsing history, and geolocation data.[18]

The CCPA applies to for-profit businesses that conduct business in California, collect consumer personal information, and determine the means of processing such information.[19] Excluded from the definition are not-for-profit organizations, and organizations that (1) have annual gross revenues of less than $25 million; (2) annually purchase, receive for commercial purposes, sell, or share personal information of less than 50,000 consumers, households, or devices; or (3) derive less than 50% of their annual revenue from selling consumers' personal information.[20] Other enumerated exceptions apply to the CCPA.[21]

The CCPA grants consumers explicit rights over their personal information. Subject to enumerated exceptions, those rights are the right to (1) access their personal information;[22] (2) know what personal information was collected;[23] (3) know whether personal information was sold or disclosed to third parties;[24] (4) request the deletion of their personal information (the right to be forgotten);[25] (5) prohibit the sale of personal information;[26] and (6) equal service and price if they exercise any right under the Act.[27] Upon receipt of a verifiable consumer request, a business has 45 days to comply, free of charge.[28] The business may extend the time to respond once by an additional 45 days, but only "when reasonably necessary," and if the consumer is informed during the first 45-day period.[29] Disclosures must cover the 12-month period predating the request, and must be in writing.[30]

The CCPA requires changes to company websites, including specific disclosures in online privacy notices and links to permit consumers to opt-out of the sale of their personal information.[31] It creates a private cause of

18. *Id.* § 1798.140(o). "Personal information" does not include "publicly available information," defined as "lawfully made available from federal, state, or local government records" (excluding biometric information collected without notice), or de-identified or aggregate consumer information. *Id.*; *see also* AB-874.
19. Cal. Civ. Code § 1798.140 (c) (1)
20. *Id.*
21. *Id.* § 1798.145(a)–(c).
22. *Id.* § 1798.100.
23. *Id.* § 1798.110.
24. *Id.* § 1798.115.
25. *Id.* § 1798.105.
26. *Id.* § 1798.120.
27. *Id.* §§ 1798.125, 1798.130(a)(2).
28. *Id.*
29. *Id.*
30. *Id.*
31. *Id.* §§ 1798.110(c), 1798.135(a)(1), 1798.130(a)(5), 1798.135(a)(2).

action for residents whose "nonencrypted and nonredacted personal information" has been "subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices," thereby making data breach class action litigation in California easier to sustain than is true elsewhere in the country.[32] However, this provision has a much narrower definition for "personal information" than elsewhere in the Act.[33] The CCPA does not create a private right of action for any other rights. Instead, the statute is to be enforced by the California Attorney General.[34] In September 2019, amendments to the CCPA were enacted, including a one-year exemption for employment and due diligence personal information.[35] On October 10, 2019, the California Attorney General introduced draft regulations under the Act.[36]

C. *Maine*

Effective July 1, 2020, "[a]n Act to Protect the Privacy of Online Customer Information" prohibits an Internet service provider from using, disclosing, selling, or permitting access to "customer personal information" without consent.[37] The Act defines "customer personal information" as "[p]ersonally identifying information about a customer, including but not limited to the customer's name, billing information, social security number, billing address and demographic data," or (2) "[i]nformation from a customer's use of broadband Internet access service," including a customer's browsing history, application usage, and geolocation data.[38] The Act prohibits providers from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount based on the customer's decision to provide or not provide consent to use his or her personal information.[39] The law also requires providers to take "reasonable measures to protect customer personal information from unauthorized use, disclosure or access."[40]

D. *Nevada*

Effective October 1, 2019, Nevada law now prohibits Internet operators from selling personal information collected about a Nevada consumer

32. *Id.* § 1798.150.
33. *Id.* § 1798.81.5(d)(1).
34. *Id.* § 1798.155(b); *see also id.* at § 1798.150(c).
35. The enacted bills were AB-25, AB-874, AB-1146, AB-1355, and AB-1564. For exceptions for due diligence and employment data, *see* Cal. Civ. Code § 1798.145(g), (h), AB-25, AB-1355.
36. *See* 2019 CA Regulation Text 25998. The comment period and public hearings close on Dec. 6, 2019.
37. 2019 Me. Laws 216 § 9301.2 (enacted on June 6, 2019).
38. *Id.* § 9301.1.C.
39. *Id.* § 9301.3.B.
40. *Id.* § 9301.5.

where the consumer has disallowed (or opted-out of) the sale of his or her information.[41] The law also requires operators to allow opt-out requests by email, a toll-free number, or website link.[42] The law adds exceptions to the definition for "operator," including financial institutions governed by GLBA and auto manufacturers.[43] "Sale" is defined more narrowly than the CCPA to mean "the exchange of covered information for monetary consideration … for the person to license or sell … to additional persons."[44] "Sale" excludes personal information processed for business purposes, entities with whom the consumer has a direct relationship, and affiliates.[45] An operator has 60 days to respond to a verified request, but may extend the deadline if "reasonably necessary," and with notice to the consumer, by no more than 30 days.[46] There is no private cause of action.[47]

E. *New York*

Effective October 23, 2019 (for changes in data breach notification requirements), and March 21, 2020 (for new data security requirements), New York's "Stop Hacks and Improve Electronic Data Security Act" ("SHIELD Act") broadens the state's data breach notification requirements and requires covered businesses to implement "reasonable" data security safeguards.[48] The SHIELD Act applies to any person or business, even those outside of the state, owning or licensing computerized data containing "private information" of a New York resident.[49] The SHIELD Act gives the New York Attorney General enforcement powers, but does not create a private right of action.[50]

*Change in Data Breach Notification Requirements.* The SHIELD Act requires notification of a "breach of security" by any person or business conducting business in New York and which owns or licenses "computerized data which includes private information" where such information is "reasonably believed to have been, accessed or acquired by a person without valid authorization."[51] The notification must be made "in the most expedient time possible and without unreasonable delay…."[52] Notification is not required where disclosure was inadvertent by persons with authorized

41. 2019 Nev. Rev. Stat. § 603A.300-360; 2019 Nev. S.B. 220 (enacted on May 30, 2019).
42. 2019 Nev. S.B. 220 §§ 1.3, 1.8.
43. 2019 Nev. Rev. Stat. § 603A.330.2
44. 2019 Nev. S.B. 220 § 1.6.
45. *Id.*
46. *Id.* § 2.4.
47. 2019 Nev. Rev. Stat § 630A.360.
48. 2019 N.Y. S.B. 5575 (enacted on July 25, 2019).
49. *See id.* § 3(2).
50. *Id.* §§ 3(6)(a), 4(2)(d), (e).
51. *Id.* § 2.
52. *Id.*

access, and the person/business "reasonably determines" that the disclosure "will not likely result in misuse of such information," or financial or emotional harm.[53]

The SHIELD Act expands notification obligations by both adding data elements to covered information and making unauthorized "access" to data sufficient to trigger a notification obligation.[54] Specifically, the SHIELD Act now defines "breach of security" as the "unauthorized access to or acquisition of, or access to or acquisition without valid authorization, of computerized data that compromises the security, confidentiality, or integrity of personal private information maintained by a business."[55] Thus, while previously a reasonable conclusion that compromised information had not been "acquired" in an unauthorized manner could bring an incident outside of the meaning of "breach of security," now the incident qualifies as a "breach of security" if the covered data is accessed.[56] "Breach of security" does not include "good faith access to, or acquisition of" private information by an employee or agent of the business" so long as the data is not used or subject to unauthorized disclosure.[57]

The SHIELD Act also adds data elements to covered data, including biometric data.[58] The SHIELD Act defines "private information" as "personal information" combined with one or more of the following non-encrypted data elements: (1) social security number; (2) driver's license or non-driver identification card number; (3) account, credit card or debit card number, in combination with a security code, access code, password, or other information that permits access to the financial account; (4) account, credit, or debit card number if that number alone could access an individual's financial account; or (5) biometric information, such as a fingerprint, voice print, retina or iris image, or other unique physical or digital representation used to authenticate or ascertain an individual's identity.[59] "Private information" also means "a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account."[60]

53. *Id.* Notice must be made directly to affected New York residents, unless the cost of direct notice would exceed $25,000, the affected class exceeds 500,000, or the business does not have sufficient contact information. If so, a business may notify by e-mail "conspicuously" posting notice on its web page, and by notifying major statewide media. *Id.* § 3(5)(d).

54. *Id.* § 1(b), (c).

55. *Id.* § 1(c).

56. *Id.*

57. *Id.*

58. *Id.* § 1(b).

59. *Id.*

60. *Id.* § 1(b). "Personal information" is defined as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person. *Id.* § 1(a).

*Data Security Requirements.* The SHIELD Act imposes data security requirements by requiring any person or business with computerized data having a New York resident's private information to "develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information."[61] Entities having data security programs compliant under New York's DFS cyber regulations, Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, or other federal data security laws are deemed compliant with the SHIELD Act.[62] The SHIELD Act lists the criteria of reasonable administrative, technical, and physical safeguards required in a data security program in order to comply with the SHIELD Act's requirements.[63] Businesses also must conduct due diligence on third-party service providers for "maintaining appropriate safeguards," and must require data security safeguards by contract.[64]

Small businesses are not exempt from implementing data security safeguards, but the safeguards need only be "appropriate for the size and complexity of the small business, the nature and scope of the small business's activities, and the sensitivity of the personal information the small business collects from or about consumers."[65] The SHIELD Act defines a "small business" as "any person or business with (i) fewer than fifty employees; (ii) less than three million dollars in gross annual revenue in each of the last three fiscal years; or (iii) less than five million dollars in year-end total assets, calculated in accordance with generally accepted accounting principles."[66]

### F. *Ohio*

Effective November 1, 2018, the Ohio Data Protection Act (the "Ohio Act"),[67] provides a legal safe harbor from tort liability for the failure to maintain an adequate data security program so long as the organization, at the time of the incident, maintained and complied with (1) "a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection" of personal or restricted information, and that (2) "reasonably conforms to an industry recognized cybersecurity framework."[68] The Ohio Act incorporates the definition for "personal information" under Ohio's data breach notification law.[69] The Ohio Act

61. *Id.* § 4(2).
62. *Id.* §§ 4(1)(a), 4(2)(i).
63. *Id.* § 4(2).
64. *Id.* § 4(b).
65. *Id.* § 4(2)(c).
66. *Id.* § 4(1)(c).
67. Ohio Rev. Code Ann. §§ 1354.01–.05 (enacted Aug. 3, 2018).
68. *Id.* § 13540.2(A), (D).
69. *Id.* § 1354.01(D); *see also id.* § 1349.19(7).

defines "restricted information" as non-encrypted "information about an individual" that can be used to identify the individual, and the breach of which "is likely to result in a material risk of identity theft or other fraud to person or property."[70] Industry-recognized frameworks include the NIST Cybersecurity Framework, as well as programs under GLBA, HIPAA, or data security program after the payment card industry data security standard (PCI DSS).[71]

The cybersecurity program must be designed to (1) protect the security and confidentiality of the information; (2) protect against any anticipated threats or hazards to the security or integrity of the information; and (3) protect against unauthorized access to and acquisition of the information that is likely to result in a material risk of identity theft or other fraud.[72] The Ohio Act recognizes that a one-size-fits-all approach is unworkable and delineates five factors to measure the appropriate scale and scope of a program: (1) size and complexity of the covered entity; (2) nature and scope of the activities of the covered entity; (3) sensitivity of the information to be protected; (4) cost and availability of tools to improve information security and reduce vulnerabilities; and (5) resources available to the covered entity.[73]

## II. TORT PRINCIPLES OF LAW

### A. *Negligence*

An important decision from the Pennsylvania Supreme Court found that an entity that affirmatively collects and stores the personal and financial information of data subjects on its internet-accessible computer systems has a reasonable duty to exercise reasonable care with respect to such information.[74] The decision suggests that the mere act of collecting and storing the personal and financial data of another gives rise to a duty, no matter the relationship between the data subject and the custodian of the data. This decision may deter entities that do not have proper security safeguards from collecting and storing data. Additionally, both the Pennsylvania Supreme Court and the Western District of Wisconsin issued decisions examining the availability of the economic loss doctrine as a defense against

70. *Id.* § 1354.01(E).
71. *Id.* § 1354.03(A), (B), (C). Others include NIST special publications 800-171 and 800-53, Federal Risk and Authorization Management Program (FedRAMP) security assessment framework, the CIS Critical Security Controls for Effective Cyber Defense, ISO 27000, and the Federal Information Security Modernization Act (FISMA).
72. *Id.* § 1354.02(B).
73. *Id.* §§ 1354.02(C).
74. Dittman v. UPMC, 196 A.3d 1036, 1048 (2018).

negligence claims arising from data breaches.[75] The holdings in those cases indicate that the issue will depend on the state law being applied.

In *Dittman v. UPMC*, the plaintiffs brought a class action complaint against the University of Pittsburgh Medical Center and UPMC McKeesport (collectively, "UPMC"), arising from UPMC's alleged breach of its duty to exercise reasonable care to protect the plaintiffs' "personal and financial information within [UMPC's] possession or control from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties."[76] The plaintiffs alleged that UPMC suffered a data breach involving the personal and financial information, including names, birth dates, social security numbers, addresses, tax forms, and bank account information, of all 62,000 UPMC employees and former employees which were accessed and stolen from UPMC's computer systems.[77] The plaintiffs also alleged that the stolen data was used to file fraudulent tax returns on behalf of UPMC's employees.[78]

In support of their allegations, the plaintiffs argued that because UPMC collected and stored the sensitive personal and financial information of UPMC employees, information which UPMC required employees to provide, it owed a duty to its employees to exercise reasonable care to protect the information from the foreseeable risk of a data breach.[79] The plaintiffs cited to principles of tort law, and argued that: "anyone who does an affirmative act is under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act."[80] Further, the plaintiffs argued that UPMC committed an affirmative act in collecting its employees' personal data and storing it on internet-accessible computer systems.[81] The plaintiffs contended that UPMC's practice of storing large amounts of data on internet-accessible computers made it foreseeable to UPMC that it would be the target of hackers, and therefore, the failure to use basic security measures could result in financial harm to victims.[82]

Moreover, while the plaintiffs acknowledged that, for the most part, one does not owe a duty to protect others from criminal acts, they argued that one does owe a duty to take reasonable anticipatory measures against *foreseeable* criminal conduct.[83]

75. *Id.* at 1056; Fox v. Iowa Health Sys., 2019 WL 3349988, at *8 (W.D. Wis. July 24, 2019).
76. Dittman, 196 A.3d at 1038–39.
77. *Id.* at 1038.
78. *Id.* at 1039.
79. *Id.* at 1044.
80. *Id.*
81. *Id.*
82. *Id.* at 1044–45.
83. *Id.* at 1045.

UPMC argued that it did not commit an affirmative act in collecting and storing its employees' personal and financial information because it merely possessed its employees' information as a result of a general employment relationship.[84] That it was the criminal acts of third parties, and not any affirmative conduct on its part that created the risk of harm.[85] Consequently, it could not be held liable for a third party hack based solely on the frequency and likelihood of hacks in contemporary society.[86] UPMC characterized the plaintiff's argument as a "radical reconstruction of duty" by seeking to impose liability on it for the criminal acts of unknown third parties.[87] According to UPMC, the criminal act of a third party is not "foreseeable by a negligent actor merely because he or she could have speculated that they might conceivably occur."[88]

The court noted that "[i]n scenarios involving an actor's affirmative conduct, he is generally 'under a duty to others to exercise the care of a reasonable man to protect them against an unreasonable risk of harm to them arising out of the act.'"[89] Further, the court reasoned that UPMC engaged in affirmative conduct, and created the risk of a data breach, by requiring its employees to provide personal and financial information as a condition of employment, and subsequently "collect[ing] and stor[ing] [that information] on its internet-accessible computer system without use of adequate security measures, including proper encryption, adequate firewalls, and an adequate authentication protocol."[90]

Further, the court referenced a previous decision finding that the criminal acts of a third party are not a superseding cause where the negligent actor "realized or should have realized the likelihood that such a situation might be created and that a third person might avail himself of the opportunity to commit such a tort or crime."[91] The court again referred to UPMC's collection and storage of employees' "requested sensitive personal data without implementing adequate security measures to protect against data breaches, including encrypting data properly, establishing adequate firewalls, and implementing adequate authentication protocol."[92] Thus, "[t]he alleged conditions surrounding UPMC's data collection and storage are such that a cybercriminal might take advantage of the vulnerabilities in

84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.* at 1046.
90. *Id.* at 1047.
91. *Id.* at 1048 (quoting Mahan v. Am-Gard, Inc., 841 A.2d 1052, 1061 (2003)).
92. *Id.*

UPMC's computer system and steal Employee's information; thus, the data breach was 'within the scope of the risk created by' UPMC."[93]

Because UPMC affirmatively collected and stored the personal and financial information of its employees on internet-accessible servers, it found that UPMC owed its employees a duty to exercise reasonable care over said information.[94] Additionally, the court found that duty was not negated because it was foreseeable that hackers would attempt to access that information.[95]

Notably, the court did not consider UPMC's position as an employer in finding that UPMC owed a duty to exercise reasonable care over the information it stored.[96] Nor did the court consider whether UPMC was in the business of providing data security when it found UPMC owed a duty to its employees.[97] The court's decision in *Dittman* should serve as a deterrent for entities that do not have proper security safeguards who are considering collecting and storing data.

### B. *Economic Loss Doctrine*

The *Dittman* court also considered whether the plaintiffs' claims were barred by Pennsylvania's Economic Loss Doctrine.[98] Under that doctrine, "no cause of action exists for negligence that results solely in economic damages unaccompanied by physical injury or property damage."[99] The plaintiffs argued that the economic loss doctrine did not apply because it does not bar negligence actions involving only financial harm where "the plaintiff establishes that the defendant owed a common law duty arising independently from any contract between the parties."[100] Thus, on the one hand, whether the economic loss doctrine applies depends on the source of the duty, and here, UPMC's duty to exercise reasonable care over the plaintiffs' personal information did not arise from contract.[101]

On the other hand, UPMC argued that it is well-settled in Pennsylvania that negligence claims seeking damages for purely economic loss are barred under the doctrine.[102] Additionally, UPMC claimed that the plaintiffs' argument regarding the source of the duty applied only to a narrow

93. *Id.*
94. *Id.* at 1047.
95. *Id.* at 1047–48.
96. *Id.* at 1046–48; *see also* Joshua Mooney, *Pennsylvania Supreme Court Holds Employers Have Duty to Protect Employee Data from Cyberattacks* (Nov. 26, 2018), https://www.whiteandwilliams.com/pp/alert-4376.pdf?24829.
97. *Id.* at 1047.
98. *Id.* at 1048–56.
99. *Id.* at 1042.
100. *Id.* at 1049.
101. *Id.*
102. *Id.*

group of cases.[103] For example, UPMC argued that the plaintiffs "argue for an improperly expansive interpretation of that case which would effectively render the economic loss doctrine a nullity by exempting all common law negligence claims from its application."[104]

In its reasoning, the court noted that "Pennsylvania has long recognized that purely economic losses are recoverable in a variety of tort actions," and that "a plaintiff is not barred from recovering economic losses simply because the actions sound in tort rather than contract law."[105] Further, the court agreed with the plaintiffs that whether the economic loss doctrine applies "turns on the determination of the source of the duty plaintiff claims the defendant owed."[106] Specifically, "if the duty arises independently of any contractual duties between the parties, then a breach of that duty may support a tort action."[107] Therefore, the court held that because the plaintiffs argued that UPMC breached its common law duty to act with reasonable care in collecting and storing its employees' personal and financial information, and that duty existed regardless of any contract between the parties, the economic loss doctrine did not bar the plaintiffs' claims.[108] The court's opinion suggests that the economic loss doctrine will be largely irrelevant where plaintiffs bring claims for breaches of the duty to exercise reasonable care over stored data regardless of the contractual relationship between the parties.[109]

In contrast, *Fox v. Iowa Health System* found that the Illinois and Iowa plaintiffs' claims for negligence and negligence *per se* were barred by the economic loss doctrine.[110] The *Fox* court examined the applicability of the economic loss doctrine in negligence actions and the viability of invasion of privacy claims in response to data breaches.[111] Four plaintiffs from Wisconsin, Illinois, and Iowa brought 14 claims on behalf of a proposed class against a defendant administrator of hospitals, clinics, home care services, and health insurers, operating throughout Wisconsin, Illinois, and Iowa.[112] The defendant stored the personal information of its patients and customers, including patient names, Social Security numbers, payment information, phone numbers, and email addresses.[113] The defendant also stored

103. *Id.*
104. *Id.* at 1049–50.
105. *Id.* (quoting Bilt-Rite Contractors, Inc. v. Architectural Studio, 866 A.2d 270, 288 (2005)).
106. *Id.* at 1054 (quoting Bilt-Rite, 866 A.2d at 288).
107. *Id.*
108. *Id.* at 1056.
109. *Id.* at 1054–56.
110. 2019 WL 3349988, at *7 (W.D. Wis. July 24, 2019).
111. *Id.* at *8–9.
112. *Id.* at *1–2.
113. *Id.* at *2.

patient health care information, including lab results, treatment notes, and diagnoses.[114] The defendant's privacy policy stated that it would store its customer's personal information "in a secure database behind an electronic firewall."[115]

In November 2017, hackers obtained access to the email accounts of the defendant's employees and stole the personal health information of over 16,000 of the defendant's patients.[116] Further, "[t]he hackers were 'motivated to steal' and 'specifically targeted' health information and other sensitive information including Social Security numbers."[117] While the defendant discovered the breach in February 2018, it did not inform victims until two months later.[118] In its letter to victims informing them of the breach, the defendant expressly stated that the stolen information did not include Social Security numbers.[119] The same day it sent that letter to victims of the breach, however, the defendant disclosed to the Wisconsin Department of Agriculture, Trade and Consumer Protection that the breach included Social Security numbers.[120] Further, in May 2018, the defendant discovered an additional hack of its employees' email accounts had occurred.[121] In that data breach, hackers obtained the data of about 1.4 million patients.[122] Similar to the first breach, the defendant waited two months before it informed victims.[123]

The *Fox* court dismissed the argument that application of the economic loss doctrine "turns on the determination of the source of the duty plaintiff claims the defendant owed" which the *Dittman* court had accepted in finding the doctrine inapplicable.[124] Similar to the plaintiffs in *Dittman*, the plaintiffs in *Fox* argued that the economic loss doctrine did not apply to the plaintiff from Illinois or the proposed class members from Illinois because "Illinois has an exception to the economic loss doctrine for duties that exist independent of any contract."[125] However, the court determined that under Illinois law, this exception applied only in professional malpractice cases, where for example, "the defendant is a member of a skilled profession and

114. *Id*.
115. *Id*.
116. *Id*.
117. *Id*.
118. *Id*.
119. *Id*.
120. *Id*.
121. *Id*.
122. *Id*.
123. *Id*.
124. *Id*. at *8 (quoting Dittman v. UPMC, 196 A.3d 1036, 1054 (2018)).
125. 2019 WL 3349988 at *8. Here, the plaintiffs argued the defendant "had a preexisting duty to protect patient health records under federal law." While neither party identified that federal law, the court suspected this was the Health Insurance Portability and Accountability Act ("HIPAA").

has a duty of reasonable professional competence."[126] While the *Dittman* court found that the economic loss doctrine did not apply because of Pennsylvania's history of finding it inappropriate in a variety of tort actions, the court in *Fox* was limited by Illinois precedent finding the doctrine inapplicable for only minor exceptions.[127]

C. *Right to Privacy*

While states strive to protect the privacy of consumers' personal information by enacting data breach notification and data security statutes, courts continue to address an individual's right to privacy through tort principles and discovery. Courts must balance the privacy rights of a plaintiff with the defendant's right to discover information which is relevant to the plaintiff's claims against the defendant.

The Western District of Wisconsin in the *Fox* case, discussed *supra*, dismissed plaintiffs' claim that defendant violated Wisconsin's Invasion of Privacy statute.[128] There, plaintiffs argued that Wisconsin's Invasion of Privacy statute provides relief where one's "privacy is unreasonably invaded," and the inclusion of the word "unreasonably" in the statute implied a negligence standard.[129] On the other hand, the court noted that among the elements of publication of private information (one of Wisconsin's Invasion of Privacy torts), is "a public disclosure of facts regarding the plaintiff."[130] Further, the court noted that while the statute did not state whether this required an intentional disclosure by the defendant, or an unreasonable one, it noted that under a separate Wisconsin statute, Invasion of Privacy is categorized as an intentional tort.[131] Additionally, the court noted that other courts that had considered similar claims had found that an intentional action was required, and that Wisconsin's Invasion of Privacy statute stated that the section was to be "interpreted in accordance with the developing common law of privacy."[132] Therefore, the court dismissed the plaintiffs' claim under Wisconsin's Invasion of Privacy statute because there was no intentional public disclosure of facts about the plaintiffs.[133] Given that data breaches are necessarily unintentional by the custodian of data, the court's decision in *Fox* suggests that future plaintiffs will likely be unable to bring claims under Wisconsin's Invasion of Privacy statutes arising from data breaches.

126. *Id.*
127. *Id.*
128. *Id.* at *10.
129. *Id.* at *9.
130. *Id.*
131. *Id.*
132. *Id.*
133. *Id.* at *10.

In *Henson v. Turn, Inc.*, the Northern District of California denied a defendant's requests for production related to the plaintiffs' mobile devices and web history as too broad and invasive of the plaintiffs' privacy.[134] In *Henson*, two plaintiffs brought claims for violations of New York's General Business Law § 349 and trespass to chattels on behalf of a class and arising from the defendant's alleged practice of placing "zombie cookies" on users' devices: "cookies that users either cannot delete or block or that, when users try to delete them, 'respawn' to continue tracking users cross the web."[135] The defendant was allegedly able to implement the zombie cookies through Verizon's practice of assigning each of its customers a unique identifier header, referred to as a "UIDH" or "X-UIDH".[136] That X-UIDH identifier was placed into the header of every HTTP request Verizon customers made from their mobile devices.[137] Further, when a Verizon customer visited one of the defendant's partner websites, a cookie would be placed in the customer's browser with a certain ID number.[138] If that user deleted her cookies, and subsequently visited another website operated by one of the defendant's partners, the website would recognize the user's Verizon X-UIDH number, and place a cookie with the same ID number as before.[139] Consequently, all of the browsing history from the user's previously deleted cookies would be placed back on the device.[140]

In its discovery requests, the defendant requested that the plaintiffs allow it direct access to the plaintiffs' mobile devices, or in the alternative, complete forensic images of the plaintiffs' mobile devices.[141] Additionally, the defendant requested that the plaintiffs produce the entirety of their web browsing history from their mobile devices and all of the data from the cookies stored or deleted from their mobile devices.[142] In support of its argument to obtain this information, the defendant argued that an inspection of the plaintiffs' phones was required in order to determine, for example, whether the defendant placed and replaced cookies on the plaintiffs' phones, and whether the plaintiffs regularly deleted cookies and their web browsing history from their phones.[143]

In response, the plaintiffs argued that allowing the defendant direct access to their phones or producing a complete forensic image of their phones would allow the defendant "access to Plaintiffs' entire phones and

134. Henson v. Turn, Inc., 2018 WL 5281629, at *5–8 (N.D. Cal. Oct. 22, 2018).
135. *Id.* at *1.
136. *Id.* at *2.
137. *Id.*
138. *Id.* at *3.
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.* at *4.

thus access to their private text messages, emails, contact lists, photographs and web browsing histories unrelated to [the defendant]."[144] Accordingly, they argued the request violated Federal Rule of Civil Procedure Rule 26(b)'s relevancy and proportionality requirements.[145]

In considering the defendant's request, the court noted that under Federal Rule of Civil Procedure 26(b)(1), discovery is limited to matters that are: (1) "relevant to any party's claim or defense" and (2) "proportional to the needs of the case."[146] In its relevancy analysis, the court noted that the defendant's request would likely include such irrelevant materials as "the plaintiffs' private text messages, emails, contact list, and photographs."[147] Regarding the proportionality requirement, the court noted that courts have held that privacy interests can be a consideration in evaluating the proportionality of a discovery request.[148] The court cited from the Supreme Court's decision in *Riley v. California* to highlight the significant privacy concerns of allowing unfettered access to an individual's cell phone.[149] Finally, the court noted that the defendant could not cite another case where a party had been allowed direct access to an opponent's device or forensic images of that device.[150]

As to the defendant's request for plaintiffs' full web browsing history, including websites other than the defendant's partner sites, the court again cited to *Riley*, and noted that the plaintiffs' compliance with this request presented significant privacy concerns.[151] Further, the court noted that cookies are closely associated with websites, and it would raise similar privacy concerns if plaintiffs turned over the entirety of the data from their cookies on their mobile devices.[152] Therefore, the court held that the defendant's requests were not relevant or proportional to the needs of the case.[153]

144. *Id.*
145. *Id.*
146. *Id.* at *5.
147. *Id.*
148. *Id.* (citing Crabtree v. Angie's List, Inc., 2017 WL 413242, at *3 (S.D. Ind. Jan. 31, 2017) (denying request to forensically examine plaintiff's personal cell phones and holding that the forensic examination "is not proportional to the needs of the case because any benefit the data might provide is outweighed by Plaintiffs' significant privacy and confidentiality interests.")).
149. *Id.* at *6 (quoting Riley v. California, 134 S. Ct. 2473, 2494–95 (2014)) ("Modern cell phones are not just another technology convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'")).
150. *Id.*
151. *Id.* at *8 (quoting Riley, 134 S. Ct. at 2490) ("An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns – perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.")).
152. *Id.*
153. *Id.*

The court also critiqued the scope of the defendant's discovery requests.[154] For example, the court found that it was ironic that, in order to obtain relief for the defendant's secret monitoring of the plaintiffs' mobile devices and browsing history, the plaintiffs had to provide the defendant with even more personal information.[155] Though the court stated that it did not intend for its opinion to imply that there could never be an instance where requests similar to the defendant's would be relevant and proportional, the court's decision suggests that discovery requests related to mobile devices and web activity will be denied where there is no discernment by the requesting party regarding the information it seeks.[156] The court likely would have been more inclined to look favorably upon the defendant's requests if they were limited to browsing history and cookies related to the defendant's partner websites, rather than plaintiffs' *complete* browsing history, and *all* of the cookies stored on the plaintiffs' mobile devices.[157]

## III. FEDERAL TRADE COMMISSION ENFORCEMENT

The Federal Trade Commission ("FTC" or "Commission") is charged with protecting consumers from unfair, deceptive and fraudulent practices in the marketplace.[158] Through the Bureau of Consumer Protection, the FTC enforces consumer protection laws by collecting complaints, conducting investigations, and suing companies and individuals that break the law.[159] In the area of identity theft protection and data privacy and security, the Division of Privacy and Identity Theft Protection enforces the statutes and rules within its jurisdiction.[160] During the survey period, settlements with the FTC related to, among other things, alleged violations of (1) the Children's Online Privacy Protection Act ("COPPA") Rule in *United States of America, et al. v. Google LLC & YouTube LLC* ($170 million settlement)[161]

154. *Id.*

155. *Id.* ("There is an Orwellian irony to the proposition that in order to get relief for a company's alleged surreptitious monitoring of users' mobile device and web activity, a person has to allow the company unfettered )access to inspect his mobile device or his web browsing history. Allowing this discovery would further invade the plaintiffs' privacy interests and may deter current and future plaintiffs from pursuing similar relief.").

156. *Id.*

157. *Id.* at 4–5.

158. 15 U.S.C. §§ 41–58, as amended; *see also* Fed. Trade Comm'n, What We Do, https://www.ftc.gov/about-ftc/what-we-do (last visited Apr. 8, 2020).

159. Fed. Trade Comm'n, Bureau of Consumer Prot., https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection (last visited Apr. 8, 2020).

160. Fed. Trade Comm'n, Division of Privacy and Identity Protection, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/our-divisions/division-privacy-and-identity (last visited Apr. 8, 2020).

161. United States v. Google LLC and YouTube, LLC, No. 1:19-cv-02642 (D.D.C. Sept. 10, 2019) (FTC allegations that the companies illegally collected personal information of children without parental consent).

and *United States of America v. Musical.ly, Inc.* ($5.7 million settlement),[162] (2) the Safeguards Rule of the Graham Leach Bliley Act in *Federal Trade Commission v. Equifax* ($425 million settlement),[163] and (3) the European Union-United States Privacy Shield in *In the Matter of LotaData, Inc.* (consent order).[164]

## IV. CYBERCRIMES

Industry reports indicate the market for cyber insurance continues to grow,[165] with some forecasting that it will rocket from $4 billion in 2019 to more than $23 billion by 2025.[166] As in previous years, in 2019, cyber threats caused courts to interpret and nuance cyber insurance policies that, after the attack or after the court decision, were seemingly inapt or obsolete when they were issued. Courts continue to wrestle with applying conventional legal notions to novel fact patterns, often resulting in inconsistent or disappointing court decisions.[167]

### A. *"Computer Fraud" Coverage and Social Engineering*

The Second Circuit found that a "computer fraud" provision applied in *Medidata Solutions v. Federal Insurance Co.*,[168] in the context of a social engineering attack perpetuated from *within* a policyholder's computer network.[169] When juxtaposed to a 2018 decision from the Ninth Circuit, this Second Circuit case highlights a critical fact in social engineering attacks:

---

162. United States v. Musical.ly, Inc., No. 2:19-cv-1439 (C.D. Cal. Feb. 27. 2019) (FTC allegations that the company illegally collected personal information of children).

163. Federal Trade Commission v. Equifax, No.: 1:19-cv-03297-TWT, at 2 (N.D. Ga. July 23, 2019). (FTC allegations that Equifax violated the Safeguards Rule of the GLBA by failing to secure personal information).

164. *In re* LotaData, Inc., FTC File No. 182 3194, 84 FR 47295, 47295–47296 (Sept. 9, 2019) (FTC allegations that the company falsely claimed on their website that it was certified under the E.U.-U.S. Privacy Shield).

165. *State of the Cyber Insurance Market—Top Trends, Insurers and Challenges: A.M. Best*, Ins. J. (June 18, 2019), *available at* https://www.insurancejournal.com/news/national/2019/06/18/529747.htm.

166. Bruce Sussman, *5 Reasons Cyber Insurance Market Will Hit $23 Billion*, Secure World (Apr. 16, 2019), *available at* https://www.secureworldexpo.com/industry-news/5-reasons-cyber-insurance-market-will-hit-23-billion.

167. *See, e.g.*, Shaun S. Wang, *Integrated Framework for Information Security Investment and Cyber Insurance*, 57 Pac. Basin Fin. J. 9 (Oct. 2019) ("The global cyber insurance market is quite complex with over 600 cyber insurance policy forms offered by more than a hundred insurers globally, with different wordings and inconsistent court interpretations of the scope of insurance coverage. Uncertainty about the scope of insurance policy reduces the confidence of firms in seeing their insurance policy as a definite guaranteed protection against potential cyber loss. Lack of clarity on insurance coverage has been suggested as a major reason for limited adoption of cyber insurance.").

168. 729 F. App'x 117 (2d Cir. 2018)

169. Social engineering fraud is generally conducted by enlisting the trust of its victims to voluntarily disclose information or perform the fraudulent transaction.

whether the attack was launched from "inside" or "outside" the target company's enterprise. The Ninth Circuit affirmed a decision from the Western District of Washington that a social engineering attack originating from *outside* a company's network was not covered by the target company's "computer fraud" provision, because the policy excluded coverage for acts of authorized users, even where an authorized user was "duped" by an external fraudster.[170] By contrast, the Second Circuit addressed the inverse circumstances, finding that a social engineering attack launched from *inside* a target company's network was covered by a "computer fraud" provision.

In *Medidata*, fraudsters manipulated Medidata's email systems through a spoofing code, allowing the fraudsters to send messages that appeared, in all respects, to come from a high-ranking member of Medidata's organization.[171] In doing so, the fraudsters tricked Medidata into wiring $4.8 million to an overseas account.

Medidata brought suit against its insurer, Federal Insurance, claiming that its losses were covered by a computer fraud provision in its insurance policy.[172] The provision covered losses stemming from any "entry of Data into" or "change to Data elements or program logic of" a computer system.[173]

Federal Insurance asserted that the spoofing attack was not covered because there had been no "changes to data elements."[174] Federal Insurance further argued that Medidata did not sustain a "direct loss" as a result of the spoofing attack, within the meaning of the policy.[175] The spoofed emails directed Medidata employees to transfer funds in accordance with an acquisition, and the employees made the transfer that same day.[176] In effect, Federal Insurance argued that the social engineering portion of the scheme, severed the causal relationship between the spoofing attack and the losses incurred. As such, Federal Insurance argued, Medidata did not experience a "direct loss" as contemplated by the policy.

The Second Circuit disagreed and affirmed the district court's summary judgment award in favor of Medidata finding that the computer fraud

170. *See* Aqua Star (USA) Corp. v. Travelers Cas. & Sur. Co. of Am., No. 16-35614, at 2 (9th Cir., Apr. 18, 2018) ("[E]ven assuming without deciding that the policy generally covers "Computer Fraud" of the kind that duped Aqua Star, the policy's exclusions foreclose coverage . . . [because the policy] unambiguously provides that the policy 'will not apply to loss or damages resulting . . . [from] a natural person having the authority to enter the Insured's Computer System . . . [and because] Aqua Star's losses resulted from employees authorized to enter its computer system . . . sending four payments to a fraudster's account.").

171. *Id.* at 118.

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.* at 119.

176. *Id.*

provision applied.[177] Specifically, while Medidata conceded that no hacking occurred, the fraudsters nonetheless crafted a computer-based attack that manipulated Medidata's emails systems (which the parties did not dispute constituted a "computer system" within the meaning of the policy.)[178] Thus, the attack represented a fraudulent entry of data into Medidata's computer system, since the spoofing code was introduced *into* the email systems.[179]

Furthermore, the Second Circuit found a direct loss, which was equated to a "proximate cause" standard under New York courts, holding that the spoofing attack was the proximate cause of Medidata's losses.[180] While the Medidata employees themselves had to take action to effectuate the transfer, the court did not see their actions as sufficient to sever the causal relationship between the spoofing attack and the losses incurred.[181]

B. *Personal Injury and General Liability Policies*

The Middle District of Florida recently found no coverage for third party breaches in *St. Paul Fire & Marine Ins. Co. v. Rosen Millennium, Inc.*[182] In *St. Paul*, Rosen Hotels & Resorts, Inc. ("RHR") detected malware installed on its payment network, potentially affecting customers' credit cards for over a year and a half at one of its hotels.[183] At the time of the breach, Rosen Millennium, Inc. ("Millennium"), provided data security services for RHR.[184] St. Paul Fire and Marine Insurance Company ("St. Paul") had issued Millennium two consecutive commercial general liability insurance policies (the "CGL"), which were in effect during the relevant time periods.[185]

Millennium submitted a Notice of Claims to St. Paul in response to an e-mail Millennium received from RHR; in that email, RHR indicated its belief that Millennium's negligence caused the data breach and inquired as to whether Millennium had insurance to cover such a loss.[186]

St. Paul sought declaratory judgment that, *inter alia*, St. Paul had no duty to defend Millennium against RHR, asserting that as a matter of contract interpretation RHR's claim was not covered under a "personal injury" provision of Millennium's CGL Policies.[187] The CGL Policies defined "personal injury," as an "injury, other than bodily injury or advertising injury,

177. *Id.*
178. *Id.* at 118.
179. *Id.*
180. *Id.* at 119.
181. *Id.*
182. 337 F. Supp. 3d 1176, 1185 (M.D. Fla. 2018).
183. *Id.* at 1180.
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.* at 1183.

that's caused by a personal injury offense."[188] A "personal injury offense" includes, "making known to any person or organization covered material that violates a person's right of privacy."[189] As the term "making known" was not defined, the parties disputed whether the "making known" requirement had been met.[190] Specifically, whether third-party data breaches (as opposed to breaches by the insured) could satisfy this requirement.[191]

The court relied upon *Innovak International, Inc. v. Hanover Insurance Company*.[192] In that case, the court found that the only plausible interpretation of the insurance policy was that it required the insured (and not a third party) to be the publisher of the private information; noting that as a matter of South Carolina law, construing the policy to include the acts of third parties would have improperly expanded coverage beyond what the insurance carriers had knowingly agreed to and issued.[193] Finding that Millennium's CGL defined "personal injury" similar to the provisions of *Innovak*, the court in *St. Paul* found that third party breaches were not covered by Millenniums's CGL.[194]

Moreover, the court held that the CGL Policies required covered personal injuries to "result from the insured's business activities."[195] The court narrowly held that RHR's alleged injuries did not result from Millennium's business activities but rather the actions of third parties. Therefore, the Court found that RHR's personal injury claim was not covered under the CGL Policies.[196]

188. *Id.* at 1184.
189. *Id.* at 1184–85.
190. *Id.* at 1185.
191. *Id.*
192. 280 F. Supp. 3d 1340, 1347–48 (M.D. Fla. 2017)
193. *St. Paul Fire & Marine Ins. Co.*, 337 F. Supp. 3d at 1185 (internal quotes and citations omitted).
194. *Id.*
195. *Id.* (internal quotes and citations omitted).
196. *Id.*