Journal of Business & Technology Law

Volume 13 | Issue 2 Article 4

Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?

Loren F. Selznick

Carolyn LaMacchia

LOREN F. SELZNICK* AND CAROLYN LAMACCHIA*

Cybersecurity Liability: How Technically Savvy Can We Expect Small Business Owners to Be?

INTRODUCTION

"Target Data Breach Spilled Info on As Many As 70 Million Customers."[1] "Home Depot's breach could be as big as Target's."[2] Data breaches at the nation's largest retail companies dominate the news, but small businesses are at greater risk.[3] Hackers recognize that small businesses have neither the financial resources nor the technical expertise to protect their data.[4] Cyberattacks on small businesses intensify, but the law's cybersecurity liability model develops with only the largest corporations in mind.[5]

When the public learns of data breaches at the megastores, its reaction is outrage.[6] State regulators are inclined to punish the corporation.[7] How could the corporation have been so careless with customer information? The hacker behind the breach is presumed to be untraceable and, in any event, too poor to pay for all the

* Dr. Selznick (J.D. Cornell University) is an Assistant Professor of Business Law and Dr. LaMacchia (Ph.D. Nova Southeastern University) is an Assistant Professor of Information and Technology Management at Bloomsburg University of Pennsylvania.

1. Maggie McGrath, *Target Data Breach Spilled Info on as Many as 70 Million Customers*, FORBES (Jan. 10, 2014, 8:56 AM), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#4b03288be795.

2. Jaikumar Vijayan, *Home Depot Breach Could be as Big as Target's*, COMPUTERWORLD (Sept. 2, 2014, 1:13 PM), http://www.computerworld.com/article/2600309/data-security-home-depot-breach-could-potentially-be-as-large-as-targets.html.

3. Jane Chen, *Cyber Security: Bull's-Eye on Small Businesses*, 16 J. INT'L BUS. & L. 97, 97–100 (2016).

4. *Id.* at 100.

5. *See id.* at 108 (noting that current cyber-security regulations do not discuss the requirements of small businesses prior to a breach).

6. Lauren Zumbach, *Massive Equifax Data Breach Prompts Outrage, Investigations, Bills to Ban Credit Freeze Fees*, CHI. TRIB. (Sept. 16, 2017, 5:32 PM), http://www.chicagotribune.com/business/ct-equifax-data-breach-0917-biz-20170915-story.html.

7. *Id.*; *see infra* notes 199–206.

consumer harm.[8] The corporate victim of the breach is blamed for failing to adopt reasonable cybersecurity measures.[9] Customers with compromised data bring class action lawsuits and regulators seek fines.[10] Some courts have been reluctant to impose liability on the corporate victim of a third-party hacker, but a growing number have allowed claims on a variety of theories.[11]

This legal trajectory poses a threat to small businesses.[12] Small businesses face the same risk of data breach as their larger counterparts but lack the resources for cybersecurity measures.[13] A cyberattack, followed by customer suits and state fines, could mean the end of a small business unfairly held to an impossible standard of cybersecurity.[14]

This interdisciplinary article describes the unique cyber dangers to small businesses. It then surveys the emerging law of data breach liability—the variety of liability and damage theories customers have asserted around the country and the potential for lawsuits and fines under state data breach notification laws. Next, the article considers whether the potential liability of a small business for a third-party hacker data breach is unacceptably high. Finally, an alternative market-driven statutory approach is suggested to protect small businesses.

I. THE RISKS TO SMALL BUSINESSES

Cyberattacks are surging and smaller businesses are likely to be targeted.[15] Because of their limited resources and technological skills, small businesses are easy prey for hackers.[16] Large corporations employ teams of information technology personnel, an

8. Justin C. Pierce, *Shifting Data Breach Liability: A Congressional Approach*, 57 WM. & MARY L. REV. 975, 990 (2016).

9. *Id.* at 990–91.

10. *Id.* at 54; Charlotte A. Tschider, *Experimenting with Privacy: Driving Efficiency Through a State-Informed Federal Data Breach Notification and Data Protection Law*, 18 TUL. J. TECH. & INTELL. PROP. 45, 51 (2015).

11. *Compare* Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011) (dismissing a claim against a payroll processing firm for damages caused by a breach for lack of Article III standing), *with In re* Target Corp. Customer Data Security Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (holding that plaintiffs did have standing based on collateral consequences from the breach).

12. *See infra* Part IV.

13. *See infra* Part I.

14. *See, e.g.*, Brief of Appellant at 7, LabMD, Inc. v. Federal Trade Comm'n, No. 16-16270, 2014 WL 2994344 (11th Cir. Dec. 27, 2016) (citing the severe costs of compliance with an FTC investigation and litigation to the business of a small medical laboratory).

15. *See* Chen, *supra* note 3, at 100.

16. *See id.*

impossibility for small businesses.[17] The larger businesses also mount multi-faceted defenses against data breaches, which smaller businesses cannot do.[18]

A. Data Breach Targets

The number and severity of cyber security attacks increase each year.[19] About 80 percent of executives and security experts surveyed reported a security breach in their organizations within the past year.[20] Since many incidents go undetected, this figure is undoubtedly understated.[21] Cyber-attacks are "becoming progressively destructive and target a broadening array of information and attack vectors."[22] All business, both large and small, are targeted.[23]

In 2016, reported data breaches increased by 40 percent over 2015.[24] Yahoo announced the largest data breach in history affecting more than one billion accounts.[25] 2017 was also an active year.[26] Examples of major breaches using a variety of techniques can be found in business, academia, health care, and governments around the world.[27] Cyber criminals stole approximately $54.5 million from FACC, an Austrian-based aerospace parts manufacturer (with clients like Airbus and

17. Chris Morris, *14 Million US Businesses are at Risk of a Hacker Threat*, CNBC (July 25, 2017, 10:02 AM), https://www.cnbc.com/2017/07/25/14-million-us-businesses-are-at-risk-of-a-hacker-threat.html.

18. Taylor Armerding, *Why Criminals Pick on Small Business*, CSO (Jan. 12, 2015, 4:04 AM), https://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html.

19. Herb Weisbaum, *Data Breaches Happening at Record Pace, Report Finds*, NBC NEWS (July 24, 2017, 10:18 AM), https://www.nbcnews.com/business/consumer/data-breaches-happening-record-pace-report-finds-n785881; PRICEWATERHOUSECOOPERS, US CYBERSECURITY: PROGRESS STALLED KEY FINDINGS FROM THE 2015 US STATE OF CYBERCRIME SURVEY 3 (2015), https://www.pwc. com/us/en/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf.

20. PRICEWATERHOUSECOOPERS, *supra* note 19, at 3.

21. *Id.*

22. *Id.*

23. *See, e.g.*, Sam Thielman, *Yahoo Hack: 1bn Accounts Compromised by Biggest Data Breach in History*, GUARDIAN (Dec. 15, 2016, 7:23 AM), https://www.theguardian.com/technology/2016/dec/ 14/yahoo-hack-security-of-one-billion-accounts-breached.

24. Olga Kharif, *2016 Was a Record Year for Data Breaches*, BLOOMBERG TECH. (Jan 19, 2017, 7:00 AM), https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked.

25. Thielman, *supra* note 23.

26. Abigail Summerville, *Protect Against the Fastest-Growing Crime: Cyber Attacks*, CNBC (July 25, 2017, 1:12 PM), https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html.

27. PRICEWATERHOUSECOOPERS, *supra* note 19, at 5.

Boeing).[28] Chipotle reported unauthorized network activity on its in-restaurant payment processor impacting several weeks of payment card transactions.[29] Information including Social Security numbers belonging to over 150,000 current and former students, faculty, and staff was stolen from the University of Central Florida[30] and the University of California, Berkeley.[31] Newkirk Products, Inc., a service provider that issues healthcare identification cards, announced a data breach that affected up to 3.3 million people.[32] Unidentified hackers were able to gain access to a server that contained sensitive member information, including names, mailing addresses, dates of birth, and details about health insurance plans.[33] Hackers angry about U.S. foreign policy called attention to their cause by breaching the U.S. Department of Justice's database and releasing data on 10,000 Department of Homeland Security employees one day and then releasing data on 20,000 FBI employees the next day.[34]

Large companies are responding to these threats; the cybersecurity industry collects approximately $75 billion annually.[35] Recent studies indicate, however, that hackers indiscriminately choose their victims[36] and small businesses have become frequent targets.[37] Over the last five years, attacks on businesses with 250 or fewer employees has increased.[38] As of mid-2016, one study reported that 43 percent of

28. Graham Cluley, *Hackers Steal $55 million From Boeing Supplier*, TRIPWIRE (Jan. 21, 2016), https://www.tripwire.com/state-of-security/security-data-protection/boeing-supplier-hacked-claims-55-million-worth-of-damage-as-stock-price-falls/.

29. Whitney Filloon & Brenna Houck, *Massive Chipotle Data Breach Affected Roughly 2,250 Restaurants*, EATER (May 30, 2017), https://www.eater.com/2017/4/26/15433866/chipotle-data-breach-credit-cards.

30. Elizabeth Weise, *Data breach hits 63,000 U. of Central Florida Students, Staff*, USA TODAY (Feb. 4, 2016, 11:17 AM), https://www.usatoday.com/story/tech/news/2016/02/04/data-beach-63000-university-of-florida-students-staff/79813904/.

31. Janet Gilmore, *Campus alerting 80,000 individuals to cyberattack*, BERKELEY NEWS (Feb. 26, 2016), http://news.berkeley.edu/2016/02/26/campus-alerting-80000-individuals-to-cyberattack/.

32. Robert Abel, *Newkirk Medical Records Breach Impacts 3.3M, Blue Cross Blue Shield Customers Affected,* SC MEDIA US (Aug. 8, 2016), https://www.scmagazine.com/unauthorized-individual-gains-access-to-a-server-containing-data-on-33m/article/528104/.

33. *Id.*

34. Mary Kay Mallonee, *Hackers Publish Contact Info of 20,000 FBI Employees*, CNN (Feb. 8, 2016, 8:34 PM), http://www.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/.

35. Steve Morgan, *Cybersecurity Market Reaches $75 Billion in 2015, Expected to Reach $170 Billion By 2020*, FORBES (Dec. 20, 2015, 3:01 PM), https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2 %80% 8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/#48e3724330d6.

36. SYMANTEC, INTERNET SECURITY THREAT REPORT 44 (2016), https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

37. *Id.* at 43.

38. *Id.* at 42.

cyber-attacks targeted small businesses.[39] Research on the cybersecurity in small and medium-sized businesses revealed that no business is small enough to evade a cyberattack or data breach.[40] Unfortunately, a smaller organization may not have the budget and in-house expertise to determine the cause of a breach and harden its systems and networks against potential threats.[41] All businesses, regardless of size, are faced with the growing probability of a breach by criminals who use more creative and complicated techniques.[42] However, larger businesses are better equipped to mitigate the risk and recover from a breach.[43]

B. Vulnerabilities of Small Business Data

Although most of the cyber breaches that make the headlines are from large companies, the breaches of smaller companies are far greater in number.[44] Small companies also hold valuable customer information.[45] Hackers regard the data systems at small businesses as "low-hanging fruit."[46]

Most cybercriminals seek personally identifiable information ("PII") for financial gain.[47] PII is any data that distinguishes one individual from another which, when disclosed, can result in harm to the individual whose privacy has been breached.[48] Surprising to some, medical PII is a key to a very profitable door that is

39. Joshua Sophy, *43 Percent of Cyber Attacks Target Small Business. Technology Trends*. SMALL BUS. TRENDS (Apr. 28, 2016), https://smallbiztrends.com/2016/04/cyber-attacks-target-small-business. html.

40. *See* PONEMON INST. LLC, 2016 STATE OF CYBERSECURITY IN SMALL & MEDIUM-SIZED BUSINESSES (SMB) (2016), http://www.triscal.com.br/shared/docs/seguranca-state_cybersecurity_ small_medium_ businesses-2016.pdf.

41. *Id.*

42. Paul Gordon, *Rise of The Cyber Criminals*, HUFFINGTON POST (Aug. 25, 2016, 7:50AM), https://www.huffingtonpost.com/entry/rise-of-the-cyber-criminals_us_57bed90ae4b06384eb3e60b9.

43. Disha Pandit, *Intricacies Involved with Cyber–Insurance*, CYBER SECURITY COMMUNITY (Nov. 2, 2017), https://securitycommunity.tcs.com/infosecsoapbox/articles/2017/11/02/intricacies-involved-cyber-insurance.

44. Rosalie L. Donlon, *Small, Mid-Sized Businesses Hit by 62% of All Cyber Attacks,* PROP. CASUALTY 360° (May 27, 2015, 5:20 AM), http://www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber?slreturn=1496753378.

45. Joseph Steinberg, *Small Businesses Beware: Half of all Cyber-Attacks Target You*, INC. (Mar. 21, 2017), https://www.inc.com/joseph-steinberg/small-businesses-beware-half-of-all-cyber-attacks-target-you.html.

46. Julie Knudson, *Small Business Security Trends You Need to Know*, SMALL BUS. COMPUTING (Feb. 23, 2016), https://www.smallbusinesscomputing.com/News/Security/small-business-security-trends-you-need-to-know.html.

47. Robert E. Holdfreter, *Cyber Criminals Step Up Their Games to Harvest PII*, FRAUD MAG. (Mar.-Apr. 2014), http://www.fraud-magazine.com/article.aspx?id=4294982013.

48. *See* U.S. DEP'T OF COMMERCE, SPECIAL PUBLICATION 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (2010), at ES-1.

worth much more to cyber criminals than banking PII.[49] Health records give cybercriminals information not just for fake medical claims but also for acquiring credit card accounts and mortgages.[50]

Despite good intentions, a doctor's office can be easy prey.[51] Through continuing education, board-certified physicians are well-informed about medical protocol, insurance coverage, and the Health Insurance Portability and Accountability Act ("HIPAA").[52] Apart from privacy concerns, which are beyond the scope of this article, medical and banking PII, desirable to hackers for financial gain, can be vulnerable in a small physician's office as the following example shows.

The physician shares the importance of protecting patient information with the small staff of nurses and office workers. Although the staff members know how to use computers, no one is formally educated in information technology or cybersecurity management. The practice has purchased licenses to access, through the Internet, a patient management system that interfaces with the major health insurance carriers. All programs and data are managed by the application service provider for the patient management system. At the direction of the application service provider, the physician's office connects to the patient management system via the Internet. All data is encrypted using the very secure asymmetric-key encryption method and includes digital signatures.[53] There is a computer in each examination room and each office cubicle. Each computer has a wireless Wi-Fi connection to the office router, which saves the cost of wiring and provides for flexibility in configuring the workspace. The office router provides each computer with a wireless connection to the Internet and the shared office printer through a password-protected, encrypted connection. The reception area includes a bank-provided credit card chip reader for processing examination fees.

Even though a cyber security audit of this business's technology infrastructure would be favorable, there are multiple risks of a breach. Exposure begins when a new

49. Justin Bonnema, *Why Cybercriminals Are After Your Identity*, SECURITY AWARENESS COMPANY (Nov. 9th, 2016), https://www.thesecurityawarenesscompany.com/2016/11/09/why-cybercriminals-are-after-your-identity/.

50. *Id.*

51. Dan Munro, *Data Breaches in Healthcare Totaled Over 112 Million Records in 2015*, FORBES (Dec. 31, 2015, 9:11 PM), https://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#74b9af4d7b07.

52. The Health Insurance Portability and Accountability Act is designed to protect the privacy of health care information. U.S. DEP'T OF HEALTH & HUMAN SERVS., HEALTH INFORMATION PRIVACY, SUMMARY OF HIPAA SECURITY RULE (2013), https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

53. The asymmetric-key encryption method that includes digital signatures is considered a preferred method for secure digital transmission of data. Margaret Rouse, *Asymmetric Cryptography (public key cryptography),* TECHTARGET (June 2016), http://searchsecurity.techtarget.com/definition/ asymmetric-cryptography.

patient first visits the practice. This patient completes a set of forms that require personal information such as social security number, credit card numbers, driver's license information, contact details, health insurance information, personal and family medical history, and employment information. The physician refers to the paper document during the initial examination. After the visit, an office worker keys the patient's information into the patient management system. The original papers are scanned, saved electronically in an encrypted format, and then shredded. All seems safe.

What if the office is busy with pressing patient needs? Keying new patient data into the patient management system is not considered a priority task since the patient has already been examined. New patient forms are kept in a neat pile on the office worker's desk awaiting processing. Anyone with physical access to the forms--another staff member, a delivery person, or another patient--can take one or more forms and have access to the PII. An office worker could take the forms to lunch or home to 'catch up' on work. The office worker keys in patient information while eating lunch in an open-access network café. Also in the café is a hacker eavesdropping through a man-in-the-middle attack on café customers.[54] The hacker mechanically records all data entered by the officer worker in addition to all of the lunch transactions. The hacker sips coffee and blends into the customer base as a device surreptitiously collects information.

The doctor's office computers connect to the Internet through a password-enabled Wi-Fi router. The password was initially established as the office phone number and never changed. This password is convenient because it is easy to remember. The staff is not aware of the steps to change the password. As a result, all computers in the office connect to the Wi-Fi with the same password. Sometimes the waiting room fills with anxious patients who bring their smart phones and tablets to pass the time. The patients see the staff using the office Wi-Fi and ask for the password. The receptionist knows most, if not all, the patients and sees no harm in sharing the Wi-Fi password. Unwittingly, a patient may provide a point of entry to the physician's computer network through his or her compromised device. Over time, the router's password becomes meaningless protection. Wi-Fi access provides an entry into the local network, the patient management system, and credit card payment system.

Finally, a group of cyber criminals generates an impressive impersonation of an email from an insurance company. The company logo and contact name is digitally copied from the insurance company website. A list of small physician practices and contact information is gathered from a physician listing website. The cyber criminals

54. A man-in-the-middle ("MITM") attack is a form of eavesdropping where communication between two devices is monitored by an unauthorized party. The purpose of the interception can be to modify then resend the message, or just gather information from the message. *Man-in-the-Middle Attack (MITM)*, TECHNOPEDIA, https://www.techopedia.com/definition/4018/man-in-the-middle-attack-mitm (last visited Feb. 8, 2018).

create a phishing cyber-attack by mechanically issuing emails to the small physician practices that look as though they are generated from an insurance company. The emails direct the office managers to apply for the new payment system. The link in the email is very convincing because it displays the actual web address of the insurance company. Clicking on the link brings the user to the cyber criminals' website. The office worker is not suspicious because the site requests publicly available information about the physician's office. But, the site also installs key-logging software that records all activities made on the office worker's computer. This places all financial and PII of the practice in jeopardy. Reports of security breaches show that most do not result from clever attackers discovering new kinds of flaws, but rather from repeated tries of well-known hacks.[55] There are many avenues for attack at this physician's office. The physician and the employees can access the application service provider to record patient records at home. Their devices at home may not have been updated with the latest operating system security fixes. Typically, there is a flood of breaches following the announcement of an operating system fix since many users do not regularly apply updates. The employee's home network may not be secure, so anyone can mechanically eavesdrop on digital activity. Employees may be using their own devices filled with applications from unknown developers. The applications may seem interesting to use but contain trap doors for collecting data. The patients' PII is only as secure as the weakest link in this chain of activities.

C. Preparedness Comparison—Large and Small Businesses

Why is it easier to hack a small business? There is a vast difference in the cybersecurity management of large and small businesses specifically in managerial perception, employee expertise, regulatory compliance, and technology infrastructure.[56] Small businesses often believe they are safe from cyberattacks because of a perception that they don't have anything worth stealing.[57] However, small businesses have information valuable to cybercriminals including employee and customer PII and intellectual property.[58] In addition, small businesses provide access to larger networks such as supply chains.[59] Given their role in the nation's

55. David Bisson, *Takeaways from the 2016 Verizon Data Breach Investigations Report*, TRIPWIRE: STATE OF SECURITY (Apr. 28, 2016), https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/takeaways-from-the-2016-verizon-data-breach-investigations-report/David Bisson.

56. JUHEE KWON & M. ERIC JOHNSON, *Healthcare Security Strategies for Regulatory Compliance and Data Security*, 30 J. MGMT. INFO. SYS. 41 (2013).

57. SYMANTEC, *supra* note 36, at 36.

58. Michael Kemps & Kimberly Pease, "*Information Security: The Human Factor*" LAW J. NEWSL. (Apr. 2017), http://www.lawjournalnewsletters.com/sites/lawjournalnewsletters/2017/04/01/ information-security-the-human-factor/.

59. Daniel Clapper & William Richmond, *Small Business Compliance with PCI DSS*, 19.1 J. MGMT. INFO. & DECISION SCI. 54, 56 (2016).

supply chain and economy and their limited resources to secure their information, systems, and networks, small businesses are attractive targets for cybercriminals.[60]

Large businesses hire information security analysts who have the expertise to develop, implement, and maintain cybersecurity management systems.[61] Demand will continue to be high for information security analysts who create innovative solutions to prevent hackers from stealing information or interfering with computer networks.[62] Employment of information security analysts is projected to grow 18 percent from 2014 to 2024, much faster than the average for all occupations.[63] Information security analysts are employed by large, not small, organizations.[64]

Most small firms lack funds or personnel to dedicate to cybersecurity.[65] Establishing a secure cyber environment is difficult for small businesses because of the financial burden of implementing security techniques and the inadequate technology skills of their employees.[66] The typical owner focuses on the product or service that the business provides and does not have extra time or money for cybersecurity challenges, even if a breach could mean the death of the business.[67]

A variety of compliance laws and regulations address cybersecurity protection and large corporations employ dedicated experts to address these obligations.[68] The Sarbanes-Oxley Act ("SOX") of 2002 requires publicly-traded firms to report material deficiencies in financial reporting processes.[69] While information security is not specifically discussed, modern financial reporting systems are heavily dependent on technology and associated controls.[70] Sections 302 and 404 indirectly force scrutiny of information security controls.[71] A review of internal controls must

60. *Introduction to Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/content/ introduction-cybersecurity (last visited Feb. 24, 2018).

61. *How to Become an Information Security Analyst*, NEW HORIZONS COMPUTER LEARNING CTR., https://www.omahanh.com/solutions/career-solutions/information-security-analyst (last visited Feb. 24, 2018).

62. *Information Security Analysts,* U.S. BUREAU OF LAB. STAT., OFF. OF OCCUPATIONAL STAT. & EMP. PROJECTION, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm (last visited Feb. 24, 2018).

63. *Id.*

64. *Id.*

65. Daniel Clapper & William Richmond, *Small Business Compliance with PCI DSS*, 19.1 J. MGMT. INFO. & DECISION SCI. 54, 55 (2016).

66. *Id.*

67. Rob Marvin, *10 Cybersecurity Steps Your Small Business Should Take Right Now*, PC MAG. (May 2, 2016, 4:37 PM), http://www.pcmag.com/article/344181/10-cybersecurity-steps-your-small-business-should-take-righ.

68. *See infra* notes 69–80.

69. 15 U.S.C. § 7213(a)(2)(A)(iii)(III) (2012).

70. *An Overview of Sarbanes-Oxley for the Information Security Professional*, SANS INST. (2004), https://www.sans.org/reading-room/whitepapers/legal/overview-sarbanes-oxley-information-security -professional-1426.

71. 15 U.S.C. §§ 7241, 7262 (2012).

address information security.[72] An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or data manipulation.[73] A corporation may also need to address privacy protection laws including the HIPPA.[74] The Federal Trade Commission can issue fines and require external auditing for several years for companies that fail to protect private information.[75] Large organizations typically employ a chief security officer or chief information security officer who has formal training as an information security analyst to address legal and compliance issues.[76]

Businesses may also choose to follow standards in order to participate in various business arrangements. For example, the Payment Card Industry–Data Security Standards ("PCI-DSS") includes 12 general requirements for secure processes for firms that accept credit card payment.[77] Although not covered by SOX, privately held businesses, even small businesses are required to comply with privacy protection laws and must comply with PCI-DSS if they choose to accept credit cards.[78] However, employees of the small businesses do not have information security analyst expertise.[79] Most small business owners value technology and recognize its importance to the growth of their businesses, but are concerned about their own lack of knowledge and the unaffordability of technology resources.[80] Over 40 percent of small businesses report being ill-prepared to establish cybersecurity.[81]

An organization's IT infrastructure includes all of the hardware devices, operating systems, application code, network resources, procedures, and personnel

72. CELIA PAULSON & PATRICIA TOTH, SMALL BUSINESS INFORMATION SECURITY: THE FUNDAMENTALS 1 (Nov. 2016), https://doi.org/10.6028/NIST.IR.7621r1.

73. *An Overview of Sarbanes-Oxley for the Information Security Professional*, SANS INST. (2004), https://www.sans.org/reading-room/whitepapers/legal/overview-sarbanes-oxley-information-security-professional-1426.

74. Leuan Jolly, *Data Protection in the United States: Overview*, THOMSON REUTERS PRAC. L. (July 1, 2017), https://uk.practicallaw.thomsonreuters.com/6-502-0467?transitionType=Default&bhcp=1&contextData=(sc.Default)&firstPage=true.

75. FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2016 3 (Jan. 2017), https://www.ftc.gov/reports/privacy-data-security-update-2016.

76. Nader Mehravari & Julia Allen, *Structuring the Chief Information Security Officer (CISO)*, SOFTWARE ENG'G INST. CARNEGIE MELLON UNIVERSITY (Feb. 22, 2016), https://insights.sei.cmu.edu/sei_blog/2016/02/structuring-the-chief-information-security-officer-ciso-organization.html.

77. PCI SECURITY STANDARDS COUNCIL, PCI DSS QUICK REFERENCE GUIDE 8 (2010), https://www.pcisecuritystandards.org/documents/PCI%20SSC%20Quick%20Reference%20Guide.pdf.

78. *Id.*

79. Sarah Shemkus, *Growing Skills Gap: 80% of Small Businesses Can't Find Qualified Staff*, GUARDIAN (June 22, 2015), https://www.theguardian.com/sustainable-business/2015/jun/22/skills-gap-small-business-qualified-staff.

80. Michael Chmura, *The State of Small Business in America 2016*, BABSON (June 7, 2016), http://www.babson.edu/news-events/babson-news/Pages/2016-state-of-small-business-in-america-report.aspx.

81. *Id.*

necessary to operate its computer systems.[82] These multiple physical, logical, and human components are uniquely integrated to support business processes.[83] Since cybersecurity vulnerabilities can be found anywhere--in the network, hosts, access points, application code, and user procedures--a comprehensive plan is necessary to secure the data as it travels through the IT architecture to its final destination.[84] Regardless of their size, businesses need to protect their technology infrastructure from unauthorized, malicious events.[85] Comprehensive security closes all routes of attack found in the network, hosts, access points, application code, and user procedures. Governance frameworks like COBIT ("Control Objectives for Information and Related Technologies") provide guidelines and directions for establishing centralized security management that considers border and internal site management, control of remote connections, and inter-organizational systems with other firms.[86]

Security professionals recommend that a business adopt a defense-in-depth approach which protects resources with several safeguards.[87] An attacker must breach all countermeasures in the series to succeed.[88] Implementing security policy with a defense-in-depth approach is complex and demands unique skills and knowledge for risk mitigation and incident response.[89] An important component of the technology infrastructure is accessing the Internet.[90] This raises multiple security issues.[91] A business could elect to have a permanent connection to the Internet and

82. DAVID T. BOURGEOIS, INFORMATION SYSTEMS FOR BUSINESS AND BEYOND Ch. 1.1 (Pressbooks, 2014) (ebook).

83. *IT Infrastructure*, TECHNOPEDIA https://www.techopedia.com/definition/29199/it-infrastructure (last visited Feb. 15, 2018).

84. *See* CATHERINE PAQUET, IMPLEMENTING CISCO IOS NETWORK SECURITY (IINS 640-554) FOUNDATION LEARNING GUIDE (Cisco Press, 2d ed. 2013) (ebook) ("Therefore, detective controls are aslo part of a comprehensive security program because they enable you to detect a security breach and to determine how the network was breached.").

85. Chmura, *supra* note 80.

86. *See generally* ISACA, IS STANDARDS, GUIDELINES AND PROCEDURES FOR AUDITING AND CONTROL PROFESSIONALS (Jan. 15, 2009), https://obamawhitehouse.archives.gov/files/documents/ cyber/ISACA%20-%20IS%20Standards,%20Guidelines,%20and%20Procedures%20for%20Auditing %20and%20Control%20 Professionals.pdf.

87. Chad Perrin, *Understanding layered security and defense in depth*, TECH REPUBLIC (Dec. 18, 2008, 6:05 AM) https://www.techrepublic.com/blog/it-security/understanding-layered-security-and-defense-in-depth/.

88. *Id.*

89. Lance Hayden, *Security is More than a Process…It's a proficiency*, CSO ONLINE (Dec. 11, 2015, 9:22 AM), http://www.csoonline.com/article/3013714/security/security-is-more-than-a-process-its-a-proficiency.html.

90. *IT Infrastructure*, TECHOPEDIA https://www.techopedia.com/definition/29199/it-infrastructure (last visited Feb. 15, 2018).

91. Wired Staff, *The Biggest Security Threats Coming in 2017*, WIRED (Jan. 2, 2017, 7:00 AM) https://www.wired.com/2017/01/biggest-security-threats-coming-2017/; *see generally Top 10 Threats to*

privately allocate internal IP addresses[92] to computer devices. Special routers can be established to include mapping information so that outsiders are not able to determine the address of key employee equipment.[93] Businesses that elect to connect to the Internet through an Internet Service Provider are allocated IP addresses.[94] In this case, the IP address associated with the routers and employee devices is accessible to the Internet.[95]

Secure management of access control should include two factor authentication and management of an access control list.[96] Two factor authentication requires the purchase and distribution of special equipment--like secure ID cards--to all employees.[97] It also includes the assignment of unique usernames and passwords for each employee.[98] The access control list provides the appropriate levels of security access to the many systems and file directories in an organization.[99] This complex process requires at least one, and often several, IT professionals to manage access to company technology resources.[100] A business may opt for a more economical option. Access control may use single factor authentication that includes the assignment of a unique username and password to each employee and does not implement access control list management.[101]

Information Security, GEORGETOWN UNIV., https://scsonline.georgetown.edu/programs/ masters-technology-management/resources/top-threats-to-information-technology (last visited Feb. 15, 2018).

92. An *IP address* (abbreviation of Internet Protocol address) is an identifier assigned to each computer and other device (e.g., printer, router, mobile device, etc.) to connect to the Internet. The address is used to locate and identify the device in communications with other devices on the Internet. *See* Stephanie Crawford & Howstuffworks.com, *What is an IP Address*, HOWSTUFFWORKS (Jan. 12, 2001), https://computer.howstuff works.com/internet/basics/question549.htm.

93. DEP'T OF HOMELAND SECURITY INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM, RECOMMENDED PRACTICE: IMPROVING INDUSTRIAL CONTROL SYSTEM CYBERSECURITY WITH DEFENSE-IN-DEPTH STRATEGIES 10, 36, 41, 43 (Sept. 2016), https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/ NCCIC_ICS-CERT_ Defense_in_Depth_2016_S508C.pdf.

94. *About Static IP addresses*, AT&T https://www.att.com/esupport/article.html#!/u-verse-high-speed-internet/KM1002300 (last visited Feb. 15, 2018).

95. *Id.*

96. *2FA / Two Factor Authentication – How it Works in Access Control*, KISI, https://www.getkisi.com/ technologies/2fa-access-control (last visited Feb. 15, 2018).

97. *Id.*; *see also Two-Factor Authentication (2FA) Solutions*, GEMALTO, https://safenet.gemalto. com/multi-factor-authentication/two-factor-authentication-2fa/ (last visited Feb. 15, 2018).

98. *Two-Factor Authentication (2FA) Solutions*, *supra* note 97; *see also 2FA / Two Factor Authentication – How it Works in Access Control*, *supra* note 96.

99. Matthew Schartz, *Access Control: 10 Best Practices*, ENTER. SYS. J. (Mar. 27, 2007), https://esj.com/ articles/2007/03/27/access-control-10-best-practices.aspx.

100. *Id.*

101. Margaret Rouse, *Single-factor Authentication*, TECHTARGET (Mar. 2, 2017), http://searchsecurity. techtarget.com/definition/single-factor-authentication-SFA.

Several intrusion detection systems are available that look for anomalies in network traffic and alert information security professionals to possible breaches.[102] These tools automatically record network activities then feed data into analytics software for analysis.[103] The data analytics software provides reports of anomalies in network traffic for investigation by the security professional.[104] A business can discover an intrusion early and possibly mitigate the damage.[105] This type of protection is only common in large businesses.[106]

Recognizing the cybersecurity risk to both their financial prospects and company brands, large businesses invest in security governance frameworks and employ professionally trained individuals to establish an IT infrastructure that can withstand increasingly complex cyber threats.[107] Small businesses have neither the economic resources nor the in-house expertise to establish a secure cybersecurity infrastructure.[108] Small businesses have less robust security in every aspect of the IT architecture.[109] As a result, cybercriminals often target small businesses because their information technology infrastructure is easier to penetrate.[110]

II. THEORIES OF LIABILITY

Businesses targeted by third-party hackers have found themselves in litigation with their customers and state regulators.[111] Although the cybercriminal caused the damage, the business is alleged to be responsible for failing to prevent it.[112] Plaintiffs with compromised data have been testing a variety of legal theories around the country with some success.[113] Some courts have been reluctant to impose liability,

102. Tony Bradley, *Introduction to Intrusion Detection Systems (IDS)*, LIFEWIRE (Aug. 13, 2017), https://www.lifewire.com/introduction-to-intrusion-detection-systems-ids-2486799.

103. *Id.*

104. *Id.*

105. *Targeted Cyber Intrusion Detection and Mitigation Strategies*, INDUS. CONTROL SYS. CYBER EMERGENCY RESPONSE TEAM (Feb. 6, 2013), https://ics-cert.us-cert.gov/tips/ICS-TIP-12-146-01B.

106. *Cost and Value of Cyber Security*, FIREEYE https://www.fireeye.com/current-threats/tco.html (last visited on Feb. 13, 2018).

107. James Kaplan, Shantnu Sharma & Allen Weinberg, *Meeting the Cybersecurity Challenge*, MCKINSEY & COMPANY (June 2011), https://www.mckinsey.com/business-functions/digital-mckinsey/ our-insights/meeting-the-cybersecurity-challenge.

108. Commissioner Luis A. Aguilar, *The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses*, U.S. SEC. AND EXCH. COMM'N (Oct. 19, 2015), https://www.sec. gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html.

109. *Id.*

110. Donlon, *supra* note 44.

111. *See infra* Parts II.A, II.B, II.C.

112. *See infra* Parts II.A, II.B, II.C.

113. *See infra* Parts II.A, II.B, II.C..

but a data breach leaves a business owner legally vulnerable.[114] Plaintiffs able to clear the hurdle of standing have had a number of theories of liability accepted in one or more jurisdictions.[115]

A. Standing

The first line of defense against a breach-victims suit has been Article III standing. Business owners argue that the plaintiffs have not sustained "an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical."[116] This argument does not go far when stolen data has already been misused.[117] When no misuse has yet followed the theft, however, plaintiffs have had difficulty convincing some courts they have sufficient injury to support standing.[118]

If a fraudulent occurrence closely follows a hacking event, most courts agree that the defrauded plaintiff has standing.[119] A common scenario is stolen credit card information resulting in "unlawful charges, restricted or blocked access to bank accounts, inability to pay other bills, and late payment charges or new card fees."[120] Another recurring example is when the hacker or an accomplice files a false tax return using stolen personal information to obtain a fraudulent refund.[121]

The real disagreement is whether plaintiffs whose information was hacked have standing when the data has not yet been put to dishonest use.[122] Some courts say the increased risk alone of identity theft and harm is sufficient injury for standing

114. *See infra* Parts II.A, II.B, II.C.

115. *See infra* Parts II.A, II.B, II.C.

116. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992).

117. *Id.* at 559.

118. *Id.* at 563–64 (discussing the lack of an "imminent" injury or who hasn't been "directly" affected yet is not sufficient for standing).

119. Hapka v. CareCentrix, Inc., No. 16-2372, 2016 U.S. Dist. LEXIS 175346, at *5–7 (D. Kan. Dec. 19, 2016) (finding that allegations of future harm must be taken in light of tax fraud that already happened); *In re* Cmty. Health Sys., Inc., No. 15-CV222-KOB, 2016 U.S. Dist. LEXIS 123030, at *40–41 (N.D. Ala. Sept. 12, 2016); Smith v. Triad of Alabama, LLC, No. 1:14-CV-324-WKW, 2015 U.S. Dist. LEXIS 130935, at *3–4 (M.D. Ala. Sept. 29, 2015); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1158–59 (D. Minn. 2014); Strautins v. Trustwave Holdings, Inc., 27 F. Supp. 3d 871, 876–77 (N.D. Ill. 2014).

120. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014).

121. Brush v. Miami Beach Healthcare Grp., Ltd., 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017); Hapka v. CareCentrix, Inc., No. 16-2372-CM, 2016 U.S. Dist. LEXIS 175346, at *5–7 (D. Kan. Dec. 19, 2016); Welborn v. IRS, 218 F. Supp. 3d 64, 77 (D.D.C 2016); *In re* Anthem Data Breach Litig., 162 F. Supp. 3d 953, 987 (N.D. Cal. 2016); Burrows v. Purchasing Power, LLC, No. 1:12-CV-22800-UU, 2012 U.S. Dist. LEXIS 186556, at *8–9 (S.D. Fla. Oct. 18, 2012).

122. *See Strautins*, 27 F. Supp. 3d at 878 (showing the disagreement between courts on whether there is standing when information has been hacked but an injury has not occurred yet).

purposes.[123] Others hold that as long as one plaintiff was defrauded, then other victims of the same hack have sufficient reason to fear imminent harm.[124] A third group rejects increased risk of harm as too speculative.[125]

Since a number of courts have declined to recognize standing based on fear of increased risk of harm, plaintiffs have attempted a number of other creative theories of economic harm. The stress and time associated with canceling and replacing credit cards with the attendant loss in productivity have been accepted to confer standing.[126] Other types of damages gaining acceptance include benefit of the bargain damages, loss of value of personal information, consequential out-of-pocket damages,[127] unjust enrichment (based on the failure to use payments to protect data in accordance with a privacy notice[128] or on a would-not-have-patronized the business theory),[129] and overpayment for a product that did not include the reasonable security the company represented it would provide.[130] The overpayment theory—that the price plaintiffs paid for the product or service was supposed to, but did not, include protection of their data—has met skepticism in retail store cases because customers who paid cash and provided no personal information paid the same price as the credit card

123. "[I]t is plausible to infer that the plaintiffs have shown a substantial risk of harm from the Neiman Marcus data breach. Why else would hackers break into a store's database and steal customers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities." Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 693 (7th Cir. 2015). *See also* Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016); Krottner v. Starbucks Corp., 628 F.3d 1139, 1142–43 (9th Cir. 2010); Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007).

124. Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *17 (N.D. Ill. July 14, 2014).

125. Reilly v. Ceridian Corp., 664 F.3d 38, 44–46 (3d Cir. 2011); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 753 (W.D.N.Y. 2017); *In re* Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *34–38 (N.D. Ala. Sept. 12, 2016); Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 U.S. Dist. LEXIS 89992, at *10–22 (E.D. Mo. July 12, 2016); Torres v. Wendy's Co., 195 F. Supp. 3d 1278, 1283 –84 (M.D. Fla. 2016); Khan v. Children's Nat'l Health Sys., 188 F. Supp. 3d 524, 531 (D. Md. 2016); Alonso v. Blue Sky Resorts, LLC, 179 F. Supp. 3d 857, 863–65 (S.D. Ind. 2016) (holding that no "concrete, particularized injury" or "future injury…certainly impending;" "cannot manufacture standing by incurring costs in anticipation of a non-imminent harm"); *In re* Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 25–26 (D.D.C. 2014).

126. Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *18–20 (S.D. Cal. Nov. 3, 2016).

127. *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594, at *123 (N.D. Cal. May 27, 2016). *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1204 (D. Or. 2016).

128. Resnick v. AvMed, Inc., 693 F.3d 1317, 1328 (11th Cir. 2012); Weinberg v. Advanced Data Processing, Inc. 147 F. Supp. 3d 1359 (S.D. Fla. 2015). *See In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d at 1204.

129. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1178 (D. Minn. 2014); *In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d at 1204.

130. *In re* Adobe Sys., Inc. Privacy Litig., 66 F. Supp. 3d 1197, 1224 (N.D. Cal. 2014); *see In re Premera Blue Cross Customer Data Sec. Breach Litig.*, 198 F. Supp. 3d at 1204.

customers.[131] A loss of privacy or breach of confidentiality, unaccompanied by economic harm, was considered insufficient to confer standing in a case involving personal identification information.[132]

B. Contract and Related Claims

Courts fearing unlimited liability have been more receptive to claims sounding in contract.[133] The benefit of contract and related claims is that they require privity.[134] If a business owner promised to protect customer data, why should the courts hesitate to enforce the bargain?

1. Breach of Written Contract

Cases involving written contracts generally seek to incorporate a privacy policy or other document relating to data security into the written agreement.[135] When a description of privacy obligations is one of the clauses of the agreement or is physically attached to the contract, it will be enforced as part of the contract.[136] More commonly, the question is whether contracts incorporate separate privacy notices and policies by reference.[137] Assuming there is a contractual duty, the plaintiff must

131. Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 754 (W.D.N.Y. 2017), *rev'd in part on reconsideration sub nom.* No. 6:15-CV-06569 EAW, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018); *In re* Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *27–31 (N.D. Ala. Sept. 12, 2016); Duqum v. Scottrade, Inc., No. 4:15-CV-1537-SPM, 2016 WL 3683001, at *6 (E.D. Mo. July 12, 2016), *aff'd sub nom.* Kuhns v. Scottrade, Inc., 868 F.3d 711 (8th Cir. 2017); Carlsen v. GameStop, Inc., 112 F. Supp. 3d 855, 861 (D. Minn. 2015), *aff'd on other grounds*, 833 F.3d 903 (8th Cir. 2016).

132. *Duqum*, 2016 WL 3683001, at *8.

133. *See, e.g.*, Kuhns v. Scottrade, Inc., 868 F.3d 711, 716 (8th Cir. 2017).

134. *Id.*

135. *In re* Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *75–80 (N.D. Ala. Sept. 12, 2016); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1197–98 (D. Or. 2016) (dismissing contract claim with leave to replead to allege privacy notices and policies were incorporated by reference into health benefits contracts).

136. *In re* Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 U.S. Dist. LEXIS 70594, at *151–55 (N.D. Cal. May 27, 2016). Absent a contract between the plaintiff and defendant, courts have been reluctant to attach liability based on a third-party beneficiary theory. *Id.*; *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 577–81 (S.D. Tex. 2011), *rev'd in part sub nom.* Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013). Plaintiffs must show they were intended third-party beneficiaries. *Id.*; Cmty. Bank of Trenton v. Schnuck Mkts., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *15–16 (S.D. Ill. May 1, 2017); Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 767–69 (W.D.N.Y. 2017), *rev'd in part on reconsideration sub nom.* No. 6:15-CV-06569 EAW, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018).

137. *Fero*, 236 F. Supp. 3d at 760–61; *In re Anthem, Inc. Data Breach Litig.*, U.S. Dist. LEXIS 70594, at *109–22.

also demonstrate how the defendant breached it, which generally takes the form of failing to implement reasonable security measures.[138]

2. Implied contract

Some courts have sustained a claim that an implied contract exists obligating the defendant to protect the personal information of the plaintiff.[139] An implied contract requires a direct contractual relationship between plaintiff and defendant.[140] Courts may not find a contract implied when there is no offer and acceptance[141] or ascertainable intent to enter into a contract.[142] Like express contracts, implied contracts require consideration in both directions.[143] For a claim to survive, there must also be actual economic damage, at least where the theft involves identity information.[144]

138. *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) (holding that in a contract requiring defendant to "use security measures that comply with federal law," plaintiffs failed to allege what law defendant violated).

139. *Compare* Enslin v. Coca-Cola Co., 136 F. Supp. 3d 654, 675 (E.D. Pa. 2015) ("Through privacy policies, codes of conduct, company security practices, and other conduct, implicitly promised to safeguard [personal information] in exchange for [plaintiff's] employment . . . Plaintiff has fairly alleged the existence of an agreement between the parties that included a covenant by the Coke Defendants to protect Plaintiff's [personal information], which Plaintiff alleges that the Coke Defendants breached."), *with* Longenecker-Wells v. Benecard Servs. Inc, 658 F. App'x 659, 662 (3d Cir. 2016) ("Plaintiffs have failed to plead any facts supporting their contention that an implied contract arose between the parties other than that Benecard required Plaintiffs' personal information as a prerequisite to employment. This requirement alone did not create a contractual promise to safeguard that information, especially from third party hackers."). Breach of implied warranty claims have been less common. In the Sony Gaming Networks litigation, common law breach of implied warranty claims were dismissed because the written contract disclaimed implied warranties. *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 980–84 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014). Statutory implied warranty claims in the same litigation were dismissed because the services provided were not "goods" under the Uniform Commercial Code. *Id.*

140. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 582–83 (S.D. Tex. 2011), *rev'd in part sub nom*. Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013).

141. Cmty. Bank of Trenton v. Schnuck Mkts., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *13 (S.D. Ill. May 1, 2017).

142. Dittman v. UPMC, 154 A.3d 318, 325–26, (Pa. Super. Ct. 2017), *appeal granted*, 170 A.3d 1042 (Pa. 2017).

143. *Dittman*, 154 A.3d at 326.

144. Moyer v. Michaels Stores, Inc., No. 14 C 561, 2014 U.S. Dist. LEXIS 96588, at *20–21 (N.D. Ill. Jul. 14, 2014).

3. Unjust Enrichment

Unjust enrichment is another claim that has been successfully asserted.[145] This has been explained in several ways, but the most common are the overpayment and would-not-have-shopped theories.[146] The overpayment argument is that plaintiff paid a price that included steps to guard personal information.[147] The problem in the retail store setting, like for the overpayment theory in the standing cases, is that credit card customers pay the same price as cash customers who provide no personal data to the store.[148] The argument that fared better in the *Target* litigation was that the store was unjustly enriched because customers would not have shopped at the store had they known about poor data security.[149]

C. Negligence

Negligence seems like a natural fit. What all data security plaintiffs are essentially alleging is: "If only the defendant business had taken reasonable security measures, the hacker-thief would have been unable to obtain our personal identification information and we would not have been injured." Some courts have permitted such claims.[150] A negligence claim, of course, requires (1) duty; (2) breach of duty; (3) causation; and (4) injury.[151] Courts reluctant to impose tort duties in new situations

145. Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 769–70 (W.D.N.Y. 2017), *rev'd in part on reconsideration sub nom.* No. 6:15-CV-06569 EAW, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018); Cmty. Bank of Trenton v. Schnuck Mkts., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *22 (S.D. Ill. May 1, 2017); *In re* Cmty. Health Sys., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *81–82 (N.D. Ala. Sept. 12, 2016); *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1200–01 (D. Or. 2016); Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1368–69 (S.D. Fla. 2015); *In re* Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177–78 (D. Minn. 2014). *But see* Carlsen v. GameStop, Inc., 112 F. Supp. 3d 855, 864–65 (D. Minn. 2015), *aff'd on other grounds*, 833 F.3d 903 (8th Cir. 2016); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 984–85 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

146. *See, e.g.*, *In re* Target Corp., 66 F. Supp. 3d at 1178 ("This theory contends that, had Target notified its customers about the data breach in a timely manner, Plaintiffs would not have shopped at Target and thus any money Plaintiffs spent at Target after Target knew or should have known about the breach is money to which Target is not entitled.").

147. *Id.* ("Target charges all shoppers the same price for the goods they buy whether the customer pays with a credit card, debit card, or cash.").

148. *Id.* at 1177–78; *Cmty. Bank of Trenton*, 2017 U.S. Dist. LEXIS 66014, at *22.

149. *In re* Target Corp., 66 F. Supp. 3d at 1177–78.

150. *In re* Target Corp. Customer Data Sec. Breach Litig., 309 F.R.D. 482, 487–88 (D. Minn. 2015) (holding classwide proof established elements of prima facie case of negligence).

151. *See, e.g.*, Zimmerman v. Norfolk S. Corp., 706 F.3d 170, 189 (3d Cir. 2013) ("The well-worn elements of common-law negligence are, of course, duty, breach, causation, and damages."); Wright v. House of Imports, Inc., 381 S.W.3d 209, 213 (Ky. 2012); Brown v. Brown, 739 N.W.2d 313, 316–17 (Mich. 2007).

reject an expansion into the data breach area based on a variety of failures to meet these elements.[152]

1. Duty

Courts recognizing a duty to protect personal identification information from cyber thieves reason that because "harm was foreseeable, defendant had the duty to exercise reasonable care to prevent that harm."[153] According to a federal district court in California, such a duty was supported by both state law and "common sense."[154] Imposing a duty was ruled appropriate pursuant to the "undertaker's doctrine"—defendant voluntarily agreed to provide services and take the confidential information; therefore, defendant assumed a duty to act carefully and not put plaintiff at risk of harm.[155] One court even said, despite a growing list of authorities to the contrary,[156] that it is "well established that entities that collect sensitive, private data from consumers and store that data on their networks have a duty to protect that information…"[157]

Other courts are hesitant to impose liability for the criminal act of an unknown third party. They say that state legislatures could have permitted private negligence actions when they passed data breach notification laws, but since they did not, they made an affirmative election not to impose such a duty.[158] Courts worry about the

152. *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 636–37 (7th Cir. 2007).

153. Hapka v. CareCentrix, Inc., No. 16-2372-CM, 2016 U.S. Dist. LEXIS 175346, at *13 (D. Kan. Dec. 19, 2016).

154. "Although neither party provided the Court with case law to support or reject the existence of a legal duty to safeguard a consumer's confidential information entrusted to a commercial entity, the Court finds the legal duty well supported by both common sense and California and Massachusetts law. . . As a result, because Plaintiffs allege that they provided their Personal Information to Sony as part of a commercial transaction, and that Sony failed to employ reasonable security measures to protect their Personal Information, including the utilization of industry-standard encryption, the Court finds Plaintiffs have sufficiently alleged a legal duty and a corresponding breach." *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014), *order corrected*, No. 11MD2258 AJB (MDD), 2014 WL 12603117 (S.D. Cal. Feb. 10, 2014).

155. Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1366 (S.D. Fla. 2015).

156. Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 636–37 (7th Cir. 2007); Cmty. Bank of Trenton v. Schnuck Mkts., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *6–7 (S.D. Ill. May 1, 2017); *In re* Anthem, Inc. Data Breach Litig., 162 F. Supp. 3d 953, 975–976 (N.D. Cal. 2016); Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1054 (E.D. Mo. 2009); Dittman v. UPMC, 154 A.3d 318, 323–24, (Pa. Super. Ct. 2017), *appeal granted*, 170 A.3d 1042 (Pa. 2017); Steven L. Caponi, *Data Breach Negligence Claims Not Recognized in Pennsylvania*, 27 INTELL. PROP. & TECH. L. J. 22, 23 (2015). *See* Alonso v. Blue Sky Resorts, LLC, 179 F. Supp. 3d 857, 865–66 (S.D. Ind. 2016), *appeal dismissed sub nom.* (May 16, 2016).

157. Brush v. Miami Beach Healthcare Grp. Ltd., 238 F. Supp. 3d 1359, 1365 (S.D. Fla. 2017).

158. *Pisciotta*, 499 F.3d at 636–37 (denying class certification where plaintiffs sought to hold banking institution liable for a third-party hacking breach of their personal information because there was no injury present); *Cmty. Bank of Trenton*, 2017 U.S. Dist. LEXIS 66014, at *15–16; *Anthem Inc.*, 162 F. Supp. 3d at 975–76; *Amburgy*, 671 F. Supp. 2d at 1054; *Dittman*, 154 A.3d at 323–24; Caponi, *supra* note 156, at 23 (2015). *See Blue Sky Resorts*, 179 F. Supp. 3d at 865–66.

limits of a duty of care imposed on a defendant not directly related to a plaintiff.[159] Nor do they want to upset an allocation of liability agreed upon by the parties in a contract.[160] In Pennsylvania, courts raised public policy concerns about jurors deciding what was reasonable care in the data security context[161] and the legal system interfering with employers electronically storing information.[162]

2. Breach of duty

How to allege the breach of duty is another area of contention.[163] For some courts, the cyber invasion is enough on its own.[164] An intermediate position is that a bare allegation that "defendant breached its duty to implement adequate cybersecurity precautions" is sufficient to survive a motion to dismiss.[165] The most stringent rule is that it is not enough to highlight deficiencies in a cybersecurity system; plaintiffs have to show how the system failed to meet the applicable standard of care.[166]

159. Willingham v. Glob. Payments, Inc., No. 1:12-CV-01157-RWS-JFK, 2013 U.S. Dist. LEXIS 27764, at *61 (N.D. Ga. Feb. 5, 2013).

160. Digital Fed. Credit Union v. Hannaford Bros. Co., No. BCD-CV-10-4, 2012 Me. Bus. & Consumer LEXIS 22, at *6–10 (Me. Bus. & Consumer Ct. Mar. 14, 2012). "'New Jersey courts have consistently held that contract law is better suited to resolve disputes where a plaintiff alleges direct and consequential losses that were within the contemplation of sophisticated business entities that could have been the subject of their negotiations.'. . . The New Jersey cases repeatedly emphasize that respecting the parties' voluntary agreements to allocate risk best serves the public interest." *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 582–83 (S.D. Tex. 2011), *rev'd in part sub nom.* Lone Star Nat. Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421 (5th Cir. 2013) (citations omitted).

161. Dittman v. UPMC, No. GD-14-003285, 2015 WL 4945713, at *6 (Pa. Ct. Com. Pl. May 28, 2015). The court "recognized that there is an absence of guidance as to what actions constitute reasonable care and allowing juries to determine what constitutes reasonable care is not a 'viable method for resolving the difficult issue of the minimum requirements of care that should be imposed in data breach litigation.'" Caponi, *supra* note 156, at 23.

162. *Dittman*, 154 A.3d at 323–24 (declining to impose duty of reasonable care in collecting and storing employee information). "Employers . . . have an obvious need to collect and store personal information about their employees. . . While a data breach (and its ensuing harm) is generally foreseeable, we do not believe that this possibility outweighs the social utility of electronically storing employee information. In the modern era, more and more information is stored electronically and the days of keeping documents in file cabinets are long gone. Without doubt, employees and consumers alike derive substantial benefits from efficiencies resulting from the transfer and storage of electronic data. Although breaches of electronically stored data are a potential risk, this generalized risk does not outweigh the social utility of maintaining electronically stored information. We note here that [plaintiffs] do not allege that [defendant] encountered a specific threat of intrusion into its computer systems." *Id.*

163. Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1587–90 (2005).

164. Smith v. Triad of Ala., LLC, No. 1:14-CV-324-WKW, 2017 WL 1044692, at *12 (M.D. Ala. Mar. 17, 2017).

165. Hapka v. CareCentrix, Inc., No. 2:16-cv-02372, 2016 WL 7336407, at *5 (D. Kan. Dec. 19, 2016).

166. Silverpop Sys., Inc. v. Leading Mkt. Tech., Inc., No. 1:12-cv-2513-SCJ, 2014 WL 11164763, at *3 (N.D. Ga. Feb. 18, 2014).

3. Causation

Businesses have questioned the causal relationship between the breach of duty and injury.[167] How can the plaintiff prove that this data breach was the one that caused the harm? The data may have been exposed somewhere else as well. The usual response is that a coincidence of time and sequence between the data breach and the harm is insufficient alone to establish causation, but will meet the requirement when accompanied by other factors.[168] For example, identity thefts occurring ten and fourteen months after a data breach were held to be causally related when the same types of sensitive information hacked were later used to steal the identities.[169] In another case that held causation was established, the defendant had a serious data breach that went uncorrected for two years, the defendant exposed information from a plaintiff who had a practice of protecting it and had never had his identity stolen before, and data of the same type was used to file a false tax return.[170]

4. Injury

A number of states adhere to the "economic loss doctrine" and have employed it to dismiss negligence claims in the data breach context.[171] In these states, negligence claims alleging purely economic loss unaccompanied by a physical injury are deficient as a matter of law.[172] Absent a duty imposed by law or a special relationship between the plaintiff and defendant, the doctrine bars negligence claims for solely

167. *See* Michael Hooker & Jason Pill, *You've Been Hacked, and Now You're Being Sued: The Developing World of Cybersecurity Litigation*, 90 FLA. B. J. 30, 36 (2016).

168. *See, e.g.*, Hamid Salim & Stuart Madnick, Cyber Safety: *A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack*, CYBERSECURITY INTERDISCIPLINARY SYS. LAB. (Aug. 2016), http://web.mit.edu/smadnick/www/wp/2016-09.pdf.

169. Resnick v. AvMed, Inc., 693 F.3d 1317, 1327 (11th Cir. 2012).

170. Brush v. Miami Beach Healthcare Grp., Ltd., 238 F. Supp. 3d 1359, 1365–66 (S.D. Fla. 2017).

171. Longenecker-Wells v. Benecard Servs. Inc., 658 F. App'x 659, 661 (3d Cir. 2016). *See also* Silverpop Sys., Inc. v. Leading Mkt. Tech., Inc., 641 F. App'x 849, 852–53 (11th Cir. 2016); Dugas v. Starwood Hotels Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, LEXIS 152838, at *36–37 (S.D. Cal. Nov. 3, 2016); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1171–72 (D. Minn. 2014) (stating that the economic loss doctrine bars claims under Alaska, California, Illinois, Iowa, and Massachusetts law, but claims are not dismissed under District of Columbia, Georgia, Idaho, New Hampshire, New York, and Pennsylvania law); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966–73 (S.D. Cal. 2014) (dismissing California and Massachusetts claims); Dittman v. UPMC, 154 A.3d 318, 325 (Pa. Super. 2017); Caponi, *supra* note 156. *But see* Lone Star Nat'l Bank, N.A. v. Heartland Payment Sys., Inc., 729 F.3d 421, 426–27 (5th Cir. 2013) (finding that purely economic data breach negligence claim not dismissed because plaintiffs might be left with no other remedy "defying 'notions of fairness, common sense and morality;'" it was unclear whether the conduct of the defendant was covered by a contract).

172. *Beware the Economic Loss Rule*, COHEN AND WOLF, P.C. (Oct. 2006), http://www.cohenandwolf.com/?t=40&an=4619&format=xml&p=3199.

economic loss.[173] Since retail data breaches generally involve fraudulent purchases or tax returns at most, negligence claims are regularly dismissed in these states.[174]

D. Misrepresentation

Fraud by omission claims resemble unjust enrichment claims; if the defendant had disclosed its actual data security measures, the plaintiffs would not have purchased from the store.[175] One federal district court recognized such a claim was possible if the plaintiffs pled what defendant should have disclosed to avoid being misleading.[176]

At least one federal district court allows for negligent or innocent misrepresentation causes of action, but such claims ordinarily meet with little success.[177] Negligent misrepresentation claims generally require the elements of reliance and a special relationship, which courts may not find present in retail transactions.[178] In fact, in most retail transactions, there would be no communication about data security.[179] Apart from these deficiencies, misrepresentation claims may fail for lack of a pecuniary loss.[180]

E. Other Common Law Claims

Plaintiffs have tried a number of other common law claims without success. Courts have uniformly rejected invasion of privacy claims.[181] The problem is that it is an

173. Dittman v. UPMC, 154 A.3d 318, 325–26, (Pa. Super. Ct. 2017), *appeal granted*, 170 A.3d 1042 (Pa. 2017).

174. *See, e.g.*, *In re* TJX Cos. Retail Sec. Breach Litig., 564 F. 3d 489, 498 (1st Cir. 2009) (affirming dismissal of negligence claim by banks against retail chain that suffered a data breach because "purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage."); Cumis Ins. Soc'y, Inc. v. BJ's Wholesale Club, Inc., 918 N.E. 2d 36, 46–7 (Mass. 2009) (affirming dismissal of negligence claims under the Economic Loss Doctrine concluding that credit cards were "canceled by the plaintiff credit unions for the purpose of avoiding future economic losses."); Sovereign Bank v. BJ's Wholesale Club, Inc., 533 F. 3d 162 (3d Cir. 2008) (affirming dismissal of bank's negligence claim against retailer).

175. *In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1194–95 (D. Or. 2016).

176. *See id.*

177. *In re* Heartland Payment Sys., Inc. Customer Data Sec. Breach Litig., 834 F. Supp. 2d 566, 596–97 (S.D. Tex. 2011) (permitting amendment to complaint to allege negligent misrepresentation based on failure to correct verifiable factual statements).

178. Fero v. Excellus Health Plain, Inc., 236 F. Supp. 3d 735, 772–74 (W.D.N.Y. 2017), *rev'd in part on reconsideration sub nom.* No. 6:15-CV-06569 EAW, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018).

179. *In re* Sony Gaming Networks & Customer Data Security Breach Litig., 996 F. Supp. 2d 942, 973–75 (S.D. Cal. 2014).

180. *Id.* at 975.

181. *See, e.g.*, Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *35–36 (S.D. Cal. Nov. 3, 2016) (dismissing claim because data breach was unintentional); Burton v. MAPCO Express, Inc. 47 F. Supp. 3d 1279, 1286–87 (N.D. Ala. 2014) (dismissing claim when only negligent data breach alleged because invasion of privacy is an intentional tort); Burrows v.

intentional tort,[182] inappropriate when a defendant commercial business fails to protect against an unknown third-party hacker.[183] Bailment claims have fared no better because data was not placed in the exclusive possession of the defendant and there was no agreement that it would be returned.[184] Breach of fiduciary duty claims have failed as well because the parties were not in a fiduciary relationship.[185]

F. Statutory Claims

In addition to the panoply of common law claims, plaintiffs have asserted violations of a variety of federal and state statutes with mixed success.[186] Generally, the federal statutes provide no private right of action, but some courts have used violations to support negligence *per se* claims.[187] Some state statutes impose liability for failure to protect customer data.[188]

1. Federal Statutes

The two most common federal statutes plaintiffs claim are violated when their data is compromised are the Health Insurance Portability and Accountability Act of 1996

Purchasing Power, LLC, No. 1:12-cv-22800-UU, 2012 U.S. Dist. LEXIS 186556, at *19-21 (S.D. Fla. Oct. 18, 2012).

182. *See Dugas*, 2016 U.S. Dist. LEXIS 152838, at *35–36 (dismissing claim because data breach was unintentional); Burton v. MAPCO Express, Inc. 47 F. Supp. 3d 1279, 1286–87 (N.D. Ala. 2014) (dismissing claim when only negligent data breach alleged because invasion of privacy is an intentional tort); *Burrows*, 2012 U.S. Dist. LEXIS 186556, at *19-21.

183. Galaria v. Nationwide Ins. Co. 663 F. App'x 384, 392 (6th Cir. 2016).

184. *See generally* Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016) (dismissing a bailment claim based on a lack of Article III standing). *See also In re* Cmty. Health Sys., Inc., Customer Sec. Data Breach Litig., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *34–38 (N.D. Ala. Sept. 12, 2016) (dismissing claim because data not placed in exclusive possession of purported bailee); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1177 (D. Minn. 2014) (dismissing bailment claim because plaintiffs did not agree with defendant that defendant would return the purported bailed property to them); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 903 F. Supp. 2d 942, 974–75 (S.D. Cal. 2012) (dismissing bailment claim because no intentional conduct by defendant; personal information was not personal property delivered to defendant and expected to be returned; and claim was duplicative of negligence and consumer protection claims).

185. *See In re* Premera Blue Cross Customer Data Sec. Breach Litig., 198 F. Supp. 3d 1183, 1200–01 (D. Or. 2016) (dismissing claim because parties not in type of relationship historically considered fiduciary); Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1367 (S.D. Fla. 2015) ("[M]ere receipt of confidential information is insufficient by itself to transform an arm's-length transaction into a fiduciary relationship.").

186. *See infra* Parts II.C.1, II.C.2.

187. *See infra* Part II.C.1.

188. *See infra* Part II.C.2.

("HIPAA") and the Fair Credit Reporting Act.[189] Courts agree that HIPAA provides no private right of action.[190] However, some have held that the failure to adhere to its privacy protection provisions for confidential medical information can form the basis of a negligence or negligence *per se* claim.[191] The Federal Trade Commission Act, which also does not give rise to a private right of action, has been used in this manner as well; the argument is that since the Federal Trade Commission ("FTC") considers the failure to take reasonable steps to secure data an unfair trade practice, a cyber breach can be a statutory violation that constitutes negligence *per se*.[192]

Violations of the Fair Credit Reporting Act are frequently asserted.[193] The Act specifically permits a private right of action when its provisions are not followed.[194] However, courts have uniformly held that it is directed at consumer reporting agencies and is inapplicable to a retail customer data breach.[195]

2. State Data Breach Notification Laws

After a series of major data breaches made the news, nearly all the states passed breach notification laws.[196] Some of these are disclosure laws alone; they simply

189. Health Insurance Portability and Accountability Act of 1966, Pub. L. No. 104-191, 110 Stat. 1936 (codified in Titles 18, 26, and 42 of the United States Code) (West 2018); Fair Credit Reporting Act, Pub. L. No. 91-508, 84 stat. 114-2 (codified at Titles 12 U.S.C. §§ 1830–31; 15 U.S.C. § 1681 et seq.) (West 2018).

190. Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010); Wilkerson v. Shinseki, 606 F.3d 1256, 1267 n.4 (10th Cir. 2010); Webb v. Smart Document Sols., LLC, 499 F.3d 1078, 1081 (9th Cir. 2007); Arcara v. Banks, 470 F.3d 569, 570–71 (5th Cir. 2006); Warren Pearl Constr. Corp. v. Guardian Life Ins. Co. of Am., 639 F. Supp. 2d 371, 377 (S.D.N.Y. 2009).

191. *Compare In re* Cmty. Health Sys., Inc., Customer Sec. Data Breach Litig., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *87–94 (N.D. Ala. Sept. 12, 2016) (finding no private right of action, but HIPAA can define the standard of care in a negligence *per se* action in some states and a negligence claim in others), *with* Weinberg v. Advanced Data Processing, Inc., 147 F. Supp. 3d 1359, 1365-66 (S.D. Fla. 2015) (holding that negligence claim based on HIPAA violations fails). *See also* Smith v. Triad of Ala., LLC, No. 1:14-CV-324-WKW, 2017 U.S. Dist. LEXIS 38574, at *38-39 (M.D. Ala. Mar. 17, 2017).

192. *In re Cmty. Health Sys*., 2016 U.S. Dist. LEXIS 123030, at *87–94.

193. Jennifer L. Conn & Ryan T. Bergsieker, *Cybersecurity & Data Privacy: An Overview for Health Care, Pharmaceutical, and Biotech Companies*, GIBSON DUNN (Aug. 8, 2017), https://www. gibsondunn.com/cyber security-data-privacy-an-overview-for-health-care-pharmaceutical-and-biotech-companies-2/.

194. Safeco Ins. Co. of America v. Burr, 551 U.S. 47, 53 (2007).

195. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384, 390-91 (6th Cir. 2016); *In re Cmty. Health Sys.*, 2016 U.S. Dist. LEXIS 123030, at *48-60 (N.D. Ala. Sept. 12, 2016) (dismissing claim because defendant not consumer reporting agency and fees collected were for healthcare services, not evaluating credit); Falkenberg v. Alere Home Monitoring, Inc., No. 13-cv-00341-JST, 2015 U.S. Dist. LEXIS 22121, at *14 (N.D. Cal. Feb. 23, 2015) (holding the Fair Credit Reporting Act does not cover healthcare provider communications with insurers about coverage); Burton v. MAPCO Express, Inc., 47 F. Supp. 3d 1279, 1286–87 (N.D. Ala. 2014); *In re* Sony Gaming Networks & Customer Data Security Breach Litig., 996 F. Supp. 2d 942, 1010–12 (S.D. Cal. 2014) (dismissing claim because defendant not a consumer reporting agency).

196. Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1313 n.1 (M.D. Fla. 2010). As of June 2017, only Alabama and South Dakota had no data breach notification laws. *Security Breach Notification Laws*, NAT.

require a business to notify customers in the event of a breach.[197] Others impose an affirmative duty to protect data.[198]

In more than half the states, the data breach notification laws provide that only the state attorney general (or other state official) may bring a claim against a business under the statute.[199] Eleven states and the District of Columbia provide for a private

CONF. ST. LEGS. (Feb. 6, 2018), http://www.ncsl.org/research/ telecommunications-and-information-technology/security-breach-notification-laws.aspx.

197. *See, e.g.*, KAN. STAT. ANN. § 50-7a02 (2017).

198. *See, e.g.*, CAL. CIV. CODE § 1798.81 5(b) (West 2018) ("A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."); Beryl A. Howell, *Cyber-Security Liability: Is it Time to Get Off the Soapbox?*, 22 COMPUTER & INTERNET L. 1, 3 (2005) ("The recent California mandatory disclosure law (SB 1386) requires companies holding computerized personal information of California residents to take steps either to encrypt this personal information or adopt, as part of an information security policy, notice and disclosure procedures for any computer security breaches, whether or not the breach occurs in California. Noncompliant companies are subject to civil suits, including class actions, for damages and injunctive remedies in California courts.").

199. ARIZ. REV. STAT. ANN. § 18-545 (2016); ARK. CODE ANN. § 4-110-101 *et seq.* (West 2017); COLO. REV. STAT. ANN. § 6-1-716 (West 2018); CONN. GEN. STAT. ANN. § 36a-701b (West 2018); DEL. CODE ANN. tit. 6 § 12B-101 *et seq.* (West 2017); HAW. REV. STAT. ANN. § 487N-1 *et seq.* (West 2017); IDAHO CODE ANN. § 28-51-104 *et seq.* (West 2017) (providing that state regulator can enforce notification provision); IND. CODE ANN. § 4-1-11-1 *et seq.* (West 2017) (enabling the attorney general to seek penalties for failure to comply with data maintenance obligations); IOWA CODE § 715C.1-2 (2014); KAN. REV. STAT. § 50-7a01 *et seq.* (2014) (explaining that the attorney general can enforce compliance and seek to injunction of further violations); 10 ME. REV. STAT. ANN. § 1346 *et seq.* (2018); MASS. GEN. LAWS ANN. CH. 93H § 1 *et seq.* (West 2018); MICH. COMP. LAWS ANN. § 445.63, 72 *et seq.* (West 2018); MISS. CODE ANN. § 75-24-29 (West 2018) (failing to comply is unfair trade practice; law enforced by attorney general); NEB. REV. STAT. ANN. § 87-801 *et seq.* (West 2017) (providing that the attorney general can seek economic damages for every affected Nebraska resident injured by violation of statute); NEV. REV. STAT. ANN. § 603A.010 *et seq.* (West 2018) (explaining that the attorney general can seek injunctive relief; data *collector* can sue hacker or person who unlawfully benefitted); 2017 H.B. 15, Chap 36 (N. Mex.) (effective Jun. 16, 2017); N.Y. GEN. BUS. LAW § 899-aa (McKinney 2018); N.D. CENT. CODE § 51-30-01 *et seq.* (West 2017); OHIO REV. CODE ANN. § 1349.19 (West 2017) (providing that the attorney general can bring a civil action for failure to comply with law); 24 OKLA. STAT. ANN. tit. § 161 *et seq.* (West 2014) (explaining that the attorney general can seek actual damages or $150,000 per breach of security or series of related breaches); 73 PA. CONST. STAT. AND CONS. STAT. ANN. § 2301 *et seq.* (West 2017) (describing how the attorney general has exclusive authority to bring action under Unfair Trade Practices and Consumer Protection Law for violation of statute); 11 R.I. GEN. LAWS ANN. § 49-2-1 *et seq.* (West 2012) (providing that each violation is a civil violation carrying penalty up to $100, not more than $25,000 in the aggregate); 11 TEX. BUS. & COM. CODE ANN. §§ 521.002, 521.053 (West 2017) (explaining that the attorney general can seek injunctive relief, civil penalties of at least $2,000 but not more than $50,000 per violation; failure to notify raises penalties up to $100 per person per day and up to $25,000 per breach); UTAH CODE ANN. §§ 13-44-101, 13-44-202, 13-44-301 (West 2017) (providing that the attorney general can seek up to $2,500 per consumer, $100,000 per related violations); 9 VT. STAT. ANN. tit. 9 §§ 2430, 2435 (West 2017); VA. CODE ANN. § 18.2-186.6 (West 2017) (describing how the attorney general can seek civil penalties up to $150,000 per breach or related breaches); W.VA. CODE ANN. § 46-A-2A-101 *et seq.* (West 2017); WYO. STAT. ANN. § 40-12-501 *et seq.* (West 2017) (explaining that the attorney general may bring action to ensure compliance, recover damages, or both).

right of action in their statutes.[200] Eight states have data notification acts that are silent about who enforces them, which leaves it to the courts to decide whether there is a private right of action.[201] A private action, even in a state that allows one, may require an injury.[202] Some states will not allow claims to move forward absent an injury beyond a statutory violation.[203]

Private rights of action aside, many states impose stiff penalties on businesses that compromise customer data.[204] Some state statutes impose strict liability; if the information is compromised, the business holding the information will be liable and may have to pay fines as high as $1,000 per exposed record.[205] A number of state data breach statutes also require businesses to pay plaintiffs' legal fees.[206]

200. ALASKA STAT. ANN. § 45.48.010 *et seq.* (West 2017); CAL. CIV. CODE §§ 1798.29, 1798.80 *et seq.* (West 2018); D.C. CODE ANN. § 28-3851 *et seq.* (West 2018) (including costs of action and attorneys' fees, but not including dignitary damages such as pain and suffering); 815 ILL. COMP. STAT. ANN. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25 (West 2018) (violating act constitutes unlawful business practice under Illinois Consumer Fraud and Deceptive Business Practices Act); LA. STAT. ANN. § 51:3071 *et seq.* (2017) (requiring damages from failure to disclose breach); MD. CODE ANN., COM. LAW § 14-3501 *et seq.* (West 2018) (providing that consumers may sue under Unfair and Deceptive Trade Practices Act; attorney general also enforces act); MINN. STAT. ANN. § 325E.61 (West 2017) (explaining that the attorney general also enforces act); N.H. REV. STAT. ANN. § 359-C:19 *et seq.* (2017) (requiring double or triple damages if intentional, plus costs of suit, plus attorneys' fees; attorney general also enforces act); N.C. GEN. STAT. ANN. §§ 75-61, 75-65 (West 2018) (explaining that the attorney general also enforces act with criminal and civil penalties); S.C. CODE ANN. § 39-1-90 (2017) (requiring damages if willful and knowing, but only actual damages if negligent; injunction to enforce compliance, attorneys' fees and court costs if successful; $1,000 fine for every state resident whose information was accessible); TENN. CODE ANN. § 47-18-2107 (West 2017); WASH. REV. CODE ANN. § 19.255.010 *et seq.* (West 2017).

201. FLA. STAT. ANN. § 501.171 (West 2017); GA. CODE ANN. § 10-1-910 *et seq.* (West 2017); KY. REV. STAT. ANN. § 365.732 (West 2017); MO. REV. STAT. § 407.1500 (2017); MONT. CODE ANN. § 30-14-1701 *et seq.* (West 2017); N.J. STAT. ANN. § 56:8-163 (West 2017); OR. REV. STAT. ANN. §§ 646A.600, 646A.602, 646A.604, 646A.624, 646A.626 (West 2017); WIS. STAT. ANN. § 134.98 (West 2017). *See* Amburgy v. Express Scripts, Inc. 671 F. Supp. 2d 1046, 1055 (E.D. Mo. 2009) (holding no private right of action in Missouri); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1166–70 (D. Minn. 2014) (dismissing claims since statutes provided for attorney general enforcement only, but sustained for statutes with nonexclusive remedies or statutes silent on enforcement).

202. Bella Chasse Auto. Care, Inc. v. Advanced Auto Parts, Inc., No. 08-1568, 2009 U.S. Dist. LEXIS 25084, at *4–7 (E.D. La. Mar. 24, 2009).

203. *In re* SuperValu, Inc., Customer Data Sec. Breach Litig., No. 14-MD-2586 ADM/TNL, 2016 U.S. Dist. LEXIS 2592, at * 21–22 (D. Minn. Jan. 7, 2016).

204. *See, e.g.*, IND. CODE ANN. § 4-1-11-1 *et seq.* (West 2017); NEB. REV. STAT. ANN. § 87-801 *et seq.* (West 2017); 24 OKLA. STAT. ANN. tit. § 161 *et seq.* (West 2014).

205. Gwendolyn A. Williamson & Mary C. Moynihan, *The Liability Hole—Cybersecurity Risks and the Apportionment of Liability*, 21 INV. LAW. 1, 5 (2014). *See supra* notes 198–200 and accompanying text.

206. *See supra* note 199 and accompanying text.

3. State Deceptive and Unfair Trade Practices Acts

In some states, plaintiffs have successfully alleged breaches of consumer protection laws prohibiting deceptive and unfair trade practices.[207] In New York, for example, which does not permit private actions under its data breach notification law, a plaintiff class avoided a motion to dismiss a claim under a provision prohibiting "[d]eceptive acts or practices in the conduct of any business or trade or commerce or in the furnishing of any service."[208] The claim was that the defendant businesses made "representations in their privacy policies and on their websites concerning data security…[that] would lead a reasonable consumer to believe that the [businesses] were providing more adequate data security than they purportedly were."[209] Claims like these, pursuant to deceptive business practice statutes, have survived motions to dismiss in a number of states, many of which do not permit private rights of action under the more specific data breach notification laws.[210]

III. WHAT IS "REASONABLE" DATA SECURITY?

Apart from the state statutes that hold business owners strictly liable for data breaches regardless of fault, most claims are based on the failure of owners to provide "reasonable" data security.[211] There is little case law yet on what is reasonable; many

207. *In re* Anthem, Inc. Data Breach Litigation, 162 F.Supp.3d 953, 984, 987–91, 995–96 (N.D. Cal. 2016); *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1161–66 (D. Minn. 2014); Fero v. Excellus Health Plan, Inc., 236 F. Supp. 3d 735, 774–78 (W.D.N.Y. 2017), *rev'd in part on reconsideration sub nom.* No. 6:15-CV-06569 EAW, 2018 WL 507320 (W.D.N.Y. Jan. 19, 2018).

208. *Excellus Health Plan*, 236 F. Supp. 3d at 774–78; N.Y. GEN. BUS. LAW § 349 (McKinney 2018).

209. *Excellus Health Plan*, 236 F. Supp. 3d at 776.

210. *In re* Target Corp., 66 F. Supp. 3d at 1161–66; *In re* Cmty. Health Sys. Inc. Customer Sec. Data Breach Litig., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *100–04 (N.D. Ala. Sept. 12, 2016); *In re* Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 985, 988, 990-92, 995-96, 999-1000, 1003 (S.D. Cal. 2014). *See, e.g.*, Florida Deceptive and Unfair Trade Practices Act, FLA. STAT. ANN. § 501.204(1) *et seq*. (West 2017); New Mexico Unfair Practices Act, N.M. STAT. ANN. §§ 57-12-2(D)(5)(7) & (14) & 57-12-3, *et seq*. (West 2018); Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 PA. CONST. STAT. ANN. AND CONS. STAT. ANN §§ 201-2(4)(v)(vii) & (xxi), 201-3, *et seq*. (West 2017). *But see* Cmty. Bank of Trenton v. Schnuck Mkt. Inc., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *21 (S.D. Ill. 2017) ("The Court does not find a concrete public policy that has been violated. Defendant was not explicitly advertising data security or luring customers into the store on the premise that it practiced better data security than other retailers, nor were issuing banks being lured into authorizing transactions on the basis that Defendant's data security was top notch. Though there might have been a general market expectation that any retailer would practice prudent data security, the facts do not suggest that Defendant gamed the market to take advantage of consumers of financial institutions on these grounds.").

211. Phillip L. Gordon & Zoe M. Argento, *"Reasonable" Data Security: The FTC's Guideposts for Employers*, LITTLER MENDELSON P.C. (June 9, 2014), https://www.littler.com/publication-press/ publication/reasonable-data-security-ftcs-guideposts-employers.

lawsuits have been dismissed before the courts reached the scope of the duty[212] and data breach statutes often do not define it.[213]

The FTC may fill this hole. The FTC has "taken the lead in setting cybersecurity standards, developing something like a body of common law with its vast collection of complaints, privacy guides, and consent decrees. . ."[214] and has "emerged as the leading arbiter of what constitutes reasonable data security."[215] In one case, a federal district court refused to dismiss negligence and negligence *per se* claims that used the failure to adhere to FTC standards to signal unreasonable conduct.[216]

The FTC has eschewed regulations about what specific steps or protections constitute reasonable data security; rather it states that it approaches reasonableness on a case-by-case basis considering the size of the business and the type of data.[217] This caused one panel to wonder at a recent oral argument how businesses know whether they are in compliance.[218] Reasonableness is a moving target.[219] Despite this concern, the FTC has commenced over 200 breach of privacy cases.[220]

In the courts, a fairly general statement that the defendant failed to meet industry standards may suffice at the pleading stage,[221] but to establish a claim, the

212. *See id*. *But see* OR. REV. STAT. ANN. § 646A.622(2) (West 2018).

213. 201 MASS. CODE REGS. 17.01-17.05 (2012). *But see* OR. REV. STAT. § 646A.622(2).

214. Stuart L. Pardau & Blake Edwards, *The FTC, the Unfairness Doctrine, and Privacy by Design: New Legal Frontiers in Cybersecurity*, 12 J. BUS. & TECH. L. 227, 238 (2017).

215. *Id.* at 242.

216. *In re* Cmty. Health Sys. Inc., Customer Sec. Data Breach Litig., No. 15-CV-222-KOB, 2016 U.S. Dist. LEXIS 123030, at *87–94 (N.D. Ala. Sept. 12, 2016).

217. According to the FTC, "data-security cases pose questions 'so specialized and varying in nature as to be impossible of capture within the boundaries of a general rule.' Data-security risks and standards evolve constantly and vary based on a business's size and the type of data it maintains. The FTC, therefore, 'must retain power to deal with [such] problems on a case-by-case basis if the administrative process is to be effective.'" Brief of the FTC at 49, LabMD, Inc. v. FTC, 678 F. App. 816 (11th Cir. 2017) (No. 16-16270), https://www.ftc.gov/system/files/documents/cases/labmd_ca11 _ftc_r esponse_brief_2017-0209.pdf (citations omitted).

218. Jimmy H. Koo, *Judges Question FTC Data Security Standard at LabMD Argument*, BLOOMBERG (June 23, 2017), https://www.bna.com/judges-question-ftc-n73014460645/ ("Rulemaking isn't effective and there are too many variables, as standards are always changing, the FTC's counsel said. The court, however, questioned how companies are supposed to know 'that they're violating what they're violating,' if there are no rules.").

219. *See* Patco Constr. Co. v. People's United Bank, 684 F.3d 197, 209 (1st. Cir. 2012) (explaining that for electronic fund transfers, UCC protects banks that employ security procedures commercially reasonable for the particular customer and the particular bank); *see also* John Black, *Developments in Data Security Breach Liability*, 69 BUS. LAW. 199, 205 (2013).

220. Pardau & Edwards, *supra* note 214, at 240.

221. Under a California statute, a complaint alleging that a business failed to "appropriately encrypt customers' data" and that "'security systems and protocols' should have been designed, implemented, maintained, and tested 'consistent with industry standards and requirements'" survived a motion to dismiss. Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 U.S. Dist. LEXIS 152838, at *31–32 (S.D. Cal. Nov. 3, 2016).

plaintiff must introduce evidence of the standard, the custom within the industry.[222] Custom in the industry, however, cannot provide the whole answer. Should a physician practicing alone be held to the same standard of data security as a multi-state medical conglomerate because they are in the same industry? What factors should a court consider when determining whether a small business owner acts reasonably with respect data security? Certainly, expense must be taken into account when assessing what is reasonable for small business owners.[223] Is it also appropriate to bear the education of the business owner in mind?

In a variety of contexts, courts have recognized the need to treat small businesses differently from large corporations because of the disparity in financial resources.[224] More formality is expected at a large corporation.[225] For example, courts do not expect a small business "owner to spend the time, or incur the expense, to document individual employment decisions."[226] Small business owners are held to a reasonable small business owner standard.[227] The data security context is no different. "Reasonable efforts may vary in light of the circumstances. What is reasonable for a large corporation with sizable resources may not be reasonable for an individual small business owner."[228] Requiring a small business owner to do more can "make the cost of running a small business prohibitive."[229] The FTC has suggested that, for economic reasons, it expects less data security from small businesses.[230]

222. Silverpop Sys., Inc. v. Leading Mkt. Tech., Inc., 641 F. App'x 849, 852 (11th Cir. 2016).

223. Gordon & Argento, *supra* note 211.

224. *See*, *e.g.*, Allstar Mktg. Grp., LLC v. Your Store Online, LLC, 666 F. Supp. 2d 1109, 1131–34 (C.D. Cal. 2009) (finding in favor of small business); Del. Credit Corp. v. Aronoff, No. 92-CV-135S, 1992 U.S. Dist. LEXIS 10422, at *20-21 n.9 (W.D.N.Y. 1992) (finding in favor of small business); Bell Atlantic Tricon Leasing Corp. v. Johnnie's Garbage Serv., Inc., 439 S.E.2d 221, 225–26 (N.C. Ct. App. 1994) (finding in favor of small business); *cf.* Azari v. B&H Photo Video, No. 06 Civ. 7825 (DLC), 2007 U.S. Dist. LEXIS 12, at *8-9 (S.D.N.Y. 2007) (finding in favor of large corporation defendant). In *Pludeman v. N. Leasing Sys., Inc.*, 74 A.D.3d 420 (N.Y. App. Div. 2010), a large corporate defendant was required to pay to notify small business class members. *Id.* at 425.

225. Lough v. Brunswick Corp., 86 F.3d 1113, 1120–21 (Fed. Cir. 1996).

226. Hague v. Thompson Distrib. Co., 436 F.3d 816, 826 (7th Cir. 2006).

227. Rodrigue v. Olin Employees Credit Union, 406 F.3d 434, 451 (7th Cir. 2005) ("[Physician] could be expected to take the reasonable steps that any small business owner would take to prevent embezzlement by an employee.").

228. United States v. Aruda, No. 05–00751, 2006 WL 2051336, at *3 (D. Haw. July 19, 2006).

229. Roberts v. Tiny Tim Thrifty Check, 367 So. 2d 64, 65 (La. Ct. App. 1979).

230. Brief of Respondent at 6, LabMD, Inc. v. FTC, 678 F. App'x 816 (11th Cir. 2017) (No. 16-16270), https://www.ftc.gov/system/files/documents/cases/labmd_ca11_ftc_response_brief_2017-0209.pdf ("[B]ecause companies vary widely in size and the type and volume of data they hold, a one-size-fits-all regime would be unworkable. Instead, the Commission has made clear that '[t]he touchstone of [its] approach to data security is reasonableness: a company's data security measures must be reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its business, and the cost of available tools to improve security and reduce vulnerabilities.'"). A small laboratory company the FTC has

Economics aside, whether a small business owner is entitled to be treated differently because he or she does not know any better presents a tougher question. On the one hand, the law does not reward ignorance[231] and individuals cannot rely on their lack of sophistication to excuse a lack of diligence.[232] On the other hand, courts regularly judge the reasonableness of behavior in light of education and experience.[233] Even in large corporations with highly educated and experienced businesspeople overseeing operations, some worry that data security issues pose challenges because the people in charge know nothing about them and cybersecurity risks are changing faster than the executives can learn about them.[234] Data security

pursued with the tenacity of Inspector Javert may, however, doubt the sincerity of these words. Its billing manager downloaded a file-sharing program so she could listen to music at her work station. *Id.* at 2. The program allowed files in her document folder to be shared with other users, including a file with information about 9,300 patients. *Id.* at 3. To market its services, a data security firm trolled the Internet looking for openings to files and then contacted the compromised companies, hoping to convince them to purchase the firm's services. *Id.* at 11. The data security firm found the billing manager's file and contacted the laboratory, but the laboratory fixed the problem and refused to purchase the data security firm's services. *Id.* at 11. The data security firm reported the laboratory (and other companies who did not purchase its services) to the FTC. *Id.* at 11. Relying on fabricated evidence from the data security firm that four different IP addresses had downloaded the file, the FTC issued a complaint against the laboratory alleging it did not provide reasonable security. *Id.* at 12. An FTC administrative law judge dismissed the case, but the full commission reversed. Even though the laboratory went out of business because of the cost of the FTC proceedings and litigation, the FTC ordered expensive remedial measures. *Id.* at 12–13. The Eleventh Circuit granted a stay and the litigation is ongoing. *See* LabMD, Inc. v. FTC, 678 F. App'x 816 (11th Cir. 2016).

231. Commil USA, LLC v. Cisco Sys., Inc., 135 S. Ct. 1920, 1930 (2015), *vacating in part*, Commil USA, LLC v. Cisco Sys., Inc., 720 F.3d 1361 (E. D. Tex. 2013) ("'[O]ur law is . . . no stranger to the possibility that an act may be "intentional" for purposes of civil liability, even if the actor lacked actual knowledge that her conduct violated the law.' Tortious interference with a contract provides an apt example. While the invalidity of a contract is a defense to tortious interference, belief in validity is irrelevant. In a similar way, a trespass 'can be committed despite the actor's mistaken belief that she has a legal right to enter the property.' And of course, '[t]he general rule that ignorance of the law or a mistake of law is no defense to criminal prosecution is deeply rooted in the American legal system.' In the usual case, 'I thought it was legal' is no defense.") (citations omitted).

232. J. Geils Band Emp. Benefit Plan v. Smith Barney Shearson, Inc., 76 F.3d 1245, 1260 (1st Cir. 1996) ("Unsophisticated or not, plaintiffs cannot shroud themselves in ignorance or expect that their unsophistication will thoroughly excuse their lack of diligence.").

233. Forgues v. Select Portfolio Servicing, 690 F. App'x 896, 900 (6th Cir. 2017); United States v. Munguia, 704 F.3d 596, 604–05 (9th Cir. 2012); Bustamante v. First Fed. Sav. & Loan Ass'n, 619 F.2d 360, 364 (5th Cir. 1980); *In re* General American Life Ins. Co. Sales Practices Litig., 391 F.3d 907, 914 (8th Cir. 2004); Benedetto v. PaineWebber Grp., Inc., No. 96-3401, 1998 WL 568328, at *4 (10th Cir. 1998), *aff'g in part, rev'g in part*, 1996 WL 665460 (D. Kan. 1996); *In re* McLaren, 3 F.3d 958, 962 (6th Cir. 1993); Brown v. E.F. Hutton Grp., Inc., 991 F.2d 1020, 1032 (2d Cir. 1993); Silver v. Comm'r of Internal Revenue Serv., 2008 Tax Ct. Memo WL 4862161, at *7 (U.S. Tax Ct. Nov. 10, 2008); Key v. Cherokee Credit Life Ins. Co., 298 So.2d 892, 894 (La. Ct. App. 1974); Seaboard Planning Corp. v. Powell, 364 So. 2d 1091, 1094 (Miss. 1978); Grewing v. Minneapolis Threshing-Machine Co., 80 N.W. 176, 178 (S.D. 1899).

234. Arthur C. Delibert et al., *Cybersecurity: Could Investment Company Directors Be Liable for a Breach?*, 22 INV. LAW. 1, 1 (2015) ("Cybersecurity concerns are different than the other hot issues that boards are

issues lie like traps for small business owners who, in most cases, are untrained in technology security[235] and often have little or no college education.[236]

And their financial vulnerability to customers may get worse. Courts have hinted that they may be more likely to impose liability in the future.[237] Some, in denying liability, suggest that businesses will be expected to be more savvy about data security than they are now; in other words, the reasonableness bar will be raised.[238]

> *The entire world is moving towards electronic storage of information. With this will come a greater awareness of what is reasonable in terms of the care and storage of confidential information. At some point, the balance of weighing social utility in favor of data storage entities may shift more in favor of persons like [plaintiffs]. . . [H]arm becom[ing] foreseeable under circumstances that commonly are understood to render storage vulnerable…may weigh in favor of imposing additional duties upon an actor even absent legislative action. As for. . . the overall public interest. . .,. . . this factor too may shift as the foreseeability of harm changes with the evolution and increased use of this technology.*[239]

IV. POTENTIAL IMPACT ON SMALL BUSINESSES

When customer data is compromised in a small business, the potential statutory fines or litigation damages can be devastating. State attorneys general can seek penalties of as much as $2,500 per consumer.[240] Primary care physicians, who average 2,367

confronting nowadays . . . because cybersecurity issues are matters for which board members may not have any intuitive feel from their backgrounds in the business or regulatory worlds, because the problems in the cybersecurity realm are mutating faster than problems in other areas, and because the problems of cybersecurity are imposed largely from outside the organization.").

235. *See* Daniel Clapper & William Richmond, *Small Business Compliance with PCI DSS*, 19.1 J. MGMT. INFO. & DECISION SCI. 54, 55 (2016).

236. *The Surprising Demographics of Small Business Owners*, SMALLBIZLABS (June 21, 2016), http://www.smallbizlabs.com/2016/06/the-demographics-of-small-business-owners.html.

237. *See* Cmty. Bank of Trenton v. Schnuck Markets, Inc., No. 15-cv-01125-MJR, 2017 U.S. Dist. LEXIS 66014, at *11 (S.D. Ill. May 1, 2017); *see also id.* at *11 n.3 ("In much of the other data breach litigation, standing has been scrutinized closely. However, that issue has not been put before the Court at this juncture, so the Court is not considering the harms stated from that perspective without the benefit of argument from the parties.").

238. Dittman v. UPMC, 154 A.3d 318, 327 (Pa. Super. 2017) (Stabile, J., concurring).

239. *Id.*

240. FIRST DATA MKT. INSIGHT, SMALL BUSINESSES: THE COST OF A DATA BREACH IS HIGHER THAN YOU THINK (2014), https://www.firstdata.com/downloads/thought-leadership/Small_Businesses_Cost _of_a_Data_Breach_Article.pdf (stating that data breaches can cost small businesses up to $36,000); *The True Cost of a Data Breach to a Small Business*, CORP. INFO. TECHS., (2016), https:// www.corp-infotech.com/true-cost-data-breach-small-business/ (stating that the direct out-of-pocket costs of a data breach for most small businesses is approximately $14,000, excluding legal, regulatory, or compulsory fines and fees).

patients,[241] could easily find themselves bankrupt. A diner, serving an estimated 200,000 meals in a year,[242] could be driven out of business.

The potential losses do not stop at fines. Lawsuits brought by plaintiffs with compromised data add another layer of financial risk.[243] Identity theft protection for customers costs $25 to $60 per customer per year.[244] Fees for late payments or new cards might have to be reimbursed for anyone whose card was misused.[245] Soft damage claims like stress and lost time from canceling and replacing cards could cost much more.[246] Statutes that require businesses to pay plaintiffs' legal fees could involve significant expense.[247]

Even the cost of defending against prohibitive injunctive relief can be too great a burden for a small business. A small medical laboratory battling against the FTC claims it "was forced to wind down operations and stop diagnosing cancer" because of the "crushing burdens imposed upon it by the FTC's investigation and ensuing action…"[248] Although the Commission imposed no fine, it required the lab—already

241. Lenny Bernstein, *How many patients should your doctor see each day?*, WASH. POST (May 22, 2014), https://www.washingtonpost.com/news/to-your-health/wp/2014/05/22/how-many-patients-should-your-doctor-see-each-day/?utm_term=.93ecd0a1e2e3.

242. An estimate may be determined by considering the number of tables, the number of individual seats, hours of operation, and the average time a patron stays in the establishment. Wilhelm Schnotz, *How to Calculate the Sales in a Restaurant and Customer Turnover*, CHRON, http://small business.chron.com/calculate-sales-restaurant-customer-turnover-33155.html (last visited Feb. 21, 2018). This estimate can be adjusted to consider the frequency that the diner is not at full capacity. *Id.* Consider a diner with 30 tables, each seating 4 people. It is expected that half the time, only 2 customers will sit at a table, while 4 customers will sit at the tables the other half of the time. The diner is opened 12 hours a day, 360 days a year. An average patron stays about 2 hours in the establishment. An estimated number of customers served each day is about 540, almost 200,000 in a year.

243. *See Data Breach Lawsuit*, CLASSACTION (Dec. 20, 2017), https://www.classaction.com/data-breach/lawsuit ("When a company fails to exercise reasonable care in protecting its customers' information, affected consumers may be able to unite and file a class action lawsuit against the company.").

244. Hal Bundrick, *Should You Buy Identity Theft Insurance?*, U.S. NEWS (Mar. 24, 2014, 9:08 AM), http://money.usnews.com/money/blogs/my-money/2014/03/24/should-you-buy-identity-theft-insurance.

245. *See In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014) (allowing claims regarding unreimbursed fees to survive the pleading stage).

246. *See* Dugas v. Starwood Hotels & Resorts Worldwide, Inc., No. 3:16-cv-00014-GPC-BLM, 2016 WL 6523428, at *6 (S.D. Cal. Nov. 3, 2016).

247. Daniel R. Stoller, *Anthem Data Breach Class Action Hung Up Over Attorneys' Fees*, BIG LAW BUSINESS, (Feb. 6, 2018), https://biglawbusiness.com/anthem-data-breach-class-action-hung-up-over-attorneys-fees/ ("Anthem Inc. can't dispose of consumer class claims stemming from a 2015 data breach for now, after a federal judge raised concerns about nearly $38 million in proposed attorneys' fees.").

248. Brief of Petitioner at 6, LabMD, Inc. v. FTC, 678 F. App'x 816 (11th Cir. 2017) (No. 16-16270), https://www.scribd.com/document/335250387/2016-12-27-LabMD-Appellant-Brief#from_embed. According to the Eleventh Circuit, which granted a stay pending appeal, "LabMD ceased operations in January 2014. LabMD says its business could not bear the costs imposed by the FTC investigation and litigation, so it had to close. LabMD has essentially no assets, no revenue, and does not plan to resume business in the future. It obtained counsel pro bono because it could not afford to pay a lawyer. LabMD now has no employees, and

out of business—to adopt a "reasonably designed program" to secure patient data, to retain a qualified professional to conduct a biannual independent assessment of the program, and to notify 9,300 individuals that their data had been exposed.[249]

Many general liability insurance policies do not cover cybersecurity liability costs; insurance companies sell separate coverage for this type of peril.[250] Moreover, coverage might be rejected even under policies that include such risks.[251] If insurance does not cover breaches of contract or statutory fines, a business has significant exposure.

Without a legal safeguard for small businesses, the potential for loss is too great.

> *Indeed, in this era, where the threat of data breaches by unknown third parties is omnipresent, regardless of what preventative measures are taken, the potential disparity between the degree of a defendant's fault and the damages to be recovered could be immensely disproportionate, resulting in drastic implications for defendants named in lawsuits as well as our economic system at large.*[252]

V. A NEW APPROACH FOR SMALL BUSINESSES

Given their limited resources and lack of sophistication about information technology, it is unreasonable to expect small business owners to take independent steps to ensure data security. Consumers want the convenience of credit card payment and small businesses have been pushed into the cyber age whether they want to be there or not.[253] Unless they are to be driven out of business for third-party crimes they cannot reasonably be expected to prevent, the law needs to look at the problem in a different way for small businesses.

One improvement for breaches involving payment cards would be to impose liability, if any, on the card issuer. Credit card companies and banks require

keeps only the records required by law in a secured room, on an unplugged computer that is not connected to the Internet. LabMD has less than $5,000 cash on hand, and is subject to a $1 million judgment for terminating its lease early." LabMD, Inc. v. FTC, 678 F. App'x 816, 819 (11th Cir. 2016).

249. Brief of the FTC at 14–15, LabMD, Inc. v. FTC, 678 F. App'x 816 (11th Cir. 2017) (No. 16-16270), https://www.ftc.gov/system/files/documents/cases/labmd_ca11_ftc_response_brief_2017-0209.pdf.

250. *Cybersecurity*, NAT'L ASSOC. INS. COMM'RS, http://www.naic.org/cipr_topics/topic_cyber_risk. htm (last updated Dec. 12, 2017).

251. Matthew L. Jacobs & Daniel A. Johnson, *Pitfalls for Data Breach Coverage under Cybersecurity Insurance Policies*, LEXOLOGY (July 7, 2016), https://www.lexology.com/library/detail. aspx?g=adb8fb3e-e174-4448-b208-cea387ec6080.

252. Longenecker-Wells v. Benecard Servs. Inc., No. 1:15–CV–00422, 2016 U.S. Dist. WL 5576753, at *6 (M.D. Pa. Sept. 22, 2015), *aff'd*, 658 F. App'x 659, 2016 U.S. App. LEXIS 15696 (3d Cir. 2016).

253. TJ McCue, *Why Don't More Small Businesses Accept Credit Cards*, FORBES (Aug. 16, 2013, 9:04 AM), https://www.forbes.com/sites/tjmccue/2013/08/16/why-dont-more-small-businesses-accept-credit-cards/#3aa5e88015b4.

businesses that accept credit cards to comply with data security protocols; the Payment Card Industry Data Security Standards ("PCI DSS") apply to every merchant who accepts payment cards.[254] If these standards are breached, the businesses can suffer contractual penalties, including revocation of the right to accept the credit card.[255] In theory, these penalties apply to all businesses, large and small, but market realities cause the practice to be different.[256]

Upon a data security failure, large retailers are unlikely to lose the right to accept credit cards, even when they fail to follow PCI DSS.[257] TJX Companies, Inc., for example, owner of T.J. Maxx, Marshall's, and Home Goods, experienced a breach of about 100 million Visa and MasterCard accounts-–the largest ever experienced at that time in 2005.[258] The fraud-related losses involving Visa cards alone were about $70 million.[259] TJX had not complied with nine of the 12 security controls mandated by the PCI DSS when the breach occurred.[260] TJX knew before the breach that its wireless networks were insufficiently protected, but took no steps to mitigate the situation.[261] Nevertheless, TJX did not lose its ability to accept any major payment cards.[262] Had the TJX stores been denied charging privileges, the credit card companies would have sustained noticeable losses.

254. Mark Bernette, *How to Explain PCI Compliance Penalties to Beginners*, MERCHANT LINK (Nov. 10, 2014), http://www.merchantlink.com/how-explain-pci-compliance-penalties-beginners.

255. *See* DELL SECURE WORKS, PCI DSS COMPLIANCE FREQUENTLY ASKED QUESTIONS (2014), https://www.secureworks.com/~/media/Files/US/White%20Papers/DellSecureWorksECO1210NPCIDSSFrequentlyAskedQuestions.ashx.

256. *See generally supra* Part IV (highlighting the devastation that may occur to small businesses when statutory fines and litigation damages are incurred due to a data breach of customers' data).

257. *See* Gary G. Berg et al., *Analyzing the TJ Maxx Data Security Fiasco,* CPA J. 34–35 (2008); *see also Payments We Accept – T.J. Maxx – TJX Companies*, https://tjmaxx.tjx.com/store/jump/topic/ payments-we-accept/2400063 (last visited Feb. 20, 2018).

258. Joseph Pereira & Robin Sidel, TJX in Security-Breach Deal, Wall Street J. (Dec. 3, 2007), https://www.wsj.com/articles/SB119664612876511238 ("TJX Co s. has agreed to pay up to $40.9 million to resolve potential claims by banks that lost money . . . estimated to be the largest settlement by a retailer over lost credit-card data."); Jon Brodkin, *TJX data breach affected 94 million cards, banks allege,* NETWORK WORLD (Oct. 24, 2007), https://www.networkworld.com/article/2287572/lan-wan/tjx-data-breach-affected-94-million-cards—banks-allege.html; Larry Greenemeier, *Data, Theft, Pushback, and the TJX Effect – Details of the Largest Customer Data Heist in U.S. History are Beginning to Emerge*, INFO. WEEK (Aug. 13, 2007), http://sip-trunking.tmcnet.com/news/2007/08/13/ 2858485.htm.

259. Brodkin, *supra* note 258.

260. Jaikumar Vijayan, *TJX Violated Nine of 12 PCI Controls at Time of Breach*, COMPUTER WORLD (Oct. 26, 2007), http://www.computerworld.com/article/2539588/security0/tjx-violated-nine-of-12-pci-controls-at-time-of-breach—court-filings-say.html.

261. *Id.*

262. *See, e.g.*, *Payments We Accept – T.J. Maxx – TJX Companies*, https://tjmaxx.tjx.com/store/jump/topic/payments-we-accept/2400063 (last visited Feb. 20, 2018).

Small businesses are in a different bargaining position with the credit card companies.[263] Although they lack security expertise or dedicated in-house resources, they must still comply with PCI DSS in order to accept payment cards for purchases.[264] When a small business is compromised, it may immediately be required to hire a Qualified Security Assessor ("QSA")[265] to conduct a PCI assessment and issue a Report on Compliance ("ROC").[266] Aside from lost customer trust, the business faces contractual fines, detailed forensics investigation, and a loss of the ability to accept payment cards, any of which could put it out of business.[267] Since Visa loses little by declaring an individual small business no longer worthy of accepting its card, small businesses have sufficient incentive to comply with data security protocols to the best of their ability.[268]

In light of the lack of knowledge and sophistication of small businesses and the private penalties they already face, state legislatures should consider protecting their small businesses from any common law liability for credit card related data security, absent a specific contractual provision to the contrary. Using the number of owners, the number of employees, and annual revenue, states should be able to define small businesses that have neither: (1) the financial resources or the personnel to take on responsibility for data security; nor (2) sufficient revenue to warrant special lenient treatment by credit card companies.

This approach would shift the onus to credit card companies to provide adequate data security training, updates, and inspections to small businesses because affected consumers would turn to them in the event of a breach. Rather than requiring every physician, hairdresser, and restaurateur to get a degree in information technology, the burden will fall on parties with the knowledge, experience, and resources to battle the hackers. Consider the example of the physician's office again, now with a focus on payment card company capabilities. The physician's small business has contracts with vendors such as card companies and

263. *See* Catherine Clifford, *Rewards cards: Consumers Love'em, Retailers Don't,* CNN (July 14, 2011), http://money.cnn.com/2011/07/14/smallbusiness/rewards_credit_cards/index.htm.

264. *See* DELL SECURE WORKS, PCI DSS COMPLIANCE FREQUENTLY ASKED QUESTIONS (2014), https://www.secureworks.com/~/media/Files/US/White%20Papers/DellSecureWorksECO1210NPCIDSSFrequentlyAskedQuestions.ashx.

265. *See id.*

266. *Id.*; SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD REPORT ON COMPLIANCE 1 (2016), https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-ROC-Reporting - Template.pdf ("The . . . (ROC) is produced during onsite PCI DSS assessments as part of an entity's validation process. The ROC provides details about the entity's environment and assessment methodology, and documents the entity's compliance status for each PCI DSS requirement.").

267. DELL SECURE WORKS, PCI DSS COMPLIANCE FREQUENTLY ASKED QUESTIONS (2014), https://www.secureworks.com/~/media/Files/US/White%20Papers/DellSecureWorksECO1210NPCIDSSFrequentlyAskedQuestions.ashx.

268. *See* Clifford, *supra* note 263 (suggesting that small businesses are more dependent on credit card companies than vice versa).

banks for card processing. While the physician and staff members are not formally educated in information technology or cybersecurity management, the vendors are. The vendors have the technology infrastructure and the personnel to monitor network and system activity for anomalies. The vendors have software maintenance procedures to upgrade network and system software with necessary patches that repair security vulnerabilities. The vendors verify users with a multiple authentication system. The vendors have employee training programs and best-practice procedures to mitigate the high cybersecurity exposure from social engineering[269] and other risky behaviors.

The vendor cybersecurity management policy planning, implementation, and maintenance can extend beyond the vendor's own technology infrastructure to its small business clients. A vendor's cybersecurity preventive measures like virtual private networks, authentication systems, and intrusion detection applications can be packaged with the card payment systems. The vendors can also share employee training programs with small businesses and perform periodic inspections to ensure compliance. With this oversight, a small business can approximate the cybersecurity management of a large business.

The law of cybersecurity liability should recognize that small businesses do not have IT capabilities of their own. Their vendors are in a much better position to safeguard customer data.[270] Other possible improvements warrant discussion. Small businesses could be exempted from statutory fines in states that impose penalties for the failure to maintain "reasonable" data security.[271] Such fines do not serve as an incentive to businesses lacking the resources and background to institute security measures they don't know about; they can deter financially strapped small businesses from operating at all.[272] A related improvement would provide a safe harbor to small businesses that timely report a breach to their customers. If the business informed customers within a short time of learning about the breach, the small business would be immune from customer suits. This would encourage quick disclosure and remove the possibility of crushing liability.

269. In the context of cybersecurity, social engineering refers to the tactic of using deceptive means to fool someone into providing access to confidential information.

270. *See* Michael Delio, *Credit Card Cos. Watch Own Backs*, WIRED (Feb. 27, 2003, 2:00 AM), https://www.wired.com/2003/02/credit-card-cos-watch-own-backs; AVIVAH LITAN & JOHN PESCATORE, HUGE STOLEN CREDIT CARD CASE POSES RISKS TO MANY PARTIES 2 (2003), http://www.bus.umich.edu/kresgepublic/journals/gartner/research/113700/113712/113712.pdf; *see also* Doug Pollack, *It's a New Day for Payment Card Fraud Liability*, ID EXPERTS (Dec. 21, 2015), https://www2.idexpertscorp. com/knowledge-center/single/its-a-new-day-for-payment-card-fraud-liability (describing the ability of the Banks and Processors to pay for the initial litigation, and then later shifting the burden back to the businesses).

271. *See supra* Part III.

272. *See supra* Part III.

Small businesses face enormous liability and need legal protection.[273] Lawmakers should promptly address this cybersecurity liability threat with the suggested improvements or other legal safeguards. Absent intentional misbehavior, small business owners should not bear liability for injuries they have no hope of preventing.

CONCLUSION

Data breaches at mega-corporations have dominated the news, but hackers often target small businesses. Small business data can be more vulnerable because security measures are less sophisticated and the personnel using them are technologically unaware.

Courts and state legislatures have taken a number of approaches to liability for compromised data. Some courts have allowed contract, implied contract, unjust enrichment, negligence, misrepresentation, and statutory claims by customers (often asserted in class actions), while others have been leery of imposing liability at all. Nearly all the state legislatures have enacted data breach notification laws, some of which provide for stiff fines per affected consumer.

The standard for both common law and statutory claims is most often reasonableness. Did the business provide "reasonable" data security? Courts generally take into account the financial resources of the business in determining what is reasonable. The law should also take into account the technological expertise and education of the small business owner.

The lack of technical sophistication of small business owners suggests that the law should not hold them responsible for credit card data hacks. The burden should be on the card companies to train, update, and inspect small businesses permitted to use their cards. State legislatures should consider exempting small businesses from liability for statutory fines and providing a safe harbor against consumer suits when small businesses promptly notify customers of a breach. Lawmakers should address this issue for their small businesses as soon as possible.

273. *See* Rob Marvin, *10 Cybersecurity Steps Your Small Business Should Take Right Now*, PC MAG. (May 2, 2016), https://www.pcmag.com/article/344181/10-cybersecurity-steps-your-small-business-should-take-righ (stating that small businesses dealing with a cybersecurity challenge might mean life or death for a small business); , FIRST DATA MKT. INSIGHT, PAYMENT CARD DATA BREACHES: WHAT YOU NEED TO KNOW ABOUT YOUR RISK AND LIABILITY (2014), https://www.firstdata.com/ downloads/thoughtleadership/13405_0714_ Payment_Card_Data_Breach.pdf (stating that small merchants may be held liable for tens of thousands of dollars in fines, and identifying the liabilities the small businesses could face from various different entities).