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

Loren F. Selznick

Carolyn LaMacchia

Follow this and additional works at: http://digitalcommons.law.umaryland.edu/jbtl

Recommended Citation
Available at: http://digitalcommons.law.umaryland.edu/jbtl/vol13/iss2/4
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...

©2018 Loren F. Selznick and Carolyn LaMacchia

* 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.


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).


7. Id.; see infra notes 199–206.
CYBERSECURITY LIABILITY

Consumer harm. The corporate victim of the breach is blamed for failing to adopt reasonable cybersecurity measures. Customers with compromised data bring class action lawsuits and regulators seek fines. 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.

This legal trajectory poses a threat to small businesses. Small businesses face the same risk of data breach as their larger counterparts but lack the resources for cybersecurity measures. 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.

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. Because of their limited resources and technological skills, small businesses are easy prey for hackers. Large corporations employ teams of information technology personnel, an

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.
15. See Chen, supra note 3, at 100.
16. See id.
impossibility for small businesses. The larger businesses also mount multi-faceted defenses against data breaches, which smaller businesses cannot do.

A. Data Breach Targets

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

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

20. PRICEWATERHOUSECOOPERS, supra note 19, at 3.
21. Id.
22. Id.
25. Thielman, supra note 23.
27. PRICEWATERHOUSECOOPERS, supra note 19, at 5.
CYBERSECURITY LIABILITY

Boeing). Chipotle reported unauthorized network activity on its in-restaurant payment processor impacting several weeks of payment card transactions. 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 and the University of California, Berkeley. Newkirk Products, Inc., a service provider that issues healthcare identification cards, announced a data breach that affected up to 3.3 million people. 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. 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.

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

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/.
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/.
37. Id. at 43.
38. Id. at 42.
cyber-attacks targeted small businesses.\textsuperscript{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.\textsuperscript{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.\textsuperscript{41} All businesses, regardless of size, are faced with the growing probability of a breach by criminals who use more creative and complicated techniques.\textsuperscript{42} However, larger businesses are better equipped to mitigate the risk and recover from a breach.\textsuperscript{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.\textsuperscript{44} Small companies also hold valuable customer information.\textsuperscript{45} Hackers regard the data systems at small businesses as "low-hanging fruit."\textsuperscript{46}

Most cybercriminals seek personally identifiable information ("PII") for financial gain.\textsuperscript{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.\textsuperscript{48} Surprising to some, medical PII is a key to a very profitable door that is

\begin{itemize}
  \item \textsuperscript{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.
  \item \textsuperscript{41} Id.
  \item \textsuperscript{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=1496733378.
  \item \textsuperscript{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.
\end{itemize}
worth much more to cyber criminals than banking PII.\textsuperscript{49} Health records give cybercriminals information not just for fake medical claims but also for acquiring credit card accounts and mortgages.\textsuperscript{50}

Despite good intentions, a doctor’s office can be easy prey.\textsuperscript{51} Through continuing education, board-certified physicians are well-informed about medical protocol, insurance coverage, and the Health Insurance Portability and Accountability Act (“HIPAA”).\textsuperscript{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.\textsuperscript{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


\textsuperscript{50} Id.


\textsuperscript{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.
Loren F. Selznick & Carolyn Lamacchia

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. \textit{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

57. SYMANTEC, supra note 36, at 36.
Loren F. Selznick & Carolyn Lamacchia

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

63. Id.
64. Id.
66. Id.
68. See infra notes 69–80.
address information security. An insecure system would not be considered a source of reliable financial information because of the possibility of unauthorized transactions or data manipulation. A corporation may also need to address privacy protection laws including the HIPPA. The Federal Trade Commission can issue fines and require external auditing for several years for companies that fail to protect private information. 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.

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. 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. However, employees of the small businesses do not have information security analyst expertise. 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. Over 40 percent of small businesses report being ill-prepared to establish cybersecurity.

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

78. Id.
81. Id.
necessary to operate its computer systems. These multiple physical, logical, and human components are uniquely integrated to support business processes. 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. Regardless of their size, businesses need to protect their technology infrastructure from unauthorized, malicious events. 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.

Security professionals recommend that a business adopt a defense-in-depth approach which protects resources with several safeguards. An attacker must breach all countermeasures in the series to succeed. Implementing security policy with a defense-in-depth approach is complex and demands unique skills and knowledge for risk mitigation and incident response. An important component of the technology infrastructure is accessing the Internet. This raises multiple security issues. 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).
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 also 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.
88. Id.
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]
Several intrusion detection systems are available that look for anomalies in network traffic and alert information security professionals to possible breaches. These tools automatically record network activities then feed data into analytics software for analysis. The data analytics software provides reports of anomalies in network traffic for investigation by the security professional. A business can discover an intrusion early and possibly mitigate the damage. This type of protection is only common in large businesses.

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. Small businesses have neither the economic resources nor the in-house expertise to establish a secure cybersecurity infrastructure. Small businesses have less robust security in every aspect of the IT architecture. As a result, cybercriminals often target small businesses because their information technology infrastructure is easier to penetrate.

II. THEORIES OF LIABILITY

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

103. Id.
104. Id.
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.
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).
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. Others hold that as long as one plaintiff was defrauded, then other victims of the same hack have sufficient reason to fear imminent harm. A third group rejects increased risk of harm as too speculative.

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. Other types of damages gaining acceptance include benefit of the bargain damages, loss of value of personal information, consequential out-of-pocket damages, unjust enrichment (based on the failure to use payments to protect data in accordance with a privacy notice or on a would-not-have-patronized the business theory), and overpayment for a product that did not include the reasonable security the company represented it would provide. 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 holders.  

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).


CYBERSECURITY LIABILITY

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


134. Id.


also demonstrate how the defendant breached it, which generally takes the form of failing to implement reasonable security measures.\(^\text{138}\)

2. \textit{Implied contract}

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


\(^{139}\) 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.


\(^{143}\) Dittman, 154 A.3d at 326.

C Y B E R S E C U R I T Y L I A B I L I T Y

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

---


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

148. Id.


LOREN F. SELZNICK & CAROLYN LAMACCHIA

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).
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).
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.
236 Journal of Business & Technology Law

CYBERSECURITY LIABILITY

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

2. Breach of duty

How to allege the breach of duty is another area of contention.\textsuperscript{163} For some courts, the cyber invasion is enough on its own.\textsuperscript{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.\textsuperscript{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.\textsuperscript{166}


\textsuperscript{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.

\textsuperscript{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.


3. Causation

Businesses have questioned the causal relationship between the breach of duty and injury. 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. 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. 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.

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. In these states, negligence claims alleging purely economic loss unaccompanied by a physical injury are deficient as a matter of law. Absent a duty imposed by law or a special relationship between the plaintiff and defendant, the doctrine bars negligence claims for solely

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

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. One federal district court recognized such a claim was possible if the plaintiffs pled what defendant should have disclosed to avoid being misleading.

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

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. The problem is that it is an

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).
176. See id.
180. Id. at 975.
LOREN F. SELZNICK & CAROLYN LAMACCHIA

intentional tort, inappropreate when a defendant commercial business fails to protect against an unknown third-party hacker. 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. Breach of fiduciary duty claims have failed as well because the parties were not in a fiduciary relationship.

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. Generally, the federal statutes provide no private right of action, but some courts have used violations to support negligence per se claims. Some state statutes impose liability for failure to protect customer data.

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.
CYBERSECURITY LIABILITY

(“HIPAA”) and the Fair Credit Reporting Act. Courts agree that HIPAA provides no private right of action. 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. 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.

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

2. State Data Breach Notification Laws

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

---


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 Solns., 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).


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

---

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); CAL. CIV. CODE ANN. § 1798.81 5 et seq. (West 2017); 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. ANN. § 50-7a01 et seq. (2014) (explaining that the attorney general can enforce compliance and seek to injunction of further violations); 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); N.H. REV. STAT. ANN. § 1349.19 (West 2017); OHIO REV. CODE ANN. § 513.71 (West 2017) (providing that the attorney general can bring a civil action for failure to comply with law); OKLA. STAT. ANN. tit. 74 § 109-1 et seq. (West 2014) (explaining that the attorney general can seek actual damages or $100,000 per breach of security or series of related breaches); PA. CONST. STAT. § 12301 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); 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); S.C. CODE ANN. §§ 50-30-50, 50-30-510 (2017) (providing that the attorney general can seek injunctive relief, penalties and attorney’s fees); S.D. CODE ANN. §§ 17-16.1-1 et seq. (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. §§ 4-21-6 et seq. (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); UT CODE ANN. §§ 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); WASH. CODE ANN. § 63.01-101 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. 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. A private action, even in a state that allows one, may require an injury. Some states will not allow claims to move forward absent an injury beyond a statutory violation.

Private rights of action aside, many states impose stiff penalties on businesses that compromise customer data. 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. A number of state data breach statutes also require businesses to pay plaintiffs’ legal fees.

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. F LA. 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).


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).


206. See supra note 199 and accompanying text.

In some states, plaintiffs have successfully alleged breaches of consumer protection laws prohibiting deceptive and unfair trade practices. 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.” 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.” 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.

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. There is little case law yet on what is reasonable; many

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.
lawsuits have been dismissed before the courts reached the scope of the duty\textsuperscript{212} and data breach statutes often do not define it.\textsuperscript{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. . .”\textsuperscript{214} and has “emerged as the leading arbiter of what constitutes reasonable data security.”\textsuperscript{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.\textsuperscript{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.\textsuperscript{217} This caused one panel to wonder at a recent oral argument how businesses know whether they are in compliance.\textsuperscript{218} Reasonableness is a moving target.\textsuperscript{219} Despite this concern, the FTC has commenced over 200 breach of privacy cases.\textsuperscript{220}

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

\begin{footnotesize}
\begin{enumerate}
\item[212.] See id. But see OR. REV. STAT. ANN. § 646A.622(2) (West 2018).
\item[213.] 201 MASS. CODE REGS. 17.01-17.05 (2012). But see OR. REV. STAT. § 646A.622(2).
\item[215.] Id. at 242.
\item[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_response_brief_2017-0209.pdf (citations omitted).
\item[218.] Jimmy H. Koo, Judges Question FTC Data Security Standard at LabMD Argument, BLOOMBERG (June 23, 2017), https://www.bna.com/judges-question-ftc-data-security-standard-labmd-argument-445156/ (“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.”).
\item[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).
\item[220.] Pardau & Edwards, supra note 214, at 240.
\item[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).
\end{enumerate}
\end{footnotesize}
plaintiff must introduce evidence of the standard, the custom within the industry.\footnote{Silverpop Sys., Inc. v. Leading Mkt. Tech., Inc., 641 F. App’x 849, 852 (11th Cir. 2016).} 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.\footnote{Gordon & Argento, supra note 211.} 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.\footnote{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 Tricom 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.} More formality is expected at a large corporation.\footnote{Lough v. Brunswick Corp., 86 F.3d 1113, 1120–21 (Fed. Cir. 1996).} For example, courts do not expect a small business “owner to spend the time, or incur the expense, to document individual employment decisions.”\footnote{Hague v. Thompson Distrib. Co., 436 F.3d 816, 826 (7th Cir. 2006).} Small business owners are held to a reasonable small business owner standard.\footnote{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.”).} 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.”\footnote{United States v. Aruda, No. 05–00751, 2006 WL 2051336, at *3 (D. Haw. July 19, 2006).} Requiring a small business owner to do more can “make the cost of running a small business prohibitive.”\footnote{Roberts v. Tiny Tim Thrifty Check, 367 So. 2d 64, 65 (La. Ct. App. 1979).} The FTC has suggested that, for economic reasons, it expects less data security from small businesses.\footnote{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 and individuals cannot rely on their lack of sophistication to excuse a lack of diligence. On the other hand, courts regularly judge the reasonableness of behavior in light of education and experience. 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. Data security

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.").


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
LOREN F. SELZNICK & CAROLYN LAMACCHIA

issues lie like traps for small business owners who, in most cases, are untrained in technology security and often have little or no college education. And their financial vulnerability to customers may get worse. Courts have hinted that they may be more likely to impose liability in the future. 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.

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.

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. 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.

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.").
239. Id.
patients, could easily find themselves bankrupt. A diner, serving an estimated 200,000 meals in a year, 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. Identity theft protection for customers costs $25 to $60 per customer per year. Fees for late payments or new cards might have to be reimbursed for anyone whose card was misused. Soft damage claims like stress and lost time from canceling and replacing cards could cost much more. Statutes that require businesses to pay plaintiffs’ legal fees could involve significant expense.

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…” 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.”).


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
LOREN F. SELZNICK & CAROLYN LAMACCHIA

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.\footnote{249}

Many general liability insurance policies do not cover cybersecurity liability costs; insurance companies sell separate coverage for this type of peril.\footnote{250} Moreover, coverage might be rejected even under policies that include such risks.\footnote{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.\footnote{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.\footnote{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).


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.


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).


259. Brodkin, supra note 258.


261. Id.

Small businesses are in a different bargaining position with the credit card companies. 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. When a small business is compromised, it may immediately be required to hire a Qualified Security Assessor (“QSA”) to conduct a PCI assessment and issue a Report on Compliance (“ROC”). 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. 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.

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


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.”).


268. See Clifford, supra note 263 (suggesting that small businesses are more dependent on credit card companies than vice versa).
baths 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 engineering269 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. 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).