ALSTON & BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JANUARY 11, 2013

Data Breach Litigation – A New Frontier: *Anderson v. Hannaford Brothers Co.*

Zachary L. Neal[1]

Companies and government entities gather and aggregate an ever-increasing amount of consumer data. This data runs the gamut from the seemingly innocuous – like shopping habits – to the sensitive – like social security numbers and account numbers. As these entities gather and store data for their legitimate purposes, instances of unplanned releases of this information – or data breaches – are on the rise. And with data breaches come lawsuits from plaintiffs – or putative classes of plaintiffs – who fear their personal information may have been compromised.

The United States Court of Appeals for the First Circuit's recent decision in *Anderson v. Hannaford Brothers Co.*[2] discusses one important aspect of data breach litigation – whether plaintiffs can allege the necessary harm to survive a motion to dismiss. *Anderson* is one of the few instances where a court has concluded that the plaintiffs have alleged the necessary harm, meaning it is an important decision to consider in evaluating potential liability arising from a data breach.

Before discussing *Anderson*, this article first provides a general overview of how data breaches occur and why lawsuits tend to arise from them. This article then discusses another threshold issue – whether plaintiffs can establish Article III standing when suing in federal courts. If a plaintiff does not have standing, then the issues discussed in *Anderson* will not come into play. Finally, the article discusses *Anderson* in detail and explores its implications for future cases.

In sum, although *Anderson* will likely encourage even more data breach lawsuits, *Anderson* also underscores the difficulty plaintiffs will have in certifying classes even if they clear the other hurdles discussed in this article.

Data Breach Causes and Consequences

Data breaches may arise from a number of sources, including:

- Careless disposal of sensitive information (e.g., a company throws away sensitive information in a Dumpster);
- Inadvertent loss of sensitive information (e.g., an employee downloads sensitive information to some form of portable media and then misplaces that media);

---

[1] Mr. Neal is a Senior Associate in Alston & Bird LLP's Litigation and Trial Practice Group, and he is a member of Alston & Bird's Security Incident Management and Response Team. He is a graduate of the University of Georgia and the University of Pennsylvania Law School. The opinions expressed in this article are Mr. Neal's and do not necessarily reflect the views of Alston & Bird LLP or its potential or current clients.

[2] 659 F.3d 151 (1st Cir. 2011).

- Theft of sensitive information (e.g., an employee's laptop is stolen from his or her car); and
- Hacking to obtain sensitive information (e.g., a computer hacker breaches a company's network and obtains sensitive information).

After a data breach occurs, forty-six states require businesses or government entities to report breaches to consumers in certain circumstances. If notification is required, the data breach will become public, which, at least in the case of large data breaches, often leads to extensive coverage in both the mainstream media and on the internet. This publicity, in turn, tends to generate lawsuits, which are often brought as class actions in federal court. These suits are likely attractive to plaintiffs' lawyers because – at least in the case of large suits – there are potentially millions of class members. These class members are often sympathetic as almost everyone fears identity theft or other forms of fraud. And depending on the circumstances of the breach, plaintiffs have a number of claims to choose from, including negligence; breach of express or implied contract, State unfair and deceptive trade practices act statutes; State data breach notification laws; and the Fair Credit Reporting Act.

Article III Standing

A threshold issue in most data breach lawsuits is whether plaintiffs have standing to bring claims where they have not yet been the victim of identity theft or other fraudulent activity. In particular, courts have focused on whether plaintiffs have suffered an injury-in-fact where a data breach has occurred but the plaintiffs' information has not been misused.[3]

Circuit courts have split over whether plaintiffs have standing under such circumstances.[4] The Seventh and Ninth Circuits have been willing to find data breach plaintiffs have standing in certain circumstances even where they do not allege that they have been the victim of identity theft or other fraudulent activity.[5] The Seventh Circuit, for instance, found data breach plaintiffs, who alleged the data breach arose from a sophisticated hacking attack, had standing where no misuse of data was alleged but the plaintiffs alleged "a threat of future harm" from potential misuse of their data."[6] Similarly, the Ninth Circuit concluded that plaintiffs had standing even though they did not allege data misuse. One plaintiff, the court found, had standing where she claimed "generalized anxiety and stress" as a result of a data breach; other plaintiffs had standing under the circumstances where they alleged an increased risk of identity theft.[7]

Conversely, the Third Circuit has refused to find plaintiffs have standing where their information has not yet been misused.[8] The Third Circuit found that before information accessed in a data breach is misused any harm is speculative because whether harm will ever occur depends on the potential future actions of (at least in that case) an unknown party.[9] What must be shown to establish standing, the court found, are not allegations of hypothetical future harm, but allegations of actual or imminent harm.[10] The Third Circuit distinguished the Seventh and Ninth Circuit cases discussed above by finding that the allegations in both cases suggested more imminent harm.[11] The Seventh Circuit case, the court found, involved allegations of a "sophisticated, intentional and malicious" hacking attack.[12] And in the Ninth Circuit case someone had attempted – but

---

3 *Pisciotta v. Old Nat'l Bancorp*, 499 F.3d 629, 634 (7th Cir. 2007); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1142 (9th Cir. 2010).

4 *Compare Pisciotta*, 499 F.3d at 634 (holding such plaintiffs had standing) and Krottner, 628 F.3d 1139, 1142-43 (holding such plaintiffs had standing) *with Reilly v. Ceridian Corp.*, 664 F.3d 38, 43-46 (2011) (finding such plaintiffs did not have standing).

5 *Pisciotta*, 499 F.3d at 634; *Krottner*, 628 F.3d 1139, 1142-43.

6 *Pisciotta*, 499 F.3d at 634.

7 *Krottner*, 628 F.3d 1139, 1142-43.

8 *Reilly v. Ceridian Corp.*, 664 F.3d 38 (2011).

9 *Id.* at 42.

10 *Id.* at 43.

11 *Id.* at 44.

12 *Id.*

failed – to steal one plaintiff's identity.[13] More importantly, however, neither the Seventh nor Ninth Circuit decisions, the Third Circuit found, fully considered constitutional standing requirements as they applied to data breach claims. The Third Circuit thus found the Seventh and Ninth Circuit cases unpersuasive.[14]

Thus, at least in some cases, plaintiffs will be able to allege enough facts to establish standing. Either they will be able to allege actual harm, such as if they have already been defrauded, or their allegations will be enough to establish, at least in some court's view, a great enough threat of future harm to establish standing.

Actual Harm and Anderson v. Hannaford Brothers Co.

Even where plaintiffs can establish standing, they will still be left with the tall task of surviving a motion to dismiss their claims based on the argument that they have not alleged sufficient actual harm or damages under their substantive claims. For instance, in both the Seventh and Ninth Circuit cases discussed above, both courts found the plaintiffs had not alleged sufficient actual harm or damages to survive a motion to dismiss.[15]

In a departure from most other courts, however, the United States Court of Appeals for the First Circuit, in *Anderson v. Hannaford Brothers Co.*,[16] concluded that Maine law allows plaintiffs to recover certain damages arising from a data breach. In *Anderson*, the plaintiffs brought a class action complaint against Hannaford Brothers Company alleging several causes of actions arising from a data breach.[17] The data breach arose out of hackers accessing Hannaford's credit and debit card processing system.[18] The hackers allegedly stole credit and debit card numbers of 4.2 million Hannaford customers, leading to over 1,800 cases of fraud.[19]

Reviewing the trial court's decision partially granting and partially denying Hannaford's motion to dismiss, the First Circuit concluded that the plaintiffs had stated two causes of action under Maine law – breach of implied contract and negligence – and could likewise properly claim certain damages under those causes of action.[20] In analyzing the damage issue, the court focused on so-called "mitigation" damages.[21] The court first found under Maine law that damages must be "reasonably foreseeable."[22] The court then found that a plaintiff may "recover for costs and harms incurred during a reasonable effort to mitigate[]" harm.[23] "To recover mitigation damages, plaintiffs need only show that the efforts to mitigate were reasonable, and that those efforts constitute a legal injury, such as actual money lost, rather than time or effort expended."[24]

In deciding the plaintiffs had taken reasonable steps to mitigate their potential damages, including paying card replacement

---

13 *Id.*

14 *Id.; cf. Katz v. Pershing, LLC*, --- F.3d ----, 2012 WL 612793 (1st Cir. Feb. 28, 2012) (finding plaintiff lacked standing where she alleged only that a data breach could occur, not that one actually had occurred).

15 *Pisciotta*, 499 F.3d at 634 (finding Indiana law "would not permit recovery for credit monitoring costs" under plaintiffs' negligence and breach of implied contract claims); Krottner v. Starbucks Corp., 406 F. App'x 129 (9th Cir. 2010) (holding that plaintiffs had not alleged the necessary actual loss or damage to sustain a negligence claim under Washington law because plaintiffs alleged only the possibility of future harm).

16 659 F.3d 151 (1st Cir. 2011).

17 *Id.* at 153.

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.* at 162.

22 *Id.*

23 *Id.*

24 *Id.*

fees and buying credit insurance, the court focused on the fact that the case involved a sophisticated hacking attack that allegedly led to many fraud cases.[25] The court went to great lengths to distinguish data breach cases where no subsequent fraud had occurred or where there was no allegation that the data theft was anything other than incidental to the "theft of expensive computer equipment."[26] Instead, the court found, in this case, some people had already allegedly been fraud victims. It was thus foreseeable "that a customer, knowing that her credit or debit card data had been compromised and that thousands of fraudulent charges had resulted from the same security breach" would take steps to mitigate her potential damages.[27]

Although *Anderson* will likely encourage plaintiffs to file data breach lawsuits, *Anderson* also underscores the difficulty plaintiffs will likely have certifying a class for such claims, particularly a nationwide class. In *Anderson*, the First Circuit had to engage in extensive analysis of unsettled state law before concluding plaintiffs had properly alleged damages under a single state's law. The task of deciding whether multiple states' laws would allow for damages given the particular facts of a case will likely prevent plaintiffs from satisfying Federal Rule of Civil Procedure 23(b)(3)'s predominance requirement. Under the predominance requirement, plaintiffs must show through extensive analysis that any differences in state law are manageable.[28] This will likely prove to be a hard – if not impossible – task where more than a few states' laws are at issue, especially where the law in many states is an issue of first impression or in flux.[29]

---

25 *Id.* at 164-65.

26 *Id.* at 165.

27 *Id.* at 164.

28 *Sacred Heart Health Sys., Inc. v. Humana Military Healthcare Servs., Inc.*, 601 F.3d 1159, 1180 (11th Cir. 2010).

29 *See, e.g., Sacred Heart*, 601 F.3d at 1180-83 (district court abused its discretion in certifying a six-state class because the court had not engaged in a rigorous analysis to determine what state law variations existed); *Kirkpatrick v. J.C. Bradford & Co.*, 827 F.2d 718, 725 (11th Cir. 1987) (affirming district court's denial of a Rule 23(b)(3) multi-state class involving various state statutory and common law claims because "the differing standards of liability required by the laws of the various states would render class action treatment unmanageable").

ALSTON & BIRD LLP

CYBER ALERT

A Publication of the Security Incident Management & Response Team

WWW.ALSTON.COM JANUARY 11, 2013

Key Data Breach Jurisdictions: An Analysis

Jim Harvey,* Kristine McAlister Brown, Zach Neal and Kacy McCaffrey

Data breaches – often involving hundreds of thousands and sometimes even millions of individuals' data – are becoming more and more common place as companies, government agencies, and other entities continue to aggregate ever greater amounts of personal data. When a data breach occurs, companies are faced with deciding whether they have to notify the affected individuals about the data breach under various laws, including data breach notification laws in forty-six states, Puerto Rico, the District of Columbia, the Virgin Islands, Guam, and New York City.[1]

---

* Mr. Harvey is a Partner in Alston & Bird's IP & Technology Transactions Group, and he co-chairs the firm's Privacy & Security Group. He regularly counsels companies on sophisticated privacy, security, and network intrusion issues. His practice also involves security breach management and response, including everything from notification of the affected individuals, to e-discovery and internal investigations and law enforcement issues.

Ms. Brown is a Partner in Alston & Bird's Litigation and Trial Practice Group, and she is the chair of the firm's Telecommunications & Technology, and Privacy Litigation Practice Teams. Ms. Brown focuses her practice on complex commercial litigation, with an emphasis on class action, privacy, and antitrust litigation. Ms. Brown has also defended clients in privacy investigations brought by federal and state regulatory agencies.

Mr. Neal is a Senior Associate in Alston & Bird's Litigation and Trial Practice Group. He regularly represents clients in class actions and government investigations, including class action and government investigations involving privacy issues.

Ms. McCaffrey is an Associate in Alston & Bird's Litigation and Trial Practice Group. She regularly represents clients in class actions and government investigations, including class actions and government investigations involving privacy issues.

The opinions expressed in this article are the author's and do not necessarily reflect the views of Alston & Bird LLP, its partners or its potential or current clients.

[1] Alaska Stat. § 45.48.010 et seq.; Ariz. Rev. Stat. § 44-7501; Ark. Code § 4-110-101 et seq.; Cal. Civ. Code §§ 56.06, 1785.11.2, 1798.29, 1798.82; Colo. Rev. Stat. § 6-1-716; Conn. Gen Stat. 36a-701b; Del. Code tit. 6, § 12B-101 et seq.; Fla. Stat. § 817.5681; Ga. Code §§ 10-1-910, -911; Haw. Rev. Stat. § 487N-2; Idaho Stat. §§ 28-51-104 to 28-51-107; 815 ILCS 530/1 et seq. (Illinois); Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.; Iowa Code § 715C.1; Kan. Stat. 50-7a01, 50-7a02; La. Rev. Stat. § 51:3071 et seq.; Me. Rev. Stat. tit. 10 §§ 1347 et seq.; Md. Code Ann. Com. Law § 14-3501 et seq.; Mass. Gen. Laws § 93H-1 et seq.; Mich. Comp. Laws §§ 445.61, 445.72; Minn. Stat. §§ 325E.61, 325E.64; Miss. Code Ann. § 75-24-29; Mo. Rev. Stat. § 407.1500; Mont. Code §§ 30-14-1704, 2-6-504; Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807; Nev. Rev. Stat. §§ 603A.010 et seq., 242.183; N.H. Rev. Stat. §§ 359-C:19, -C:20, -C:21; N.J. Stat. 56:8-163; N.Y. Gen. Bus. Law § 899-aa; N.C. Gen. Stat §§ 75-60 – 75-65; N.D. Cent. Code § 51-30-01 et seq.; Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192; Okla. Stat. § 74-3113.1 and § 24-161 to -166; Oregon Rev. Stat. § 646A.600 et seq.; 73 Pa. Stat. § 2303; R.I. Gen. Laws § 11-49.2-1 et seq.; S.C. Code § 39-1-90; Tenn. Code § 47-18-2107, 2010 S.B. 2793; Tex. Bus. & Com. Code § 521.03, Tex. Ed. Code 37.007(b)(5) (2011 H.B. 1224); Utah Code §§ 13-44-101, -102, -201, -202, -310; Vt. Stat. tit. 9 § 2430 et seq.; Va. Code § 18.2-186.6, § 32.1-127.1:05 (effective January 1, 2011); Wash. Rev. Code § 19.255.010, 42.17.31922; W.V. Code §§ 46A-2A-101 et seq.; Wis. Stat. § 134.98 et seq.; Wyo. Stat. § 40-12-501 to -502; D.C. Code § 28- 3851 et seq.; 9 GCA § 48-10 et seq. (Guam); 10 Laws of Puerto Rico § 4051 et. seq.; V.I. Code § 2208; N.Y.C. Code § 20-117. The four states without notification obligations are Alabama, Kentucky, New Mexico and South Dakota.

This article does not discuss breach notification obligations under the Health Insurance Portability and Accountability Act (HIPAA) or Gramm-Leach Bliley Act (GLBA).

These laws – as laws often do – vary widely from jurisdiction to jurisdiction. But for many organizations facing a data breach involving individuals from across the country, if they have to notify under any jurisdiction's law, they will voluntarily notify under all jurisdictions' laws. Organizations take this approach because both regulators and the organization's customers expect – and, indeed, sometimes demand – the organization to notify them of the breach even if not required to do so by law. In particular, large breaches, even if only reported in one or a handful of jurisdictions, will likely garner widespread, negative media coverage. For most organizations, then, the critical question will be whether they have to notify under any jurisdiction's law. [2]

This article focuses on the three jurisdictions – New Jersey, Connecticut, and Puerto Rico – that have a lower "access" notification threshold. In these jurisdictions, companies must notify possibly affected individuals if the company reasonably believes an unauthorized person – like a computer hacker – has "access to" or has "accessed" personal information, even if the unauthorized person did not actually "acquire" that data.

In contrast to the "access" standard employed by New Jersey, Connecticut and Puerto Rico, the remaining states and territories have adopted a higher standard that requires notice only when a consumer's personally identifiable information has been "acquired" or is reasonably believed to have been acquired. Although the majority of states do not define the key term "acquire," Vermont's recent statutory amendment adopted guidance put forth by the California Office of Privacy Protection regarding how to determine whether data has been acquired. Vermont previously used the "access" standard for breach notifications. Vermont, however, recently amended its statute to define a security breach as an "unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that comprises the security, confidentiality, or integrity or a consumer's personally identifiable information maintained by the data collector."[3] In determining whether data has been acquired under Vermont's statute, one should consider whether: (i) information is in the physical possession or control of an unauthorized person, (ii) the information has been downloaded or copied, (iii) the information was used by an unauthorized person (such as to open a fraudulent account or used in identity theft), or (iv) the information has been made public.[4]

The lower-threshold "access" jurisdictions of New Jersey, Connecticut and Puerto Rico also fail to provide a definition of the key term "access." But "access," when compared to acquire, is clearly a lower standard, meaning someone may have access to or have accessed information without actually acquiring the information.

In sum, when information has not actually been acquired, whether to notify under the "access" standard is a fact-intensive inquiry that requires careful analysis and judgment. This article discusses when notification may be necessary under the access standard. First, however, we discuss common features of breach notification laws and common factual scenarios that may give rise to breach notifications obligations to lay the groundwork for analyzing whether notification is necessary under the "access" standard.

Breach Notification Laws

Although the particulars of breach notification laws differ in important ways, certain broad themes apply to most of these laws. In general, these laws apply when an unauthorized person accesses or acquires an individual's unencrypted or unredacted personal information. Personal information is not consistently defined in the various laws, but, generally speaking, personal information includes a person's name (either first name or first initial and last name) and some additional sensitive

---

[2] Texas law originally required any entity that conducted business in Texas to notify any "Texas resident" whose sensitive personal information was, or was reasonably believed to have been, acquired by an unauthorized user. This law was recently amended to require any such entity to notify all affected "individuals" regardless of whether they live in Texas—which is a notification requirement not found in other state statutes. The law went into effect on September 1, 2012. How this broad notification requirement will be interpreted in the future remains to be seen.

[3] 9 V.S.A. § 2430(8)(A) (amended and effective as of May 8, 2012).

[4] *See* 9 V.S.A. § 2430(8)(C); *see also* Recommended Practices on Notice of Security Breach Involving Personal Information" at 12, California Office of Privacy Protection, January 2012 (available at http://www.privacy.ca.gov/business/recom_breach_prac.pdf).

information, most often including a person's Social Security number, driver's license or state identification card number, or a financial account number in combination with additional information that would allow access to the account.[5]

Data breaches can occur in a number of different ways. While many breaches involve computer or database hackers, a breach can also occur by loss or improper destruction of paper records, misplacement or theft of portable electronic storage devices, inadvertent exposure of confidential data on a public website, employees accessing or disclosing information outside of their authorization, or improper disposal of digital media – to name a few.

When dealing with an unauthorized intrusion into a computer network, gathering information about the breach itself, the hacker's methods, and the personal information involved are essential steps to the fact intensive inquiry surrounding breach notification events. Understanding where the hacker was on a computer system or database plays directly into the investigation and evaluation as to whether he or she had "access" to sensitive personal information of a consumer, or whether any information was actually "acquired." Is malware present on the system? Are files missing, moved, or showing evidence of capture or exportation? Do transaction logs provide evidence of a hacker's activities? Have all traces of a hacker's presence been forensically removed by the bad actor? Have passwords been obtained by the bad actor? These are just a few of the questions to be asked when investigating a data breach and assessing notification obligations under the "access" or "believed to have been accessed" standard of Puerto Rico, New Jersey, and Connecticut.

Data breaches are time consuming, expensive to investigate and rectify, and they have the potential to damage a company's reputation. Determining the source and extent of the breach is essential to notifying the correct individuals and to preventing future breaches.

Puerto Rico

Puerto Rico has the lowest notification threshold of any jurisdiction. Puerto Rico's breach notification statute requires notification by any entity that is the owner or custodian of a database that includes personal information of citizens of Puerto Rico when that database's security has been breached.[6] A security breach is "any situation in which it is detected that access has been permitted to unauthorized persons or entities to the data files so that the security, confidentiality or integrity of the information in the data bank has been compromised."[7]

No cases in Puerto Rico interpret the statute or provide insight into the intended definition of "access" or "compromised." But all uses of either word in the laws and case law in Puerto Rico indicate the typical meaning of the words.[8] [9] Given this, a court would likely look to the dictionary definition of access, which Merriam-Webster's Collegiate Dictionary defines as "permission, liberty or ability to enter, approach, or pass to and from a place . . ." and as the "freedom or ability to obtain or make use of

---

[5] Other information, in conjunction with a name, that may be considered personal information, includes, for example, certain medical information (e.g., Arkansas, California, Missouri), health insurance information (e.g., California), biometric data (e.g., Iowa, Nebraska, North Carolina), Taxpayer Identification Number (e.g., Maryland), passport number (e.g., North Carolina, Oregon), date of birth (e.g., North Dakota), mother's maiden name (e.g., North Dakota), DNA profiles (e.g., Wisconsin), and work-related evaluations (e.g., Puerto Rico).

[6] 10 L.P.R.A. § 4052.

[7] 10 L.P.R.A. § 4051.

[8] For example, an act guaranteeing access to information for disabled persons defines the term as "the capability and ability to use and receive data and operate technological assistance equipment." PR ST T. 3 § 8310. *See also Lopez-Mendez v. Lexmark Intn'l., Inc.*, 680 F.Supp.2d 357, 372 (D.P.R. 2010) (party did have "access as an administrator, however, and was therefore able to enter plaintiff's e-mail account").

[9] A related Act requires a party to "[n]otify the certifying authority and the register authority if his/her electronic signature has been *compromised* by unauthorized third parties or has been unduly used, as soon as he becomes aware." PR ST T. 3 § 8705 ("Electronic Signature Act").

something."[10] A court would likely also look to the dictionary definition of compromise, which the same dictionary defines as "to reveal or expose to an unauthorized person esp[ecially] to an enemy." If a bad actor has the ability to enter, it also likely means the data is compromised because the information has been exposed to the bad actor.

Thus, under Puerto Rico law, notification is likely necessary if the bad actor had the ability to access the place where personal information was stored. Many questions come into play when analyzing this ability to "access" personal data. Did the bad actor have access or the ability to access the computer? The entire network? A particular database? Specific files or tables contained in a database? Was any information exported from a file or network? Where—in relation to where the bad actor may have had access—was personal information located? A court or regulator might find notification necessary when an unencrypted, non-password protected computer is stolen. In that case, the bad actor would have the ability to enter the computer and the information would also be exposed to the bad actor because he had the ability to enter the computer. Similarly, a court or regulator might find notification necessary where a bad actor had access to a particular network or database containing personal information, even if there is no evidence that the bad actor actually entered that particular database. In sum, whether a breach becomes a notification triggering event is a highly fact intensive inquiry requiring a complete understanding of the facts.[11]

New Jersey

New Jersey's breach notification statute is more complex than Puerto Rico's statute and allows an entity more flexibility in deciding whether notification is necessary. New Jersey's breach notification statute defines "breach of security" as "unauthorized access to electronic files, media or data containing personal information that compromises the security, confidentiality or integrity of personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."[12] The statute goes on to state that any business conducting business in New Jersey "shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person."[13] But "[d]isclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible."[14]

---

[10] Two federal statutes, in particular, that use the word "access" or some variant in the computer fraud context may shed light on how "access" should be interpreted in the state breach notification context. *See* Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 *et seq.*; Stored Communications Act ("SCA"), 18 USC § 2701 *et seq.* Although neither of these statutes defines the term access, courts interpreting the meaning of access under these statutes have defined the term broadly and similarly to the way state courts in this article have interpreted the word. *See, e.g.*, CFAA: *United States v. Morris*, 928 F.2d 504, 510-11 (2d Cir. 1991) (adopting, in a CFAA case, at least implicitly, the standard of looking for communications that physically entered the computer as evidence of "access"); *EV Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 579-82 (1st Cir. 2001) (describing one's use of a scraper to gather pricing information from a competitor's website as an "access" of that website); Sealord Holdings, Inc. v. Radler, No. 11-6125, 2012 WL 707075 at *7 (E.D. Pa. Mar. 6, 2012) (finding defendants' repeated attempts to log on to plaintiff's computer from various IP addresses constituted "access."); Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1272-73 (N.D. Iowa 2000) (defining, in a CFAA case, access pursuant to Merriam Webster's Dictionary as "to gain access to" and "the freedom and ability to make use of something"); SCA: United States v. Smith, 155 F.3d 1051, 1058 (9th Cir.1998) (interpreting the word access in the SCA to mean "being in position to acquire the contents of a communication"); Shefts v. Petrakis, No. 10-cv-1104, 2011 WL 5930469 at *4 (C.D. Ill. Nov. 29, 2011) (finding that regardless of whether the defendant had read plaintiff's emails or not, he had put himself in a position to acquire the contents of plaintiff's communications and had therefore "accessed" the account).

[11] See Kerr, Orin S., Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1619-628 (2003) (offering additional analysis on what may be deemed "access" from both a virtual and physical reality standpoint).

[12] N.J. Stat. § 56:8-161.

[13] N.J. Stat. § 56:8-163(a).

[14] *Id.* The statute also requires that "[a]ny determination shall be documented in writing and retained for five years." *Id.*

Unlike in Puerto Rico, then, an entity's duty to notify in New Jersey does not turn on whether the bad actor could access the data. Rather, an entity is only required to notify people if "personal information was, or is reasonably believed to have been, *accessed*" by the bad actor.[15] The difference between access and accessed is significant: access can be thought of as having the ability to open the door; accessed means the person not only had the ability to open the door but actually opened the door.

New Jersey's statute, however, cuts back on this distinction some because an entity must also notify affected individuals if the entity reasonably believes the bad actor accessed personal information.[16] Although no case has interpreted this provision, New Jersey courts have interpreted what it means to have a reasonable belief in other contexts. These cases show that whether someone has a reasonable belief is judged by an objective reasonable person standard.[17] This standard generally focuses on what a reasonable person in the defendant's position would have believed under the circumstances.[18] A person's reasonable belief need not be established by direct evidence; circumstantial evidence can be enough to show an objectively reasonable belief.[19] Indeed, all facts and the totality of the circumstances can be considered.[20]

As an example, assume a bad actor has access to a server. The server itself has hundreds of databases, and a handful of those databases contain personal information. Further assume that no direct evidence indicates that any of the databases with personal information were actually accessed. At that point, a reasonable person could conclude that notification is unnecessary because only a fraction of the databases contained personal information and no direct evidence indicates those databases were accessed.

A reasonable person, however, could delve further into the issues and consider factors such as the sophistication of the hackers, the hacker's motivation (if known), the financial value of the personal information in the databases, and whether the bad actor had the ability to erase his or her electronic tracks, indicating less importance should be placed on evidence – or lack of evidence – of direct access to the database. For instance, the bad actors and their motives may be known. If the hackers' identity is known and it is known that they breach systems to simply prove a point, and no direct evidence indicates that they accessed the databases in question, then an entity might reasonably conclude it does not reasonably believe the databases were accessed. Conversely, if the bad actors are known for breaching systems and specifically targeting personal information for eventual resale, a reasonable entity might conclude notification is necessary.

Even if an entity reasonably believes information has been accessed, that entity does not have to disclose the data breach "if the business or public entity establishes that misuse of the information is not reasonably possible."[21] Again, no case or other authority interprets this provision. And, unfortunately, no other New Jersey case law sheds much light on this provision.

That leaves the language of the statute itself. As an initial matter, the statute poses a high burden for a company choosing to take advantage of this provision: the company must "establish[]" misuse is "not reasonably possible." The "establish" provision suggests that the company must marshal convincing evidence, not rely on its subjective beliefs. The "not reasonably possible" provision of the statute also suggests an objective standard. Thus, it will be the entity's burden to prove that a reasonable person would believe it is not reasonably possible the accessed information could be misused.

---

15 *Id.* (emphasis added).

16 *Id.*

17 *E.g., State v. Galicia*, 2010 WL 3834828 (N.J. Super. App. Div. Sep. 22, 2010) (applying the objectively reasonable person standard to self-defense claim); *State v. J.G.*, 990 A.2d 1122 (2010) (applying the objective reasonable person standard to the priest-penitent privilege).

18 *See State v. Lassiter*, 2009 WL 1706005 (N.J. Super. Ct. App. Div. June 19, 2009).

19 *Guslavage v. City of Elizabeth*, 2009 WL 5125017 (N.J. Super. Ct. App. Div. Dec. 30, 2009) ("The qualifier 'reasonably' is generally understood to mean rationally supported . . . not actually so[.]").

20 *J.G.*, 990 A.2d at 1131; *see also State v. Villanueva*, 862 A.2d 1195 (N.J. Super. Ct. App. Div. 2004) ("The reasonableness of the belief is a jury issue.").

21 N.J. Stat. § 56:8-163(a).

Despite this high standard, an entity could argue that unless the entity reasonably believes the data was acquired – as opposed to merely accessed – misuse is not reasonably possible. After all, if the bad actor accessed a large data base containing records for hundreds of thousands or millions of customers, the bad actor could likely not misuse this information unless it was actually acquired and exported. This is so because the bad actors could not likely reasonably absorb the information in the database by merely viewing the database, meaning they could not misuse the information in the future. Where the data was actually acquired, however, it will be hard to take advantage of this exception.

Connecticut

Connecticut's breach notification statute is similar in relevant respects to New Jersey's statute. Connecticut's breach notification statute defines "breach of security" to mean "unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable[.]"[22] Any person conducting business in Connecticut "shall disclose any breach of security following the discovery of the breach to any resident of this state whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person through such breach of security."[23] But "[s]uch notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."[24]

The first question under Connecticut law, then, is if the entity's "personal information was, or is reasonably believed to have been, accessed by an unauthorized person." Again, no case law interprets this provision.[25] Connecticut courts, however, have interpreted what "reasonably believed" or "reasonably believes" means in other contexts. In general, courts have found that such language creates an objective standard.[26] This means that the person's reasonable belief will be judged from the perspective of a reasonable person with the same information.[27]

As discussed in relation to New Jersey's breach notification statute, reasonable people could reach different conclusions regarding whether bad actors accessed information depending on the circumstances of the data breach. Thus, Connecticut law is similar to New Jersey law in this respect.

---

22 Conn. Gen. Stat. § 36a-701b(a).

23 Conn. Gen. Stat. § 36a-701b(b).

24 *Id.*

25 One Connecticut case has rejected a claim that a company had to notify anyone regarding an alleged data breach. This case, however, is of little help in deciding whether notification is required. The case was decided on a motion to dismiss and had little analysis. Essentially, a bank claimed that a company providing it with copiers should have told the bank that the copiers could store information. When the copiers were later discarded without first wiping the copiers' memory, the bank sued the company providing the copiers, claiming the copier company should have notified the bank's customers of the potential breach. The court dismissed the case because the bank did not allege any facts even suggesting anyone had ever even attempted to access the copiers post disposal, much less access the information in their memory. Thus, the court did not analyze whether the copier company should have reasonably believed the information was accessed. *Bank v. Ikon Office Solutions, Inc.*, No. 3:10–cv–1067 (WWE), 2011 WL 2633658 (D. Conn. July 5, 2011).

26 *See State v. Wilkins*, 692 A.2d 1233, 1237 (Conn. 1997).

27 *See id.; State v. Wilchinski*, 700 A.2d 1, 10 (Conn. 1997) (explaining that a jury looks at all of the available evidence and circumstances to determine what a reasonable person should or would have done). In at least one circumstance Connecticut courts have used a subjective-objective test to determine someone's reasonable belief. Specifically, in the context of self-defense, Connecticut courts determine a person's reasonable belief (1) by looking at whether the defendant in fact believed his or her actions were proper and (2) by looking at whether his or her belief was reasonable "from the perspective of a person in the defendant's circumstances." *State v. Saunders*, 838 A.2d 186 (Conn. 2004). Under either standard, however, the reasonable person test will be at issue.

- Like in New Jersey, Connecticut has a safety-valve provision that nullifies the need for notification in certain situations. In Connecticut, even if an entity reasonably believes personal information was accessed, that entity does not have to notify people "if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed."[28] Importantly, an entity can only take advantage of this carve out if it consults with federal, state and local agencies about the breach. An entity hoping to take advantage of this exemption should expect close questioning from law enforcement. And an entity should also keep in mind that it could – depending on the circumstances and relevant jurisdiction's law – be creating discoverable communications and documents during this process.

An entity can also only take advantage of this provision if it determines "the breach will not likely result in harm" to the affected individuals. This standard is similar to New Jersey's safety-valve standard that notification is not necessary if "misuse of the information is not reasonably possible." Connecticut's standard, like New Jersey's standard, requires the entity to make a judgment call based on the available information. And, again, if a large amount of data is accessed, but there is no evidence that the bad actors actually acquired the data, there could be a good argument that harm is not likely to result.

In sum, whether notification is necessary, is an inherently fact-intensive question that is often complex and will require the entity to weigh many considerations. If a situation exists where the higher "acquire" standard is not met, then the analysis will turn on whether the lower threshold--or "access" standard-- *is* met. As an entity decides whether to notify affected individuals, it must consider how regulators and potential plaintiffs could view their notification decision. Regulators and plaintiffs will likely be inherently skeptical of an entity's decision not to notify. But if an entity notifies where no notification is necessary or required, the notification could cause unnecessary angst to those notified and generate meritless lawsuits. Thus, although an entity may believe its safest course is to notify potentially affected individuals even if not required, there may be negative consequences from the decision. Careful consideration is thus necessary.

---

[28] Conn. Gen. Stat. § 36a-701b(b).