www.laboremploymentlaw.org

the Checkoff

The Florida Bar
Vol. LXI, No. 1
SEPTEMBER 2021

A PUBLICATION OF THE FLORIDA BAR LABOR & EMPLOYMENT LAW SECTION

IN THIS ISSUE

Gil v. Winn-Dixie Will the Wave of ADA Website Cases Subside?

By Kelly M. Peña, Miami

The Americans with Disabilities Act[1] (the ADA) first became law over thirty years ago, in 1990. Title III of the ADA[2] was enacted to prohibit private businesses from discriminating against individuals or patrons with disabilities if those businesses qualify as places of public accommodation, such as hotels, restaurants, and retail establishments.[3] Under Title III, places of public accommodation are required to remove physical barriers to access for individuals with disabilities, so long as it is "readily achievable."[4]

Title III has a published set of regulations and "Standards for Accessible Design" containing specific requirements for physical locations so that persons with disabilities may access a restaurant, hotel, or another place of public accommodation, despite any mobility issues or other impairments. The Standards for Accessible Design provide detailed descriptions, with specifications for parking spaces, restrooms, transaction counters, and signage, among other things.

See "Gil v. Winn-Dixie," page 14

Cyberattacks Surge During the Pandemic and So Does the Potential for Liability

Barron F. Dickinson, Tampa

The frequency of cyberattacks dramatically increased by 600% after the shift to remote work following the onset of the COVID-19 pandemic.[1] According to a report by IBM, the average total cost of a data breach was $3.86 million dollars in 2020, and the average amount of time it took a company to identify and contain a data breach was 280 days.[2] In addition, 76% of those surveyed by IBM reported that remote work would likely increase the time necessary to identify and contain a data breach.[3]

Prior to the pandemic, a 2017 study conducted by Nationwide Insurance estimated that 58% of U.S. businesses have experienced a cyberattack.[4] More than 20% of those victims reported spending at least $50,000 on the breach and needing more than six months to recover.[5] Notwithstanding, less than half of the businesses surveyed had security policies and practices in place.

According to a report by the information security company Shred-It, employee negligence remains the primary cause of data breaches.[6] The report found that 47% of

See "Cyberattacks Surge," page 15

is a developing area of law in Florida and the Eleventh Circuit. The Eleventh Circuit has held that an elevated risk of identity theft and evidence of a data breach alone is insufficient to establish an injury-in-fact, which is necessary to confer standing under Article III of the United States Constitution.[13] Instead, a plaintiff must allege that the data breach placed him or her at a "substantial risk" of future identify theft or that the identity theft was "certainly impending."[14]

The Ninth Circuit has also dismissed claims brought by employees against the employer following the theft of their personal confidential information, finding that the injuries claimed by the employees were speculative in nature, did not reflect any actual harm, and that the employer did not owe a duty to its employees to prevent their confidential information from being stolen by third parties in a data breach.[15]

Notwithstanding, plaintiffs in Florida have enjoyed a degree of success recently in surviving the motion-to-dismiss stage when alleging data breach claims that were premised on a theory of negligence.[16] For example, the Southern District of Florida in *Burrows v. Purchasing Power, LLC*[17] held that theft of personal information accompanied by the filing of an unauthorized tax return constitutes injury-in-fact that was fairly traceable to the plaintiff's employer and a third-party benefits company.[18] The Middle District of Florida reached a similar conclusion in *Torres v. Wendy's International, LLC*,[19] where it held that that a $3 late fee resulting from a data breach, the loss of credit card reward points, and the loss of cash-back rewards each independently established cognizable injuries-in-fact to withstand a motion to dismiss.

Notification Obligations

Outside the litigation realm, nearly all fifty states, including Florida and the District of Columbia, require public and private employers to notify affected individuals of security breaches involving personally identifiable information. In addition to notifying law enforcement, under Florida's Information Protection Act of 2014 (FIPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), employers also likely have an obligation to notify their employees of a data breach that resulted in the theft of their personal information.

Under FIPA, which applies to both governmental and private entities, a data breach, or "breach of security," is defined as "unauthorized access of data in electronic form containing personal information."[20] However, good faith access of personal information by an employee or agent of the entity does not constitute a breach of security, provided that the information is not used for a purpose unrelated to the business or subject to further unauthorized use.

The term "personal information" includes an individual's first name or first initial and last name reflected on the following sources of data: 1) social security numbers, 2) identity verification documents such as a driver's license, ID card, and passport, 3) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account, 4) medical records 5) health insurance documents, and 6) a user name or e-mail address, in combination with a password or security question and answer, that would permit access to an online account.[21] Notwithstanding, the term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity, or information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

FIPA requires governmental and private entities to take reasonable measures to protect and secure data in electronic form containing personal information.[22] Following a data breach that results in the unauthorized access of an individual's personal information, an entity is required to notify each individual whose information was accessed of such breach within thirty days.[23] However, notice to the affected individuals is not required if, after an appropriate investigation and consultation with relevant federal, state, or local law enforcement agencies, the entity reasonably determines that the breach has not and will not likely result in identity theft or any other financial harm to the individuals whose personal information has been accessed.[24] Such a determination must be documented in writing and maintained by the entity for a period of at least five years. The entity must also provide a copy of the written determination to the Florida Department of Legal Affairs (FDLA) within thirty days after the determination.

Entities must provide the required notice to an affected individual by sending written notice to the individual's last known mailing address or an e-mail to the individual's last known e-mail address.[25] The required notice to an individual with respect to a breach of security must include, at a minimum: 1) the date, estimated date, or estimated date range of the breach of security, 2) a description of the personal information that was accessed or reasonably believed to have been accessed as a part of the breach of security, and 3) information that the individual can use to contact the entity to inquire about the breach of security and the personal information that the entity maintained about the individual.[26]

Notwithstanding, covered entities may provide substitute notice in lieu of direct notice if such direct notice is not feasible because the cost of providing notice would exceed $250,000, because the affected individuals exceed 500,000 persons, or because the entity does not have an e-mail address or mailing address for the affected individuals.[27] Such substitute notice must include the following: 1) a conspicuous notice posted on the website of the entity if the entity maintains a website, and 2) notice published in print and broadcast media, including major

media in urban and rural areas where the affected individuals reside.[28]

If a data breach affects more than 500 individuals, an employer must also notify the FDLA within this same time frame.[29] The written notice to FDLA must include: 1) a synopsis of the events surrounding the breach at the time notice is provided, 2) the number of individuals in this state who were or potentially have been affected by the breach, 3) a description of any services related to the breach being offered or scheduled to be offered, without charge, by the covered entity to individuals, and instructions on how to use such services, 4) a copy of the required notice provided to the affected individuals, and 5) the name, address, telephone number, and e-mail address of the employee or agent of the employer from whom additional information may be obtained about the breach.[30] The employer must also provide the following information to FDLA upon its request: 1) a police report, incident report, or computer forensics report, 2) a copy of the policies in place regarding breaches, and 3) the steps that have been taken to rectify the breach.[31]

If a data breach affects more than 1000 individuals, an entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in the Fair Credit Reporting Act, of the timing, distribution, and content of the notices.[32] In addition, notice that is provided pursuant to rules, regulations, procedures, or guidelines established by the entity's primary or functional federal regulator is deemed to be in compliance with the notice requirements of FIPA if the entity notifies affected individuals in accordance with the rules, regulations, procedures, or guidelines established by the primary or functional federal regulator in the event of a breach of security.[33] An entity that timely provides a copy of such notice to FDLA is deemed to be in compliance with the notice requirement.

Similarly, a "covered entity" under HIPAA is required to notify individuals whose protected health information has been improperly accessed of a breach within sixty days of discovering the breach.[34] In addition, if the breach results in the unauthorized disclosure of information relating to more than 500 individuals, an entity is required to notify the media and the Secretary of Health and Human Services within this same time frame.

Neither FIPA nor HIPAA provides a plaintiff with a private right of action to enforce these statutes.[35] However, entities may still face investigations and stiff fines from the State of Florida and the federal government should they fail to satisfy their obligations under FIPA and HIPAA. For example, FIPA provides for a civil penalty of up to $500,000 for violations of its notice requirements.[36]

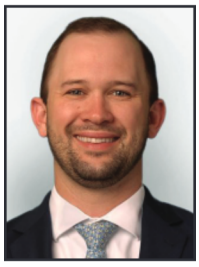
Legislation Proposed in Florida

During this year's legislative session in Florida, a bill titled "Florida Privacy Protection Act," HB 969, was introduced, containing some of the strictest data privacy provisions in the United States.[37] In addition to creating a private right of action for consumers affected by a data breach, HB 969 also proposed to expand the definition of personal information to include biometric information. The bill also provided that a consumer whose protected information was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of a covered entity's failure to implement and maintain reasonable security procedures could bring a civil action for damages or injunctive relief. Potential damages ranged from $100 to $750 per consumer, per violation or actual damages, whichever was greater. Despite initially passing the House, the bill as amended by the Senate died in House Committee on April 30, 2021, the last day of the Florida legislative session.[38]

Proactive Measures

Public and private entities should always take proactive measures to protect personal and confidential information. In particular, organizations should install encryption and wiping software on all employee-issued devices, require complex passwords, and establish mandatory and recurring cybersecurity training to educate employees on the latest cybersecurity attack methods and on best practices regarding data protection. Employers may also want to consider adopting and enforcing cybersecurity policies in their handbook as more than 50% of all security incidents are caused by employees. In drafting such policies, employers should also consider creating a cybersecurity incident response plan that includes the formation of a dedicated response team.

Finally, many insurance companies are now offering what is called "Data Breach & Cyber Liability Insurance."[39] Employers may want to consider consulting with their current coverage providers or exploring the general insurance marketplace regarding terms and provisions of such coverage, as well as providers' experiences in defending data breach claims brought by third parties. Such insurance policies may cover: 1) losses resulting from the breach of employee information, 2) expenses incurred for data breach response, remediation, and notice to appropriate legal authorities, 3) losses resulting from business interruption and reputational damages resulting from the data breach, and 4) losses suffered by third parties such as employees and third-party fraud victims. Some insurers even offer consulting services that can help minimize the risk of a data breach.


B. DICKINSON

Barron Dickinson *is an attorney with the Tampa office of Allen Norton & Blue, a statewide firm devoted exclusively to the practice of labor and employment law and representation of employers.*

Endnotes

1 Jason Firch, *10 Cyber Security Trends You Can't Ignore In 2021*, PURPLESEC (Apr. 29, 2021), https://purplesec.us/cyber-security-trends-2021/.

2 *Cost of a Data Breach Report 2020,* CAPITA (last accessed Aug. 21, 2021), https://www.

continued, next page

capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf.

[3] John Zorabedian, *What's New in the 2020 Cost of a Data Breach Report*, Sec. Intelligence (July 28, 2020), https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/.

[4] *Nationwide Survey: Nearly Half of Business Owners Have Been Victims of Cyberattacks—But Didn't Know It*, Nationwide (Oct. 9, 2017), https://news.nationwide.com/nationwide-survey-nearly-half-of-business-owners-have-been-victims-of-cyberattacks--but-didnt-know-it/.

[5] *Id.*

[6] Carmen Reinicke, *The biggest cybersecurity risk to US businesses is employee negligence, study says*, CNBC (June 21, 2018), https://www.cnbc.com/2018/06/21/the-biggest-cybersecurity-risk-to-us-businesses-is-employee-negligence-study-says.html.

[7] *Id.*

[8] *Common Types of Cybersecurity Attacks*, Rapid7 (last accessed July 12, 2021), https://www.rapid7.com/fundamentals/types-of-attacks/.

[9] Julia Ainsley and Kevin Collier, *Colonial Pipeline paid ransomware hackers $5 million, U.S. official says*, NBC News (May 13, 2021), https://www.nbcnews.com/tech/security/colonial-pipeline-paid-ransomware-hackers-5-million-u-s-official-n1267286.

[10] Emp. Benefits Sec. Admin. U.S. Dep't of Labor, Cybersecurity Program Best Practices (last accessed Aug. 21, 2021), https://www.dol.gov/sites/dolgov/files/ebsa/key-topics/retirement-benefits/cybersecurity/best-practices.pdf.

[11] Christopher Bing, *Exclusive: U.S. to give ransomware hacks similar priority as terrorism*, Reuters (June 3, 2021), https://www.reuters.com/technology/exclusive-us-give-ransomware-hacks-similar-priority-terrorism-official-says-2021-06-03/.

[12] Scott Travis, *Hackers post 26,000 Broward school files online*, Sun-Sentinel (Apr. 19, 2021), https://www.sun-sentinel.com/news/education/fl-ne-broward-schools-hackers-post-files-20210419-mypt2qtlc5a7xela4x6bcg5hdy-story.html.

[13] *Tsao v. Captiva MVP Rest. Partners, LLC*, 986 F.3d 1332 (11th Cir. 2021); *Muransky v. Godiva Chocolatier, Inc.*, 979 F.3d 917 (11th Cir. 2020) (en banc).

[14] *Tsao*, 986 F.3d at 1339 (quoting *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409, 414 & n.5 (11th Cir. 2021)).

[15] *Krottner v. Starbucks Corp.*, 406 F. App'x 129 (9th Cir. 2010). *Cf. e.g., Reilly v. Ceridian Corp.*, 664 F.3d 38, 40 (3d Cir. 2011) (lawsuit against a payroll processing firm by the firm's customers' employees); *Attias v. CareFirst, Inc.*, 365 F.Supp.3d 1 (D.D.C. 2019) (lawsuit by customers against an operator of a group of health insurance companies).

[16] *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359 (S.D. Fla. 2017); *Torres v. Wendy's Int'l, LLC*, 2017 WL 8780453 (M.D. Fla. 2017).

[17] 2012 WL 9391827 (S.D. Fla. Oct. 18, 2012).

[18] Similarly, in *Brush*, 238 F. Supp. 3d at 1365 (S.D. Fla. 2017), the Southern District of Florida held that a plaintiff had standing to bring various causes of action and concluded that the filing of an unauthorized tax return attributable to a data breach of patient data at a hospital was sufficient to show injury-in-fact traceable to the hospital.

[19] 2017 WL 8780453 (M.D. Fla. 2017).

[20] Fla. Stat. § 501.171(1)(a), (b), (f) (2020).

[21] *Id.* at § 501.171(1)(g)(1)(a)–(b).

[22] *Id.* at § 501.171(2).

[23] *Id.* at § 501.171(4)(a).

[24] *Id.* at § 501.171(4)(c).

[25] *Id.* at § 501.171(4)(d).

[26] *Id.*. at § 501.171(4)(e).

[27] *Id.* at § 501.171(4)(f).

[28] *Id.*

[29] *Id.* at § 501.171(3)(a).

[30] *Id.*. at 501.171(3)(b).

[31] *Id.* at § 501.171(3)(c).

[32] *Id.*. at 501.171(5); *see* 15 U.S.C. § 1681a(p).

[33] Fla. Stat § 501.171(4)(g).

[34] 45 C.F.R. § 164.404.

[35] Fla. Stat § 501.171(10); e.g., *Paris v. Herring*, 2019 WL 6340970 (M.D. Fla. 2019); *Owens–Benniefield v. Nationstar Mortgage LLC*, 258 F. Supp. 3d 1300 (M.D. Fla. 2017); *Torres v. Wendy's Int'l, LLC*, 2017 WL 8780453 (M.D. Fla. 2017); *Weinberg v. Advanced Data Processing, Inc.*, 147 F. Supp. 3d 1359 (S.D. Fla. 2015).

[36] Fla. Stat. § 501.171(9).

[37] H.B. 969, Reg. Sess. (Fla. 2021), https://www.flsenate.gov/Session/Bill/2021/969/BillText/Filed/PDF; Fla. H.R. Regulatory Reform Subcomm., H.B. 969 (Fla. 2021) Staff Analysis (Mar. 11, 2021), https://www.flsenate.gov/Session/Bill/2021/969/Analyses/h0969a.RRS.PDF.

[38] H.B. 969, Reg. Sess. (Fla. 2021), https://www.flsenate.gov/Session/Bill/2021/969/?Tab=BillHistory.

[39] *Cyber Insurance: Data Breach & Cyber Liability Insurance*, The Hartford (last accessed on Aug. 21, 2021), https://www.thehartford.com/cyber-insurance; Esquire Deposition Solutions, LLC, *Assessing Cyber Insurance Coverage for Data Breach Losses*, JD Supra, LLC (Jan. 27, 2021), https://www.jdsupra.com/legalnews/assessing-cyber-insurance-coverage-for-3498976/