South Carolina Law Review

Volume 71
Issue 4 *Annual Survey of South Carolina Law*

Article 14

Summer 2020

Are You in Good Hands: South Carolina's New Data Security Act and Whether It Does Enough to Protect Insurance Consumers

Zachary B. Randolph

ARE YOU IN GOOD HANDS: SOUTH CAROLINA'S NEW DATA SECURITY ACT AND WHETHER IT DOES ENOUGH TO PROTECT INSURANCE CONSUMERS

Zachary B. Randolph*

I. INTRODUCTION

On Friday, October 26, 2012, the former Governor of South Carolina, Nikki Haley, announced that the South Carolina Department of Revenue (SCDOR) experienced a cybersecurity breach in which hackers stole massive

* J.D. Candidate, May 2021, University of South Carolina School of Law. Thank you to Professor Benjamin Means of the University of South Carolina School of Law for his extraordinary feedback, guidance, and expertise in pursuing this Article. Thank you also to Adair Patterson, my Student Works Editor, for her incredible support and feedback throughout the entire process. A special thank you to my wonderful wife, Michaela, for her unwavering support. Lastly, thank you to the entire *South Carolina Law Review* for their diligent work in editing. Any errors remain completely my own.

amounts of personal information.[1] The cyberattack, the largest South Carolina state agency breach in history, resulted in the theft of 3.8 million Social Security numbers, 387,000 credit and debit card numbers, and nearly 3.3 million bank account numbers.[2] Roughly sixteen days prior to this public announcement, the SCDOR became aware of the data breach when law enforcement provided evidence that hackers stole three individuals' personal information.[3] The SCDOR contacted an information security firm, Mandiant, to conduct an investigation and determine the cause, extent, and implications of the security breach.[4]

Mandiant reported that it believed a phishing e-mail caused multiple SCDOR employees to click on an embedded link within the e-mail that executed malicious software on the computer and ultimately allowed the attacker to steal the employees' usernames and passwords.[5] The attacker then remotely accessed the SCDOR server, using the credentials from those employees who clicked on the malware link.[6] After logging into the SCDOR server, the hacker used those employees' access credentials to infiltrate the other servers.[7]

The investigation revealed that the attackers used thirty-three pieces of malicious software and compromised forty-four systems.[8] For over two months, nobody in the SCDOR was aware that a hacker breached the servers and stole taxpayer files, many of which lacked encryption safeguards.[9] Although a containment plan prevented the attackers from regaining access to the SCDOR servers, the information was gone.[10] After the investigation

---

1. Kara Durrette, *SC Department of Revenue Hacked; Millions of SC Residents Affected*, WACH (Oct. 26, 2012), https://wach.com/news/local/sc-department-of-revenue-hacked-millions-of-sc-residents-affected [https://perma.cc/MJ6N-RJ6S].

2. Robbie Brown, *South Carolina Offers Details of Data Theft and Warns It Could Happen Elsewhere*, N.Y. TIMES, Nov. 20, 2012, at A17.

3. MANDIANT, SOUTH CAROLINA DEPARTMENT OF REVENUE: PUBLIC INCIDENT RESPONSE REPORT 2 (2012); *see also Data Breach: Where Did South Carolina Go Wrong?*, GOV'T TECH. (Nov. 26, 2012) [hereinafter *Data Breach*], https://www.govtech.com/e-government/Data-Breach-Where-Did-South-Carolina-Go-Wrong.html [https://perma.cc/NMP8-K6M9] (describing timeline of the breach at the Department of Revenue).

4. *See* MANDIANT, *supra* note 3.

5. *Id.* The actual cause of the security breach was never conclusively determined, but Mandiant determined the "phishing" excursion was the most likely cause based on other facts determined through its investigation. *Id.*

6. *See id.* at 3.

7. *Id.*

8. *Id.*

9. *See id.* at 3–4; *Data Breach*, *supra* note 3; *see also* S.C. CODE ANN. § 38-99-10(6) (Supp. 2019) ("'Encrypted' means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.").

10. *See* MANDIANT, *supra* note 3, at 4.

concluded, Mandiant and government officials determined that the SCDOR lacked essential security protocols, such as minimal encryption of the data it housed, inadequate breach detection safeguards, and single-factor authentication to access data.[11]

Although the SCDOR did not publicly disclose the total cost of the breach, the agency took out a $20.1 million loan with the state Insurance Reserve Fund to guarantee free credit monitoring for individuals directly affected by the breach, implement encryption and dual passwords at the SCDOR, and give direct notification to taxpayers about the breach.[12] In response to the breach, the SCDOR implemented new security protocols, including more specialized employee training on data security, more extensive monitoring of software capabilities, and enhanced firewall technology to protect the system from outside threats.[13]

This data breach, along with other notorious data breaches in recent history,[14] led the South Carolina General Assembly, and now Governor Henry McMaster, to be the first state in the country to sign an insurance cybersecurity bill into law. The South Carolina General Assembly passed the Insurance Data Security Act (IDSA) to regulate data privacy within the state's insurance industry.[15]The IDSA requires that the industry most vulnerable to cybersecurity threats must implement standardized data security protocols to equip insurance companies with the ability to protect their consumers' personal information. Specifically, insurance licensees must implement not only the standardized protocols that the IDSA provides (investigation, notification, and penalty protocols) but also a "comprehensive written information security program" that the IDSA must approve.[16]

---

11. *See* Tim Smith, *Four Years Later, Case Still Open in DOR Data Breach*, GREENVILLE NEWS (Aug. 12, 2016), https://www.greenvilleonline.com/story/news/crime/2016/08/12/four-years-later-case-still-open-dor-data-breach/88453548/ [https://perma.cc/RP5F-KY63].

12. *See* Eric Chabrow, *$20 Million Loan to Cover Breach Costs*, BANKINFO SECURITY (Dec. 13, 2012), https://www.bankinfosecurity.com/20-million-loan-to-cover-breach-costs-a-5355 [https://perma.cc/3XCX-434U]; *see also* Mike Ellis, *A Team: What's Being Done to Stop Future Data Breaches in South Carolina?*, INDEP. MAIL (Nov. 24, 2017), https://www.independentmail.com/story/news/2017/11/24/2012-data-breach-south-carolina/890279001/ [https://perma.cc/S3UD-JX26] (reporting that free credit monitoring ended in October 2018).

13. *See* Smith, *supra* note 11.

14. *See generally* Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html [https://perma.cc/3AB7-3HNC] (providing information on the largest data breaches, including Yahoo, Marriott International, and Anthem).

15. *See* Media Release, S.C. Dep't of Ins., Governor McMaster Signs Data Security Bill into Law (May 8, 2018) (on file with author) ("In recent years, the demand for cyber insurance has increased significantly in response to sharply heightened risk awareness.").

16. *See* Bulletin, S.C. Dep't of Ins., Bulletin Number 2018-02 (June 14, 2018) (on file with author); S.C. CODE ANN. §§ 38-99-20, -30, -40, -80 (Supp. 2019).

Insurance companies are prime targets for hackers seeking to make a profit because, although some insurance entities may have money (or cryptocurrency), which they often protect heavily, all insurance entities possess their customers' personal information, which they protect less rigorously.[17] Because inadequate security renders this personal information much easier to access, hackers may steal a higher quantity of it and subsequently sell the information on the dark web.[18]

Data security is an essential part to any business that collects and stores sensitive data. Without up-to-date data security measures, any business is susceptible to a data breach that could damage the business's financial capabilities, reputation, and ability to continue operations. Due to a lack of universal federal regulation concerning cybersecurity and data protection, states are left to create a patchwork of protections, often regulating only individual industries.[19] While the National Association of Insurance Commission's (NAIC) Model Law was a key influence on the IDSA, New York's recent legislation concerning data security within the financial industry (New York Cybersecurity Requirements)[20] heavily influenced the NAIC's Model Law.[21]

Although the IDSA provides straightforward steps on how licensees should implement data security, such as requiring boards of directors to implement data security plans and listing items that the those plans must include, it does not provide direction for insurance licensees to effectively and efficiently implement these data security protection standards.[22] Furthermore, the current construction of the IDSA will have broad reaching effects, both legal and economic, on the insurance industry in South Carolina.

This Comment argues that the IDSA, although it may help prevent data security breaches in the future, leaves insurance licensees exposed to increased legal liability and economic cost beyond what is justified to incentivize improved data security. Part II introduces background information concerning the issues of cybersecurity and the IDSA, including a survey of recent major data breaches across varying industries, information regarding

17. *See* Tal Vegvizer, *Cybersecurity Threats in the Insurance Industry*, NU PROP. CASUALTY 360° (Jan. 29, 2018), https://www.propertycasualty360.com/2018/01/29/cybersecurity-threats-in-the-insurance-industry/ [https://perma.cc/6SY2-4ZMU].

18. *See id.*

19. *See* Eric J. Hyla, Note, *Corporate Cybersecurity: The International Threat to Private Networks and How Regulations Can Mitigate It*, 21 VAND. J. ENT. & TECH. L. 309, 329 (2018).

20. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.0–500.23 (2018).

21. Bulletin, S.C. Dep't of Ins., *supra* note 16; Clark Hill, *States Diverge in Following Either the NAIC or New York in Implementing Cybersecurity Regulations*, JD SUPRA (Oct. 7, 2019), https://www.jdsupra.com/legalnews/states-diverge-in-following-either-the-84205/ [https://perma.cc/QW5S-N2ME]; INS. DATA SEC. MODEL LAW (NAT'L ASS'N OF INS. COMM'RS, 2017); *see also* N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2018).

22. *See* S.C. CODE ANN. § 38-99-20(E) (Supp. 2019).

typical cybersecurity breaches, and a brief comparison between the IDSA and its contemporaries. Finally, Part III introduces the IDSA's key provisions and analyzes whether these provisions will be successful in combating data breaches and whether the IDSA's standards will be able to keep up with the technological changes in cybersecurity.

II. WE KNOW A THING OR TWO BECAUSE WE'VE SEEN A THING OR TWO: BACKGROUND ON CYBERSECURITY BREACHES AND THE IDSA

A. A Brief Survey of Past Data Breaches

Contemporary businesses do not simply house data; they are data. This data is valuable because it enables businesses to improve their services, generate more revenue, and enhance operations.[23] With more companies collecting more data, it is only fitting that more data breaches will occur.[24] Between 2018 and 2019,[25] there was a dramatic increase in breached records, reaching over four billion.[26]

Three recent and major data breaches include those committed against Anthem Medical Insurance, Yahoo, and Uber.[27] On February 18, 2014,

---

23. Emily Matta, Note, *Kansans at Risk: Strengthened Data Breach Notification Laws as a Deterrent to Reckless Data Storage*, 67 U. KAN. L. REV. 823, 823 (2019); *see also* Vindu Goel & Nicole Perlroth, *Yahoo Says 1 Billion User Accounts Were Hacked*, N.Y. TIMES (Dec. 14, 2016), https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html [https://perma.cc/3RRN-UGMX] (discussing the hacking of Yahoo).

24. *See* Matta, *supra* note 23, at 823.

25. Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#2eca5041bd54 [https://perma.cc/STC5-3DDQ]. Danny Bradbury, *Data Breach Numbers Skyrocket in 2019*, INFOSECURITY (Aug. 16, 2019), https://www.infosecurity-magazine.com/news/data-breach-numbers-skyrocket-in/ [https://perma.cc/7D84-C5PV].

26. Danny Bradbury, *Data Breach Numbers Skyrocket in 2019*, INFOSECURITY (Aug. 16, 2019), https://www.infosecurity-magazine.com/news/data-breach-numbers-skyrocket-in/ [https://perma.cc/7D84-C5PV]; Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019), https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/#2eca5041bd54 [https://perma.cc/STC5-3DDQ].

27. Rasha Altamimi et al., Anthem Hack (2015), https://www.cs.bu.edu/~goldbe/teaching/HW55815/presos/anthem.pdf [https://perma.cc/L5CM-A6NV] (PowerPoint presentation by students enrolled in Introduction to Network Security at Boston University); Robert McMillan & Ryan Knutson, *Yahoo Triples Estimate of Breached Accounts to 3 Billion*, WALL ST. J. (Oct. 3, 2017), https://www.wsj.com/articles/yahoo-triples-estimate-of-breached-accounts-to-3-billion-1507062804 [https://perma.cc/4ALT-RH7L]; Bill Chappell, *Uber Pays $148 Million Over Yearlong Cover-Up of Data Breach*, NPR (Sept. 27, 2018), https://www.npr.org/2018/09/27/652119109/uber-pays-148-million-over-year-long-cover-up-of-data-breach [https://perma.cc/J4XS-263E].

hackers gained access to Anthem's database through a spear-phishing expedition by targeting key employees through false e-mails that contained malware allowing the hackers to gain remote access to other systems within Anthem's enterprise.[28] Over the next several months, the hackers used a key employee's credentials to move about Anthem's systems and gain access to more information.[29] Eventually, the hackers found Anthem's data warehouse containing personal consumer data.[30] The breach exposed nearly 78.8 million records,[31] containing a wide variety of consumer information.[32] Anthem was unaware of the breach until January 27, 2015, when an Anthem administrator discovered his credentials being used on a task he did not initiate.[33] Although Anthem acted quickly and notified the FBI and the public, the damage was already done.[34] Due to the nearly 80 million records exposed, Anthem incurred significant costs related to its data security breach.[35]

In 2019, the "Justice Department unsealed an indictment of two Chinese nationals" for the Anthem data breach.[36] Because no Anthem information entered the dark web, where personal information is often sold,[37] authorities believe there was an ulterior motive for the stolen information.[38] Based on one leading theory foreign governmental authorities used this information to track, investigate, and root out international covert activities.[39] Regardless of the

28. *See* Marianne Kolbasuk McGee, *A New In-Depth Analysis of Anthem Breach*, BANKINFO SECURITY (Jan. 10, 2017), https://www.bankinfosecurity.com/new-in-depth-analysis-anthem-breach-a-9627 [https://perma.cc/58BP-7X7X].

29. *Id.*

30. *Id.*

31. *Id.*

32. *See* Altamimi et al., *supra* note 27, at 4 ("Accessed information may have included: [n]ames, [d]ates of birth, Social Security numbers, [h]ealth care [identification] numbers, [h]ome addresses, [e]mail addresses, [w]ork information like income date.").

33. Steve Ragan, *How Does a Breach Like Anthem Happen?*, CSO (Feb. 9, 2015), https://www.csoonline.com/article/2881532/anthem-how-does-a-breach-like-this-happen.html [https://perma.cc/ZPP8-2NDE].

34. *Id.*

35. McGee, *supra* note 28 (noting that costs included $2.5 million for expert consultations, $115 million in improved security procedures and technology, $31 million to provide notification to the public and affected individuals, and $112 million to provide credit protection). Anthem also settled its class action lawsuit for $115 million. Kevin Stawicki, *$115M Anthem Data Breach Deal Gets Final Nod*, LAW360 (Aug. 16, 2018), https://www.law360.com/articles/1073957 [https://perma.cc/GG8U-ZMVK].

36. Nicole Perlroth, *Two from China Are Charged in 2014 Anthem Data Breach*, N.Y. TIMES (May 9, 2019), https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html [https://perma.cc/XV4S-K8QK].

37. *Id.*; *see also How Cybercriminals Make Money*, KEEPER SECURITY, INC., https://keepersecurity.com/how-much-is-my-information-worth-to-hacker-dark-web.html, [https://perma.cc/8QRE-Z24X] (providing common pricing guidelines for personal information sold on the dark web).

38. Perlroth, *supra* note 36.

39. *Id.*

reason for the stolen information, Anthem paid a heavy price for the data breach.

Although the Anthem breach is the largest to affect the insurance industry, the Yahoo data breaches that occurred in 2013 and 2014 greatly surpass it in size.[40] These breaches affected 1.5–3.0 billion Yahoo account users.[41] In August of 2013, unknown attackers breached Yahoo's computer systems, where the company stored consumer data such as login information and personal data.[42] This information provided the hackers access to the contents of Yahoo users' e-mails, which likely contained other sensitive personal and financial information.[43] Although investigators are not certain exactly how the breach occurred, they believe that Yahoo's outdated encryption technology and procedures led to the documents' exposure.[44] It was not until the summer of 2013 that Yahoo started implementing updated encryption of its data.[45]

In 2014, Yahoo suffered another cyberattack. Russian nationals targeted high-level Yahoo employees through a spear-phishing campaign[46] and exposed over 500 million accounts during this breach.[47] Yahoo disclosed both the 2013 and 2014 attacks to the public in December of 2016 when Verizon was negotiating to purchase Yahoo for $4.8 billion.[48] This led to a dramatic

40. McMillan & Knutson, *supra* note 27; Nicole Perlroth, *All 3 Billion Yahoo Accounts Were Affected by 2013 Attack*, N.Y. TIMES (Oct. 3, 2017), https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html [https://perma.cc/55FZ-96M3].

41. Goel & Perlroth, *supra* note 23; Perlroth, *supra* note 40; Jonathan Stempel & Jim Finkle, *Yahoo Says All Three Billion Accounts Hacked in 2013 Data Theft*, REUTERS: TECHNOLOGY NEWS (Oct. 3, 2017), https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-three-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1 [https://perma.cc/3SFR-ER2W]; Martyn Williams, *Inside the Russian Hack of Yahoo: How They Did It*, CSO (Oct. 4, 2017), https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html [https://perma.cc/26BK-FXZG]; *see In re* Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752, 2017 WL 3727318, at *2 (N.D. Cal. Aug. 30, 2017).

42. *In re Yahoo!*, 2017 WL 3727318, at *2.

43. *Id.* (noting that the other information likely included: credit card numbers, retail accounts, banking information, account passwords, IRS documents, and Social Security information).

44. *Id.* at *3.

45. *Id.* Yahoo used encryption technology called "MD5," which was "widely recognized in the data security industry" as "unsuitable for further use." *Id.*

46. *Id.*; Steve Kovach, *FBI: Russian Hackers Likely Used a Simple Phishing Email on a Yahoo Employee to Hack 500 Million User Accounts*, BUS. INSIDER (Mar. 16, 2017), https://www.businessinsider.com/fbi-yahoo-hackers-used-spear-phishing-email-gain-access-500-million-accounts-2017-3 [https://perma.cc/Z7JX-D6RT]; Williams, *supra* note 41.

47. *In re Yahoo!*, 2017 WL 3727318, at *3. Much of the information taken in this breach included names, phone numbers, account information and unencrypted security question information. Goel & Perlroth, *supra* note 23.

48. Goel & Perlroth, *supra* note 23.

decrease in price by $350 million and an overall 1.3 billion dollar drop in Yahoo stock.[49]

Uber suffered a more recent data breach in late 2016.[50] The breach occurred when an Uber employee posted the company's access key online.[51] Targeting one of Uber's cloud-based service providers,[52] a hacker used the key to access unencrypted files that contained millions of Uber driver and rider information.[53] Uber failed to disclose the breach until November 2017, when the new CEO issued a press release advising of the attack.[54] There is debate concerning whether Uber attempted to conceal the data breach when it paid the hackers $100,000 to delete the stolen data instead of reporting the breach, as required by notification laws.[55] The data breach resulted in Uber's settling a class action suit for $148 million.[56]

Although these events represent only a few of the major data security breaches in recent years, it is clear that data security breaches greatly affect businesses' financial liability and can cause irreparable harm to a business' reputation. Furthermore, not all data security breaches concern large, well-known companies. In fact, in 2017 the majority of reported data breaches

49. Edward J. McAndrew, *The Hacked & the Hacker-for-Hire: Lessons from the Yahoo Data Breaches (So Far)*, NAT'L L. REV. (May 11, 2018), https://www.natlawreview.com/article/hacked-hacker-hire-lessons-yahoo-data-breaches-so-far [https://perma.cc/35MJ-9252].

50. West v. Uber Techs., No. 18-CV-3001, 2018 WL 5848903 (C.D. Cal. Sept. 5, 2018); *see also* Craig Smith, *110 Amazing Uber Statistics, Demographics, and Facts (2020)*, DMR, https://expandedramblings.com/index.php/uber-statistics/ [https://perma.cc/U8F6-4GFP] (stating that, in 2019, there were 99 million monthly active Uber users).

51. Christopher Olsen & Edward Holman, *Key New Takeaways from Uber's Privacy and Data Security Settlement with the FTC*, WILSON SONSINI: THE WSGR DATA ADVISOR (Sept. 1, 2017), https://www.wsgrdataadvisor.com/2017/09/uber-ftc-settlement/ [https://perma.cc/NP72-BDHP].

52. Chappell, *supra* note 27.

53. Olsen & Holman, *supra* note 51.

54. Chappell, *supra* note 27.

55. *See* Kate Conger, *Uber Settles Data Breach Investigation for $148 Million*, N.Y. TIMES (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html [https://perma.cc/Z4UH-ATYX] ("Uber's decision to cover up this breach was a blatant violation of the public's trust . . . ."). *But see* Chappell, *supra* note 27 (stating that payment to the hackers was "part of an ongoing security program and not . . . a cover-up").

56. *See* Heather Somerville, *Uber to Pay $148 Million to Settle Data Breach Cover-Up with U.S. States*, REUTERS (Sept. 26, 2018), https://www.reuters.com/article/us-uber-databreach/uber-settles-for-148-million-with-50-us-states-over-2016-data-breach-idUSKCN1M62AJ [https://perma.cc/W29K-HH5N]. The settlement terms also included changes to Uber's business practices concerning data security, reforming its corporate culture, requiring reports of any data security event, and implementation of a "comprehensive information security program." *Id.*

affected those considered small businesses.[57] With the increasing number of data security breaches,[58] it is important to be aware of the different tactics hackers use to infiltrate security systems to gain access to protected information.

B. A Brief Background on Data Security Infiltration Methods and Solutions

A data breach may have several different definitions;[59] however, the vast majority of data breaches occur using a variation of hacker technology called malware.[60] Malware is a collective term for an array of malicious software variants, including the following: viruses, worms, ransomware, spyware, and Trojan viruses.[61] A virus is the most common type of malware, where the virus attaches its malicious code to a host system and waits for the code to be activated, where it then spreads quickly, causing damage to the system's functionality and possibly locking down or destroying files.[62] A worm, on the other hand, does not need a host system to cause damage because a worm replicates its own code to find and infect other computer systems.[63] Ransomware is malware designed to lockdown entire systems.[64] It denies authorized users access to the system until they pay a ransom to the attackers to release the system.[65] Spyware is designed to operate in the background of the computer system where it collects and stores information without the user's knowledge.[66] Trojans, a variant of spyware, are embedded in software

57. Julia Whall, Comment, *Policing Cyberspace: The Uncertain Future of Data Privacy and Security Enforcement in the Wake of* LabMD, 60 B.C. L. REV. E-SUPPLEMENT II. 149, 149 (2019); VERIZON, 2018 DATA BREACH INVESTIGATIONS REPORT 5 (11th ed. 2018) (finding that fifty-eight percent of data breach victims qualify as small businesses).

58. *See* Durrett, *supra* note 1.

59. Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, S.C. LAW., May 2014, at 28, 30 ("A data beach is any release of secure information to an untrusted environment."); Nicole Martin, *What Is a Data Breach?*, FORBES (Feb. 25, 2019), https://www.forbes.com/sites/nicolemartin1/2019/02/25/what-is-a-data-breach/#7a3cb5d814bb [https://perma.cc/5WVX-WQN2] ("A data breach occurs when there is an unauthorized entry point into a corporation's database[] that allows . . . access [to] customer data . . . ."); Steve Symanovich, *What Is a Data Breach?*, LIFELOCK, https://www.lifelock.com/learn-data-breaches-data-breaches-need-to-know.html [https://perma.cc/4SUX-FND9] ("A data breach is an incident that exposes confidential or protected information.").

60. *See* Martin, *supra* note 59.

61. NWOKEDI IDIKA & ADITYA P. MATHUR, A SURVEY OF MALWARE DETECTION TECHNIQUES 4–5 (2007); *What Is Malware?*, FORCEPOINT, https://www.forcepoint.com/cyber-edu/malware [https://perma.cc/7MVE-D2A6].

62. *What Is Malware?*, *supra* note 61.

63. IDIKA & MATHUR, *supra* note 61, at 5.

64. *See What Is Malware?*, *supra* note 61.

65. *Id.*

66. *Id.*

applications or the computer system.[67] When the application or system is in use, the Trojan is performing an unauthorized action without the user's knowledge.[68] Finally, phishing is a process that attempts to trick e-mail recipients into clicking hyperlinks or attached files that contain malware.[69] Although many phishing probes are easy to spot, some phishing attacks are more difficult to discern. Spear-phishing campaigns are more troublesome to spot because they are specifically targeted to the recipient to masquerade as a known or trusted sender.[70] Although these are common ways hackers gain access to secured data, malware is continuously evolving in order to bypass new security measures, making data security especially difficult for individuals and businesses.[71] Even though it is nearly impossible to protect businesses from all data security breaches,[72] businesses can implement several security protocols—such as encryption, endpoint lockdown, multifactor authentication, and employee date security training—that can slow down a hacker's ability to retrieve and use protected data.[73]

C. Background of the IDSA

As infiltration technology and the counter measures created to combat those infiltrations become more sophisticated, hackers often look for targets that have minimal or outdated security measures but who also house large amounts of personal or business information.[74] Even though anyone operating on the internet or within a network system can fall victim to data breaches, experts consider insurance companies and small businesses, in particular, to be among the top targets for hackers.[75] While cyber criminals may seek to steal cryptocurrencies from financial institutions, these assets are heavily guarded and difficult to extract successfully.[76] Although small businesses and

67. *See* IDIKA & MATHUR, *supra* note 61, at 5.

68. *Id.* (explaining that the Trojan captures the user's keystrokes or sends unauthorized information outside of the system).

69. Aaron Glenn, *Phishing Update—"A Whale of a Tale,"* S.C LAW., May 2019, at 14.

70. *Id.* A similar variant of spear-phishing is called "whaling," where hackers target employees by sending e-mails disguised as an employer in order to elicit information. *Id.*

71. *See* IDIKA & MATHUR, *supra* note 61, at 5.

72. *See* David C. Grossman, Comment, *Blaming the Victim: How FTC Data Security Enforcement Actions Make Companies and Consumers More Vulnerable to Hackers*, 23 GEO. MASON L. REV. 1283, 1284 (2016) ("[M]any industry experts acknowledge that today it is a matter of when, not if, a company's data will be breached.").

73. *See* Steven C. Bennett, *Data Security Breaches: Problems and Solutions*, PRAC. LAW., Dec. 2008, at 41–44.

74. *See How Do Hackers Pick Their Targets?*, PANDA SECURITY, https://www.pandasecurity.com/mediacenter/mobile-news/how-hackers-pick-their-targets/ [https://perma.cc/U6TT-TU8K].

75. *See* Vegvizer, *supra* note 17.

76. *See id.*

insurance entities seldomly house excessive amounts of cryptocurrency, they do house copious amounts of personal information, making them attractive targets for cyber criminals.[77] These types of companies are "soft targets" because, while other industries have dedicated significant time and resources to implement procedures to protect against data breaches, the employees lack awareness training in this regard[78] and often cannot pay for the cybersecurity systems necessary for its enterprise.[79] This bullseye on insurance entities led South Carolina to be the first state to adopt insurance industry data security legislation which requires insurance entities to implement data security measures to protect consumer and business information.[80]

1. IDSA and NAIC Overview of Provisions

The IDSA is heavily influenced by the NAIC's Model Law (Model Law),[81] as both establish a legal framework that provides a minimum floor for cybersecurity within the insurance industry.[82] This framework requires insurance licensees to conduct an assessment concerning the cybersecurity risks the company may be subject to.[83] Based on this risk assessment, the insurance entity must "develop, implement, and maintain a comprehensive written" security program that provides extensive safeguards to protect personal nonpublic information.[84] The information security program effectively creates an objective floor for mandatory compliance, but it does not mandate a particular subjective ceiling, allowing flexibility for the licensee to go beyond the IDSA's minimum standards to provide further

77. *See id.*; *see also* Karen Painter Randall & Steven A. Kroll, *Getting Serious About Law Firm Cybersecurity*, N.J. LAW., June 2016, at 54 (stating law firms are attractive targets because "they handle a variety of high-value information," including highly regulated health and financial information for clients).

78. *See* 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 [https://perma.cc/Y584-8ZAJ].

79. *Small Business Cybersecurity*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/small-business-cybersecurity [https://perma.cc/YA43-VF7V].

80. Media Release, S.C. Dep't of Ins., *supra* note 15.

81. Bulletin, S.C. Dep't of Ins., *supra* note 16. Also, Raymond Farmer, South Carolina's Department of Insurance Director, served as the head chair to the NAIC's Cybersecurity Working Group, the main group responsible for creating the NAIC's Model Law. Media Release, S.C. Dep't of Ins., *supra* note 15.

82. Matt Franko, *Understanding the NAIC Insurance Data Security Model Law*, RSM (Apr. 17, 2018), https://rsmus.com/what-we-do/services/risk-advisory/understanding-the-naic-insurance-data-security-model-law.html [https://perma.cc/H4Y4-TRU4].

83. S.C. CODE ANN. § 38-99-20(A) (Supp. 2019).

84. *Id.*

security.[85] One of those subjective standards is the development of an information security program that is commensurate with the size and complexity of the covered entity's business activities.[86] If the covered entity engages in business that collects a vast amount of nonpublic information, the covered entity must develop and operate its information security program in light of the vast amount of information.[87] Furthermore, if the covered entity's business operations or internal information system is complex, its information security program must account for the increased possibility that breaches may occur with increased complexity.[88]

The IDSA and Model Law provide strict mandates upon covered insurance entities to assess and determine whether the procedures within their written security plans are sufficient for the entities to comply with the following: protect all nonpublic information through encryption, regularly test and monitor security systems and procedures, and implement authentication procedures to access information.[89] The IDSA and the Model Law also provide strict requirements on insurance entities to conduct an investigation if a data breach has occurred or if the entity thinks an event may have occurred.[90] The investigation must accomplish the following: determine whether a cybersecurity event occurred, assess the nature and scope of the event, identify the information that was involved in the event, and "perform reasonable measures to restore the security system that was compromised by the event."[91]

The IDSA and Model Law's primary objective is to protect nonpublic information.[92] A covered entity's entire data security program and risk assessment is largely dependent on the type and amount of nonpublic information it collects and carries.[93] Publishing similar definitions, the IDSA

85. *See id.*; *see also* David Condon, McGuffin Consulting Group, LLC, How Much Is Enough?: South Carolina's Insurance Data Security Act (Sept. 24, 2019) (on file with *South Carolina Law Review*) (distinguishing mandates from flexible options pursuant to the IDSA).

86. *See* § 38-99-20(A); *see also* § 38-99-20(D)(1) (requiring the licensee to design the information security program to mitigate identified risks from the risk assessment "commensurate with the size and complexity" of its activities).

87. *See* § 38-99-20(A).

88. *See id.* Other areas that demonstrate the IDSA's flexibility include whether the covered entity uses third-party service providers to manage nonpublic information, and the covered entity's consideration of the nonpublic information's sensitivity that is under the entity's care, custody, and control. *See* Condon, *supra* note 85.

89. *See* Condon, *supra* note 85.

90. S.C. CODE ANN. § 38-99-30 (Supp. 2019); INS. DATA SEC. MODEL LAW § 5 (NAT'L ASS'N INS. COMM'RS 2017).

91. § 38-99-30; INS. DATA SEC. MODEL LAW § 5.

92. § 38-99-20(A); INS. DATA SEC. MODEL LAW § 4(A) ("[E]ach Licensee shall develop, implement, and maintain a comprehensive written Information Security Program . . . that contains administrative, technical, and physical safeguards for the protection of Nonpublic Information and the Licensee's Information System.").

93. *See* § 38-99-20(A).

and the Model Law define nonpublic information as information that is not publicly available, thereby excluding information such as records made available to the public by any level of government and records distributed through the media.[94] Nonpublic information under the IDSA and Model Law departs somewhat from traditional data security legislation because it includes both consumer information and "certain business-related information."[95] This definition is expansive and broad, providing that the business-related information requires protection under the IDSA if it "would cause a material adverse impact to the business, operations, or security of the licensee."[96] Like business-related information, traditional consumer information also requires protection. Traditional consumer information includes Social Security numbers, driver's license numbers, credit and account numbers, security codes or passwords, and any information collected by a healthcare provider, except for age or gender.[97] The nonpublic information definition implicitly excludes those entities who do not carry such information; however, this exclusion is effectively obsolete due to the vast quantities of consumer information insurance entities possess.[98]

Along with the implementation of security programs and the investigation of cybersecurity events, the IDSA and Model Law also require covered insurance entities to notify the state's Director of the Department of Insurance (Director) within seventy-two hours after determining that a cybersecurity event has occurred.[99] This provision does not supersede other state notification laws concerning consumer information, meaning that insurance entities are required to notify both the Director and the consumer when a breach occurs.[100] Other important provisions within the IDSA and Model Law include bestowing the Director with the authority to investigate and examine covered insurance entities and to determine whether they engaged in conduct that violates the law.[101] If a covered entity violates the statute, then the

94. *Id.*; S.C. CODE ANN. § 38-99-10(11) (Supp. 2019); INS. DATA SEC. MODEL LAW § 3(K).

95. § 38-99-10(11); INS. DATA SEC. MODEL LAW § 3(K); Jeremy Rucker, *New South Carolina Insurance Data Security Act*, SPENCERFANE (Jan. 14, 2019), https://www.spencerfane.com/publication/new-south-carolina-insurance-data-security-act/ [https://perma.cc/42TM-6YEZ].

96. § 38-99-10(11)(a).

97. § 38-99-10(11)(a)–(c).

98. *See* § 38-99-10(11).

99. S.C. CODE ANN. § 38-99-40(A) (Supp. 2019); INS. DATA SEC. MODEL LAW § 6. Both the IDSA and Model Law require notification when South Carolina is the entity's domicile state or when there is a reasonable belief that information on at least two hundred fifty South Carolina residents were involved in the data breach. § 38-99-40(A); INS. DATA SEC. MODEL LAW § 6.

100. *See* S.C. CODE ANN. § 39-1-90(A) (1985 & Supp. 2019).

101. S.C. CODE ANN. § 38-99-50(A) (Supp. 2019); INS. DATA SEC. MODEL LAW § 7(A).

Director can levy a fine up to $15,000, or $30,000 if it acted willfully in violating the statute.[102]

There are exceptions under the IDSA and Model Law. A covered insurance entity is exempt from the program if it has fewer than ten employees, including independent contractors; the entity has coverage under another entity's security program; or the covered insurance entity follows the Health Insurance Portability and Accountability Act (HIPAA) requirements.[103] It is important to note that these provisions do not exempt those covered entities from the entire statute; rather, they only provide exemptions for complying with the security program development, implementation, and maintenance.[104] While the IDSA follows closely in line with the NAIC's Model Law, New York's Cybersecurity Requirements influenced much of the language adopted in the Model Law, which the New York State Department of Financial Services (DFS) promulgated to provide cybersecurity regulations for New York's financial industry.[105]

2. *Comparison of IDSA and 23 NYCRR § 500*

The New York DSF promulgated the Cybersecurity Requirements to protect consumers and itself from cybercriminals by instituting regulations that require covered entities to assess the specific risk profiles of their networks and design a cybersecurity program to mitigate those risks.[106] Like the IDSA, the New York regulations focus on finance institutions implementing a cybersecurity program based on a risk assessment, based on oversight of third-party service providers, and based on submissions of written certification of compliance.[107] Also like the IDSA, New York's Cybersecurity Requirements broadly define nonpublic information,[108] and both have

102. S.C. CODE ANN. § 38-2-10(A)(1) (2015).

103. S.C. CODE ANN. § 38-99-70(A) (Supp. 2019); INS. DATA SEC. MODEL LAW § 9(A).

104. *See* § 38-99-70(A); INS. DATA SEC. MODEL LAW § 9(A).

105. N.Y. COMP. CODES R. & REGS. tit. 23, §§ 500.0–.23 (2018); Joshua Mooney et al., *South Carolina's New Insurance Data Security Act: Pebbles Before a Landslide?*, WHITE & WILLIAMS, LLP (May 30, 2018), https://www.whiteandwilliams.com/resources-alerts-South-Carolinas-New-Insurance-Data-Security-Act-Pebbles-Before-a-Landslide.html [https://perma.cc/W8QK-LEDE].

106. N.Y. COMP. CODES R. & REGS. tit. 23 § 500.0.

107. KIM MOBLEY & MICHAEL BOYD, JOHNSON LAMBERT, MAPPING OF NYDFS CYBERSECURITY REGULATIONS TO NAIC INSURANCE DATA SECURITY MODEL LAW 2 (2017).

108. *See* § 38-99-10(11) (Supp. 2019); N.Y. COMP. CODE R. & REGS. tit. 23 § 500.1(g) (stating that "nonpublic information" includes all electronic information that is business or medical related and not publicly available); *see also* Mooney et al., *supra* note 105 ("'[N]on-public information' is broadly defined to include business information . . . consumer personal information . . . or protected health information.").

seventy-two hour notification requirements.[109] This means that covered entities, under both articles of law, must be quick and organized in order to adhere to this strict notification mandate. This provision encourages covered entities to create and implement effective detection procedures within its security program.[110] Furthermore, both the IDSA and New York's Cybersecurity Requirements offer some similar exemptions.[111] Although the IDSA and the New York regulations tackle many of the same issues, there are numerous differences between the two pieces of law.

One area in which New York's Cybersecurity Requirements and the IDSA differ is how the two define key terms. For example, under New York's regulations, "cybersecurity event means *any* act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."[112] On the other hand, "cybersecurity event" under the IDSA provides safe harbor provisions which permit a covered insurance entity not to disclose certain events that fall outside of the definition.[113]

Perhaps the most noteworthy difference is the flexibility offered with the IDSA as compared to the New York Cybersecurity Requirements. Although both mandate substantial requirements to covered entities, the IDSA provides more "flexibility to choose security measures appropriate for their size, resources[,] and the nature of the security risks they face" as compared to the New York Regulations.[114]

This background concerning the IDSA's creation and adoption is important in order to grasp the recent landscape of cybersecurity laws and provisions. With the heavy influences from the Model Law and the New York Cybersecurity Requirements, the IDSA embarks to protect insurance entities within South Carolina and its residents from the ever-increasing threat data breaches levy on both consumers and businesses. However, the question remains whether the IDSA will be effective in combating this threat.

---

109. S.C. CODE ANN. § 38-99-40(A) (Supp. 2019); N.Y. COMP. CODE R. & REGS. tit. 23 § 500.17(a).

110. Mooney et al., *supra* note 105.

111. S.C. CODE ANN. § 38-99-70(A) (Supp. 2019) (exempting compliance when entity has fewer than ten employees, including independent contractors); N.Y. COMP. CODE R. & REGS. tit. 23 § 500.19(a) (allowing exemption from compliance when entity has fewer than ten employees, including independent contractors, while also providing exemptions when certain revenue thresholds are not met).

112. N.Y. COMP. CODE R. & REGS. tit. 23 § 500.1(d) (2018) (emphasis added).

113. Mooney et al., *supra* note 105.

114. *Id.*

III. ON YOUR SIDE?: ANALYSIS OF THE IDSA'S KEY PROVISIONS

Part III analyzes select provisions of the IDSA and addresses potential issues regarding whether the IDSA does enough to protect consumers. The IDSA implements many provisions that purport to provide better information security and provide protection to both consumers and business information. However, a more in-depth analysis into these provisions presents a more nuanced reality for both consumers and regulated licensees. In this part, we will determine whether these provisions better protect consumer and business information, and whether they are holistically better for the consumer, the insurance company, or both.

A. IDSA's Exemption Provision from Information Security Program Compliance

The IDSA governs licensees,[115] which include every business entity or person subject to the license requirements under Title 38 of the South Carolina Code: insurance companies that sell insurance policies,[116] insurance producers and agencies,[117] insurance brokers,[118] and public insurance adjusters.[119] However, other entities not commonly thought to be subject to the South Carolina insurance laws include rental car companies,[120] self-storage facilities,[121] and bail bondsmen and runners.[122] Currently, it is unclear whether these entities must adhere to the IDSA requirements. Although numerous entities are subject to the IDSA, the legislation does provide several exemptions to licensees who do not have to comply with creating, maintaining, and implementing an information security program.[123]

115. S.C. CODE ANN. § 38-99-10(9) (Supp. 2019) ("[A] person licensed, authorized to operate, or registered, or required to be licensed, authorized, or registered pursuant to the insurance laws of this State . . . .").

116. S.C. CODE ANN. § 38-5-10 (2015) ("Every insurer doing business in this State must be licensed and supervised by the director or his designee . . . ."). Insurers must have a license in order to sell the following types of insurance in South Carolina: life insurance, accident and health insurance, property insurance, casualty insurance, surety insurance, marine insurance, title insurance, multi-line insurance. *See id.* § 38-5-30.

117. *Id.* § 38-43-20(A).

118. *Id.* § 38-45-20.

119. *Id.* § 38-48-20.

120. *Id.* § 38-43-500(B).

121. *See* S.C. CODE ANN. § 38-43-640(B) (Supp. 2019).

122. S.C. CODE ANN. § 38-53-90(A) (2015). A "runner" is a person employed by a bail bondsman who assists the bail bondsman present the defendant in court when it is required. *Id.* § 38-53-10(10).

123. *See* § 38-99-70(A) (Supp. 2019).

As noted above, one of these key exemptions includes licensees who have fewer than ten employees.[124] The South Carolina General Assembly added this provision because the state has a relatively low number of licensees employing fewer than ten employees; otherwise, the IDSA would have little effect if it did not cover a vast majority of the licensee population.[125] The top ten insurers of automobile insurance and the top ten insurers of homeowners insurance within South Carolina, two of the most widely purchased insurance products among consumers,[126] account for over 87%[127] and 66%[128] of the state's insurance market respectively. These top ten companies—State Farm, Nationwide, Progressive, Allstate and others—each employ well beyond the cutoff number to qualify for the exemption.[129] Although homeowners licensees likely include companies who have less than ten employees to qualify for this exemption than automobile licensees—based upon South Carolina's total insurance market share—it is likely that second- and third-tier insurance companies (regarding employment numbers) form a majority of the South Carolina market not within the top insurers' control.[130] This assumption falls in line with the purported purpose of the IDSA, in that it protects consumer information from cyber threats. The South Carolina Department of Insurance (SCDOI) should target those licensees who cover the most South Carolina residents, which would include the top- and mid-tier insurers.[131]

This analysis then begs the questions—What will happen to these small licensees? Because the IDSA exempts licensees having fewer than ten employees, it leaves those licensees with two options moving forward: choose to invest in an information security program or take advantage of their exempt status by not implementing an information security program. However, one

---

124. § 38-99-70(A)(1).

125. *See A Firm Foundation: How Insurance Supports the Economy*, INS. INFO. INST., [hereinafter *A Firm Foundation*], https://www.iii.org/publications/a-firm-foundation-how-insurance-supports-the-economy/state-fact-sheets/south-carolina-firm-foundation [https://perma.cc/6YV3-7DWL] (listing the top insurers in South Carolina, all of whom possess more than ten employees).

126. NAT'L ASS'N INS. COMM'RS, OVERVIEW OF THE 2018 INSURANCE MARKET IN SOUTH CAROLINA (2019), https://www.naic.org/state_report_cards/report_card_sc.pdf [https://perma.cc/9UY2-KLZS] (listing the premiums written by line of business in South Carolina).

127. *A Firm Foundation*, *supra* note 125.

128. *Id.*

129. *See id.*

130. *See List of Insurance Companies Authorized to Transact Business in South Carolina As of October 2019*, S.C. DEP'T OF INS. (Oct. 2019), https://doi.sc.gov/DocumentCenter/View/12238/All-Companies?bidId= [https://perma.cc/U3QX-D5VP] (identifying the insurance companies licensed to do business in South Carolina).

131. *See A Firm Foundation*, *supra* 125 (identifying the insurers covering the most South Carolina residents).

of these choices is detrimental to a small licensee's future whereas the other may save it. If a licensee chooses not to invest in information security, its customers are likely to move their businesses from that licensee to one which has invested in an information security program.[132] Therefore, although the IDSA exemption provision does not require small licensees to comply with the information security program provision, it does heavily incentivize these licensees to invest in information security because, otherwise, they will risk losing business opportunities.[133] Although consumers may not know of the small licensee's security programs because such programs often appear within a contract's fine print, which the consumer seldomly reads, with the rise of cybersecurity and data breach events in the media, it is likely that more potential customers would investigate further to discover what security initiatives are in place.[134] Furthermore, assuming that the IDSA exemption applies, a small licensee still faces subsequent liability if a data breach occurs because a consumer could use the reasons for that breach, such as objectively inadequate security protocols, to show a lack of due care towards the consumer.

The fear for these small licensees is in bearing the cost necessary to implement expensive information security initiatives in order to save business.[135] The average cost of implementing an information security program can be substantial, and the costs after an incident could be catastrophic.[136] However, because the IDSA provides an exemption for small licensees, they are not required to follow the rigorous mandates put forth in the IDSA.[137] Small licensees are free to invest as much or as little as they desire into information security, allowing them to operate their businesses as they improve their security measures. Allowing small businesses to improve their information security at their own pace, in turn, is beneficial for both the insurance industry and the consumer. The consumer benefits because they now have more options in the insurance market, and they also benefit because

132. *See* PWC, CONSUMER INTELLIGENCE SERIES: PROTECT.ME 3 ("[Eighty-five percent] of consumers will not do business with a company if they have concerns about its security practices.").

133. *See id.*

134. *See* Christopher Elliott, *Here It Is: The Reason You Must Read the Fine Print Before You Travel!*, CHRISTOPHER ELLIOTT (Aug. 18, 2019), https://chriselliotts.com/read-the-fine-print-before-you-travel/ [https://perma.cc/85D9-6M28].

135. *See* Amy O'Connor, *South Carolina Passes First Insurance Industry Cybersecurity Law*, INS. J. (May 31, 2018), https://www.insurancejournal.com/news/southeast/2018/05/31/490672.htm [https://perma.cc/K867-UGCR].

136. *See* HISCOX, 2018 HISCOX: SMALL BUSINESS CYBER RISK REPORT 4 (2018) (stating small businesses cite lack of budget as reason for not having a security program, while estimating the average cost to a small business for a cybersecurity incident is over thirty-four thousand dollars).

137. *See* S.C. CODE ANN. § 38-99-70(A)(1) (Supp. 2019).

small licensees are incentivized to invest in information security programs. Although it appears the insurance industry, at least those top insurers, is worse off because of the increased competition in the marketplace, it actually may benefit from this provision. More insurers in the market means more market distribution. Top insurers can be more selective concerning their underwriting processes, marketing themselves to a more select group of consumers who have lower risk profiles. This benefits top insurers' overall premium income because they are not forced take on more risky insureds.

B. Cybersecurity Event and Notification Under the IDSA

A cybersecurity event is the "unauthorized access to or the disruption or misuse of an information system or the information stored on an information system."[138] The definition implicitly excludes those entities who do not store electronic information on an information system because the IDSA only requires protection of data on these electronic information systems.[139] This definition also provides two safe harbor provisions that are not considered "cybersecurity events," which means that covered entities would not have to report such events to the Director.[140]

The first safe harbor provides that covered entities do not have to report an event if it includes the "unauthorized acquisition of encrypted nonpublic information," and the encryption, process, or encryption key is not acquired or released without authorization.[141] The definition essentially provides a safe harbor for unsuccessful cyberattacks on a covered entity's information system.[142] Furthermore, although this definition is in line with the NAIC's Model Law, it is significantly narrower in scope compared to the New York Regulations.[143]

---

138. S.C. CODE ANN. § 38-99-10(3) (Supp. 2019).

139. "Information system' means a discrete set of *electronic* information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of *electronic* information, as well as any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems, and environmental control systems." § 38-99-10(8) (emphasis added); Condon, *supra* note 85.

140. Mooney et al., *supra* note 105.

141. *See* § 38-99-10(3); *see also* Mooney et al., *supra* note 105 (explaining factors that are needed to satisfy the first safe harbor under the IDSA).

142. *See* Mooney et al., *supra* note 105

143. *See* N.Y. COMP. CODE R. & REGS. tit. 23 § 500.1(d) (2018) ("Cybersecurity Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System."); *see also* Mooney et al., *supra* note 105 (explaining that the New York Regulations include not only successful cyberattacks but also unsuccessful ones within their definition of "cybersecurity event" whereas the IDSA does not).

The second safe harbor equates to a good faith mistake on behalf of the covered entity.[144] Under this provision, a cybersecurity event does not occur if the breached nonpublic information, "has not been used or released and has been returned or destroyed."[145] In this scenario, a "cybersecurity event" is not triggered, and the covered entity does not have to notify the Director.[146]

The IDSA requires a licensee to notify the Director within seventy-two hours of a cybersecurity event in one of two scenarios: (1) if the licensee is domiciled in South Carolina or (2) when the licensee reasonably believes at least 250 South Carolina residents' nonpublic information is involved, and the licensee is required to notify any governmental branch or agency, or the cybersecurity event has a reasonable likelihood of materially harming consumers or the licensee's business.[147] This provides a slightly narrower notification requirement for non-domestic licensees versus domestic licensees. However, notification to the Director is unnecessary if the incident does not classify as a cybersecurity event.[148] Recall, a cybersecurity event does not include instances when the acquired nonpublic information is encrypted and when the encryption key or process is not acquired.[149] In effect, an unauthorized user could steal a licensee's entire encrypted stockpile of nonpublic information—its credit information, employees' social security numbers, customers' home addresses—without the licensee needing to report the event to the Director so long as the perpetrator did not access the encryption key.[150]

Furthermore, recall that a cybersecurity event does not include incidents where the licensee determines that the unauthorized access of nonpublic information was not used or released, and was returned or destroyed.[151] The IDSA does not provide any criteria or guidelines for a licensee to determine whether the nonpublic information was used or released.[152] It places the discretion in the hands of the licensee itself, the party that appears to have a conflict of interest in notifying of such an incident.

These safe harbors and notification requirements ultimately hurt the consumer. Due to these safe harbors and notification restrictions, licensees do not need to notify the Director of certain types of data breaches despite the

144. *See* § 38-99-10(3); *see also* Mooney et al., *supra* note 105 (explaining the necessary factors in order to satisfy the second safe harbor under the IDSA).

145. § 38-99-10(3).

146. S.C. Dep't of Ins., *Complying with the SC Insurance Data Security Act*, YOUTUBE at 14:46 (Sept. 10, 2018), https://www.youtube.com/watch?v=7GmjRWH0qvM [https://perma.cc/53S6-PL7X].

147. S.C. CODE ANN. § 38-99-40(A) (Supp. 2019).

148. *Id.*

149. § 38-99-10(3).

150. *See id.*

151. *Id.*

152. *See id.*

licensee's information security plan being compromised.[153] This deprives the Director the opportunity to examine and determine whether theses licensees comply with the IDSA. Although the South Carolina Code requires businesses to report such breaches to consumers,[154] this notification is a retrospective remedy and does not incentivize licensees to protect customer information until a breach has already occurred. If the Director was able to examine a licensee after one of these unreviewable breaches occurred, it could lead to the Director's discovering weak points in the licensee's information security program without levying an administrative penalty against it. However, because these safe harbors do not require reporting, the Director is not aware of these breaches, which may lead to less examinations of the licensees that need it the most. Thus, this provision does not promote the protection of consumer information.

C. Penalties for Violation

The IDSA provides a provision that penalizes a covered entity for failing to comply with its provisions.[155] The provision states that an insurer who violates the IDSA is subject to an administrative penalty of no more than $15,000, license revocation, or both.[156] However, if the insurer commits a willful violation, the penalty increases to be not more than $30,000, license revocation, or both.[157] If the violator is a person, the penalty for noncompliance is no more than $2,500, and for willful noncompliance, the penalty will not exceed $5,000, with the threat of license revocation present in both scenarios.[158] The IDSA penalty provision works in tandem with another provision that allows the Director to examine a licensee's affairs for violations and allows the Director to enforce the IDSA.[159] Worth noting, the IDSA's administrative penalties are in addition to any other "criminal penalties provided by law or any other remedies provided by law," and they do not preclude other criminal or civil proceedings from taking place before, during, or after the administrative proceeding.[160] However, the IDSA also declares that the documents and materials collected by the Director during an examination of a covered entity are confidential by law, precluded from

153. § 38-99-40(A).

154. *See* S.C. CODE ANN. § 39-1-90(A)–(B) (1985 & Supp. 2019).

155. S.C. CODE ANN. § 38-99-80 (Supp. 2019) (cross referencing to title 38, chapter 2, section 10 of the South Carolina Code, which details the administrative penalty for violating any of the South Carolina insurance laws).

156. S.C. CODE ANN. § 38-2-10(A)(1) (2018).

157. *Id.*

158. § 38-2-10(A)(2).

159. S.C. CODE ANN. § 38-99-50 (Supp. 2019).

160. § 38-2-10(B).

disclosure, and are neither discoverable nor admissible in a civil action.[161] In order to incentivize licensees to comply with the IDSA's mandate, the Director threatens to levy these administrative fines on the licensee.[162] However, this administrative fine is not steep enough to convince licensees to comply with the IDSA, and the consumer will ultimately be subject to its ramifications.

The IDSA enforcement provision will end up targeting mid-tier licenses[163] because the larger licensees likely do business in not only South Carolina but also in other states, like New York, which require more stringent cybersecurity standards.[164] If these larger South Carolina licensees are doing business in New York,[165] and if these licensees can also satisfy the IDSA requirements by complying with the New York Regulations,[166] then the IDSA effectively is not targeting these larger licensees because they are adhering to stricter requirements. Furthermore, these larger licensees are likely already in compliance because they have larger budgets to invest into cybersecurity and information security programs due to their expanded product lines, larger consumer bases, and more sophisticated and complex information systems.[167] New York may have arguably set the standard for data security due to its more extensive requirements for these larger licensees, but the New York Cybersecurity Requirements would likely not apply to the mid-tier licensees who do not do business outside of South Carolina or the Southeast. Furthermore, even if these larger licensees were not in compliance with the IDSA, the penalty levied against these companies is inadequate to deter future noncompliance due to the high amounts of revenue these companies collect.[168] Due to the fact that the top insurers provide insurance products to the vast majority of consumers in South Carolina and because these licensees are likely already to be in compliance with the IDSA, these realities leave the

161. S.C. CODE ANN. § 38-99-60(A) (Supp. 2019).

162. § 38-2-10(B).

163. Licensees who are not considered the major insurers in the country.

164. *See A Firm Foundation*, *supra* note 125.

165. *Compare id.* (providing lists of large insurance companies doing business in South Carolina), *with Licensed New York Insurers*, ELANY, https://www.elany.org/dc_update.aspx [https://perma.cc/6Y79-LSL2] (showing that eighty-five percent of South Carolina's top twenty insurers in both homeowners' insurance and automobile insurance also do business in New York).

166. *See* S.C. Dep't of Ins., *supra* note 146.

167. *See* Sam Friedman & Nikhil Gokhale, *Pursuing Cybersecurity Maturity at Financial Institutions*, DELOITTE (May 1, 2019), https://www2.deloitte.com/us/en/insights/industry/financial-services/cybersecurity-maturity-financial-institutions-cyber-risk.html [https://perma.cc/9S4C-XVXQ].

168. *See Facts + Statistics: Industry Overview*, INS. INFO. INST., https://www.iii.org/fact-statistic/facts-statistics-industry-overview#Insurance%20industry%20at-a-glance [https://perma.cc/9KN7-JTAG] (stating property and casualty net premiums equaled $558.2 billion in 2017).

minority of the South Carolina insurance consumer market to the mid-tier licensees to capture.[169] However, even for these mid-tier licensees, the penalty is not adequate to incentivize compliance with the IDSA.

For mid-tier licensees, the average cost to implement any information security program will be between $33,000 and $54,000.[170] This breakdown, by itself, may suggest that the cost to come into compliance is similar to the cost of the penalty; however, there are more costs associated with coming into compliance with the IDSA. The IDSA requires the licensee to either designate an employee or outside vendor to be responsible for the information security program.[171] If the licensee decides to appoint an employee, that employee must be reasonably qualified to oversee the information security program.[172] The salary for one of these cybersecurity experts ranges $64,000–$88,000, annually.[173] If the mid-tier licensee is a larger company or deals with more sensitive information, it would be reasonable to employ multiple cybersecurity experts to oversee the information security program.[174] Furthermore, the costs to upgrade technology and implement staff training to prevent a cybersecurity event will elevate those costs as well.[175] This increased cost to comply with the IDSA, coupled with the infrequent examination by the SCDOI (at least once every five years)[176] will lead these mid-tier companies to play the odds concerning the violation provision. If licensees do not invest to be compliant with the IDSA, then they will be susceptible to only one $30,000 fine every five years.[177] The costs of implementing the information security program would pay for that administrative fine at least twice within the first year.

Therefore, the administrative penalty for not complying with the IDSA will not deter the targeted licensees to comply with the IDSA. This is ultimately detrimental to the consumer because the penalty is not harsh enough to outweigh the cost of complying with the IDSA's requirements. This will lead to greater risks of cybersecurity events for those licensees which lack a comprehensive information security program.

---

169. *See A Firm Foundation, supra* note 125.

170. *See* KASPERSKY, CYBERSECURITY FOR BUSINESS–COUNTING THE COSTS, FINDING THE VALUE 6–7 (2017).

171. S.C. CODE ANN. § 38-99-20(C)(1) (Supp. 2019).

172. *See id.*

173. *See IS and Cyber Security Professional - Intermediate Salary in Columbia, South Carolina*, SALARY.COM, https://www.salary.com/research/salary/alternate/is-and-cyber-security-professional-intermediate-salary/columbia-sc [https://perma.cc/435X-RWS2].

174. § 38-99-20(A) ("Commensurate with the size and complexity of the licensee . . . each licensee shall develop . . . a comprehensive written information security program . . . .").

175. *See* KASPERSKY, *supra* note 170.

176. *See* S.C. CODE ANN. § 38-13-10(A) (2015).

177. *See id.*; S.C. CODE ANN. § 38-2-10 (Supp. 2019).

D. Third-Party Service Providers

A third-party service provider is a person that contracts with a covered entity to "maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to" the covered entity.[178] Covered entities must evaluate and include an assessment of any third-party service provider's security programs used in connection with the licensee's information security program.[179] If the covered entity has a board of directors, the IDSA places the duty on the board to oversee third-party service providers.[180] Furthermore, a licensee must "exercise due diligence" when selecting its third-party service providers.[181] After a licensee makes its selection, it must require that third-party service provider to implement appropriate measures to protect and secure the information and systems held by or accessible to the third-party service provider.[182]

If a licensee decides not to retain an in-house employee or department to implement and oversee the information security program, the licensee must outsource this job to a vendor or third-party service provider.[183] If the licensee wishes to use a third-party service provider, it must account for that provider at all steps of review and throughout the implementation of the information security program.[184] The IDSA also requires a licensee's board of directors to annually report "material matters related to the information security program," which explicitly includes third-party service provider arrangements.[185] It also requires third-party service providers implement "appropriate . . . measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider."[186] Furthermore, the IDSA implicitly requires the licensee to oversee the third-party service providers it contracts with, meaning the licensee may be subject to IDSA penalties if it fails to adequately use due diligence in selecting and overseeing the third-party service provider.[187]

178. S.C. CODE ANN. § 38-99-10(16) (Supp. 2019).
179. § 38-99-20(C)(2).
180. § 38-99-20(E)(1)(b)(ii).
181. § 38-99-20(F)(1).
182. § 38-99-20(F)(2).
183. *See* § 38-99-20(C)(1).
184. § 38-99-20.
185. § 38-99-20(E)(1)(b)(ii).
186. S.C. CODE ANN. § 38-99-29(F)(2) (2015). The Model Law provides nearly identical language, requiring licensee's to establish arrangements with third-party service providers "to protect and secure the Information Systems and Nonpublic Information that are accessible to, or held by, the Third-Party Service Provider." INS. DATA SEC. MODEL LAW § 4(F)(2) (NAT'L ASS'N OF INS. COMM'RS, 2017).
187. § 38-99-20(E)(1)(b)(ii).

Although the IDSA requires licensees to use due diligence, it does not provide clear guidance regarding the scope of "due diligence." This is problematic because, as discussed above, a licensee is subject to penalties if it does not use due diligence.[188] While not explicitly providing an answer to this dilemma, the SCDOI provided information regarding evidence on how due diligence is exercised, which includes whether the licensee investigated the reputation of the third-party service provider, what level of access and what safeguards are in place to protect the licensee's information systems, what contractual terms are in place, and whether the licensee or the third-party service provider have cyber insurance.[189]

Even though these factors are helpful and likely necessary for a licensee to exercise due diligence in making its selection, one factor stands above the rest. Specifically, the contract terms between the licensee and the third-party service provider are essential in determining whether a licensee has performed its due diligence throughout the selection process. Since the IDSA requires licensees to oversee third-party service providers because these providers may subject the licensee to IDSA violations vicariously through the provider, the licensee must endeavor to place stringent oversight and supervisory provisions within the terms of such contracts. A licensee must be able to evaluate the privacy and security practices of its third-party service provider, which means that they must agree to contract terms granting the licensee with access it needs to gain a better understanding of the service provider's operations and security measures.[190] Other terms that must be addressed in such service agreements include the following: the third-party service provider's policies align with the mandates placed upon the licensee, notification controls alert the licensee if a cyberattack occurs, and the licensee is able to create procedures that allows it to supervise the third-party service provider.[191] Although the due diligence dilemma for licensees is profound, it is not the only area of uncertainty a licensee faces with regard to its third-party service provider usage.

As noted above, the IDSA requires its third-party service providers to implement appropriate measures to protect the information systems and nonpublic information while also implicitly requiring the licensee to oversee its third-party service providers in order to remain compliant.[192] However, the

188. *See* S.C. CODE ANN. § 38-99-80 (Supp. 2019).

189. *See* S.C. Dep't of Ins., *supra* note 146, at 41:39.

190. *See* Una A. Dean et al., *How Much Will Be Enough?: Third-Party Diligence Under the NYDFS Cybersecurity Requirements*, N.Y. L.J. (May 31, 2019), https://www.law.com/newyorklawjournal/2019/05/31/how-much-will-be-enough-third-party-diligence-under-the-nydfs-cybersecurity-requirements/ [https://perma.cc/R26B-898Q] (noting "diligence" is an ongoing process).

191. *See id.*

192. *See* § 38-99-20(E)(1)(b)(ii); § 38-99-20(F).

IDSA does not provide any more direction as to how those "appropriate measures" apply to third-party service providers.[193] One may argue that licensees must require their third-party service providers to implement protective measures that correspond with the IDSA's information security program because these provisions are so intertwined with and instrumental in the licensee's use of third-party service providers in the first place.[194] Furthermore, if a licensee is going to use a third-party service provider to implement and maintain its information security program, it must follow that the third-party service provider must also adhere to the provisions mandated on the licensee.[195]

However, one may also argue that if the South Carolina General Assembly intended for third-party service providers to follow the IDSA guidelines, then it would have explicitly done so. Instead, it only requires these service providers to implement "appropriate administrative, technical, and physical measures to protect" nonpublic information and information systems.[196] The term *appropriate* is ambiguous and has two possible interpretations. One interpretation is that third-party service providers are held to the same higher standard as licensees.[197] However, the second interpretation could imply a lower standard for third-party service providers regarding their protective measures for licensees because, while licensees must comply with extensive and specific requirements under the IDSA, third-party service providers, again, only need to implement those measures deemed appropriate.[198]

The former interpretation should be adopted. Although requiring third-party service providers to adhere to the more stringent provisions of the IDSA may lead to higher contracting costs to the licensee, it will provide these licensees with invaluable information. It will provide greater insight into the third-party service provider's privacy and security procedures, provide licensees with more information concerning weak points in their security system, and provide greater opportunity to anticipate and prevent future cybersecurity events. Despite the fact that the licensee may have to pay more to contract with these third-party service providers to gain more intrusive access to its systems, these costs would likely have been spent on internal information security program expenses, such as additional employee

193. *See* § 38-99-20(E)(1)(b)(ii); § 38-99-20(F).

194. *See* Theodore Augustinos, *A Closer Look at the NAIC Insurance Data Security Model Law*, JD SUPRA (Apr. 6, 2018), https://www.jdsupra.com/legalnews/a-closer-look-at-the-naic-insurance-36022/ [https://perma.cc/JU7Z-HEUZ].

195. *See id.*

196. *See* § 38-99-20(F).

197. Under this rationale, there is no logical reason to draw a distinction between the insurance company and the third-party service providers.

198. *See* § 38-99-20(F).

salaries,[199] additional costs regarding creation of an information security program,[200] and additional cybersecurity measures within the information security program.[201]

E. Reasonably Foreseeable Risks

Although there are many important facets of the IDSA concerning a licensee's compliance, the risk assessment is the starting point for a licensee's entire information security program.[202] With the broad coverage and reach of the IDSA through the definitions of licensee and nonpublic information,[203] the South Carolina General Assembly decided to place some limits on the scope of the IDSA by providing explicit and implicit safe harbors to what constitutes a cybersecurity event.[204] Through this lens, the licensee must undergo a risk assessment that acts as the starting point to create its data security program.[205]Although the IDSA does not provide a helpful definition of risk assessment,[206] it does require a licensee to "identify reasonably foreseeable internal or external threats" that could result in a cybersecurity event.[207] Like a math problem, if you use the right formula, but use the wrong numbers, you will get a wrong answer. Similarly, the IDSA provides data security protocols, but if a licensee fails to identify the correct threats, it may lead to a noncompliant information security program.[208]

Due to the minimal guidelines the IDSA provides licensees, it is difficult for these entities to discern what it must consider when designing its information security program. Although not a sufficient factor in discerning what reasonably foreseeable risks exist,[209] a good starting point would be to consider the licensee's size and complexity.[210] This factor necessarily informs the probability of a breach occurring.[211] With larger entities, there are more access points for hackers to exploit, and generally, larger entities implement

199. *See* § 38-99-20(C)(1).
200. *See* § 38-99-20(D)(1).
201. *See* § 38-99-20(D)(2).
202. Condon, *supra* note 85.
203. *See supra* notes 94–98, 115–122 and accompanying text.
204. *See* Condon, *supra* note 85.
205. *See id.*
206. S.C. CODE ANN. § 38-99-10(14) (Supp. 2019) ("'Risk assessment' means the risk assessment that each licensee is required to conduct under this chapter.").
207. *See* § 38-99-20(C)(2).
208. *See* Condon, *supra* note 85.
209. *See id.*
210. Almudena Arcelus et al., *How Much Is Data Security Worth?*, SCITECH LAW., Spring 2019, at 12–13.
211. *Id.*

more complex information systems.[212] Furthermore, as information systems become more complex, they also become more susceptible to attacks because they usually contain more lines of code, which makes it not only harder to test these systems for weaknesses but also easier for a hacker to exploit them.[213] A licensee must take into account its size and its information system's complexity because, as these two elements increase, so does the likelihood a data breach may occur.[214]

A licensee must also consider the type and sensitivity of information it stores or possesses when conducting its risk assessment.[215] The data market is as sophisticated as any, with cybercriminals selling varying types of nonpublic information valued at different rates.[216] Licensees, many of whom are insurers or brokers, handle sensitive information: Social Security numbers,[217] drivers licenses information,[218]credit card information,[219] online payment login information,[220] and medical records.[221] Accordingly, as the type of nonpublic information the licensee possesses becomes more lucrative in nature, the likelihood of facing a cybersecurity event increases.[222] Because licensees know they handle more sensitive information that are desirable to hackers, they must consider this element in analyzing the reasonably foreseeable risks they face.

When considering the type of information a licensee possesses or handles, it must also evaluate the severity of harm that may occur due to a breakdown or breach of its information security program.[223] A licensee should evaluate, considering that it possesses sensitive information, what harm may follow if

212. *See* Patrick Ercolano, *Study: Risk of Data Breaches at Hospitals Is Greater at Larger Facilities, Teaching Hospitals*, JOHN HOPKINS U. (Apr. 5, 2017), https://hub.jhu.edu/2017/04/05/hospitals-at-risk-of-data-breach-patient-records/ [https://perma.cc/23E6-Y4X2].

213. MCCABE SOFTWARE, MORE COMPLEX = LESS SECURE: MISS A TEST PATH AND YOU COULD GET HACKED 2, http://www.mccabe.com/pdf/More%20Complex%20Equals%20Less%20Secure-McCabe.pdf [https://perma.cc/28LB-NBGY].

214. *See* Arcelus et al., *supra* note 210, at 13.

215. *Id.*

216. Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ [https://perma.cc/AC3K-M5VV].

217. *Id.* (stating that Social Security numbers are valued at one dollar each).

218. *Id.* (stating that driver's licenses are valued at twenty dollars each).

219. *Id.* (stating that credit card numbers are valued between five and one hundred-ten dollars).

220. *Id.* (stating that online payment login information is valued between twenty and two hundred dollars).

221. *Id.* (stating that medical records are valued between one and one thousand dollars).

222. *See* Darius K. Davenport & W. Ryan Snow, *Hackers and Why They Hack—and Why You Need to Know*, FOR DEF., Oct. 2018, at 39.

223. *See* Condon, *supra* note 85.

a cybersecurity event occurred. If the effect of the harm is less severe because the type or amount of information the licensee possesses is not as sensitive, then its risk assessment would likely be less extensive than a licensee who possesses great quantities of sensitive information.[224]

Finally, a licensee should consider its use of third-party service providers when it conducts its risk assessment.[225] Third-party service providers have been cited as a major vehicle for hackers to infiltrate entities and cause data breaches.[226] Third-party service providers are a potential danger to licensees because these providers could maintain the licensee's nonpublic data and provide access for a hacker into the licensee's information system.[227] Because third-party service providers are a potential liability towards a licensee's information security program, it must take adequate measures in vetting its service provider such as conducting a risk assessment on the third-party service provider itself.[228]Although the IDSA requires a licensee to conduct a risk assessment but does not provide a system in which to conduct that assessment, these factors account for the essential questions a licensee must tackle in order to design, implement, and maintain a compliant information security system. However, this assessment is not limited to these factors, rather these factors provide only a good place to start for licensees conducting their risk assessment.

IV. CONCLUSION

In today's day and age where businesses collect more valuable data to gain a competitive edge and hackers become more brazen in how they access that information, cybersecurity protocols are coming to the forefront of issues for consumers. Insurance companies, in particular, are in hacker's crosshairs because they possess vast amounts of valuable data but lack adequate security protocols to protect it. The IDSA represents a strategy to fight against these occurrences through mandatory information security programs designed to prevent cybersecurity events from happening. Although the IDSA will likely mitigate the effects of cyberattacks, it will not protect consumers in the manner that it strives for. Without more guidance to these issues regarding the IDSA's provisions, licensees will be frustrated due to penalties for noncompliance, which will lead to consumer distrust. Additionally, without a more severe penalty, licensees do not have a deep incentive to comply with

224. *See id.*

225. *Id.*

226. John Thomas A. Malatesta III et al., *A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses*, 17 SEDONA CONF. J. 761, 761 (2016) (citing the Target, Home Depot, and T-Mobile data breaches).

227. *Id.* at 763.

228. *See id.* at 769.

the mandates. Those appointed to oversee the IDSA's enforcement start out crippled due to the two major notification safe harbors, possibly leading to countless breaches going undocumented. Without more explanation from the SCDOI, consumers will ultimately pay the price, whose nonpublic information will be more vulnerable to attack without further guidance.