FOLLOW THE LAW . . . EVERYWHERE? HOW DIFFERENCES IN DATA BREACH REGULATIONS CREATE COMPLIANCE CONCERNS FOR NORTH DAKOTA PRACTITIONERS

ABSTRACT

Under modern privacy law, there is no federal comprehensive data breach notification requirement. Absent a federal standard, U.S. states and territories have enacted legislation with similar, yet varying provisions. This forces legal practitioners to navigate the lack of uniform standards, differing terminology, and various reporting requirements amongst jurisdictions, and do so quickly, when information has been compromised by an unauthorized source. When it comes to a data breach, the applicable laws in all fifty U.S. states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands can extend beyond geographical boundaries to cover notification requirements for their affected residents. This means that North Dakota practitioners must adhere to the state laws of their clients' home states in such instances, and accordingly, may be subject to the laws of other states when they offer legal services across state lines or assist in breach remediation. Moreover, an attorney retained to remedy a breach must comply with the state laws of affected persons' home states to avoid legal repercussions that may result from non-compliance.

The threat of data breaches is a growing concern in today's world with federal and state agencies receiving an increasing number of internet crime complaints. This concern is as existent in North Dakota as it is anywhere else. As technology evolves and cyberattacks become more sophisticated, North Dakota lawyers and firms need to be aware of the significant risk that data breaches pose on individual privacy. Attorneys have a legal and ethical obligation to prevent disclosure of, or unauthorized access to, client information, and understanding the intricacies of data breach compliance is at the forefront of this responsibility.

I. INTRODUCTION

The threat of cyberattacks is a growing concern, and a concern which is increasingly prevalent in North Dakota. In its annual Internet Crime Report ("2023 Internet Crime Report"), the Federal Bureau of Investigation (FBI) identified cybercrime incidents and reporting data from across the country.[1]

1. *See generally* FED. BUREAU OF INVESTIGATION, 2023 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT CTR. 3-4 (2023), https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf [https://perma.cc/9UNV-J38Z].

According to the FBI's Internet Crime Complaint Center ("IC3"), Americans filed a record number of 880,418 complaints in 2023, an almost ten percent increase from complaints received in 2022.[2] The 2023 Internet Crime Report indicated that 764 complaints arose out of North Dakota, an approximately 8.6 percent increase from North Dakota complaints received in 2022.[3]

Data breaches are not only a growing concern, but an increasingly costly one. Globally, the average cost of remediating a data breach is $4.88 million, a ten percent increase from 2023, as reported in International Business Machines Corporation's (IBM's) annual Cost of a Data Breach Report 2024.[4] This increased cost of breach remediation is due "mostly from expenses related to business disruption and post-breach responses."[5] Compared to the fifteen other geographic regions analyzed in IBM's annual report, the United States was found to have the highest average cost associated with data breaches, for the fourteenth year, at $9.36 million.[6] The most commonly compromised information, involved in forty-six percent of breaches, is "customer personal identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses."[7]

Alongside a general increase in cyber threats and cost of breach remediation, today's society is also experiencing an increase in digital storage and technology usage.[8] "A data center is a highly specialized, secure facility designed to provide a safe, dependable, and controlled environment for the fast, reliable, and uninterrupted storage, processing, management, and transmission of digital data."[9] While in office, former North Dakota Governor Doug Burgum announced the construction of a $1.9 billion data center near

2. *Id.* at 3. *See generally Frequently Asked Questions*, INTERNET CRIME COMPLAINT CTR., https://www.ic3.gov/Home/FAQ [https://perma.cc/AN4T-94R3] (last visited May 14, 2025) ("Anyone who believes they are affected by a cyber-enabled crime may file a complaint with the IC3 . . . .").

3. *See* FED. BUREAU OF INVESTIGATION, *supra* note 1, at 24; *see also* FED. BUREAU OF INVESTIGATION, 2022 INTERNET CRIME REPORT, INTERNET CRIME COMPLAINT CTR. 25 (2022), https://www.ic3.gov/AnnualReport/Reports/2022_IC3Report.pdf [https://perma.cc/RCG7-JMVF].

4. IBM, COST OF A DATA BREACH REPORT 2024 5, 8 (2024), https://www.ibm.com/downloads/documents/us-en/107a02e94948f4ec [https://perma.cc/XT74-U6XF].

5. *See id.* at 8.

6. *Id.* at 9.

7. *Id.* at 6.

8. *See generally* FED. BUREAU OF INVESTIGATION, *supra* note 1, at 3; IBM, *supra* note 4, at 5; Susan J. Booth, *Behind the Walls of a Digital Palace: Understanding, Buying, Operating, and Financing Data Centers*, 40 PRAC. REAL EST. LAW. 12, 12 (2024) ("In the United States and many other industrialized nations, almost all non-verbal communications . . . are now stored, transmitted, and processed in a digital format. Data centers are the palace in which that digital information resides.").

9. Booth, *supra* note 8, at 12.

Williston.[10] Since then, rumors have circulated regarding the future of data hubs located in North Dakota.[11] Likely an attractive location for additional data centers, "North Dakota produces vast amounts of energy from the many abundant sources available."[12] Additionally, North Dakota's cold climate to keep data centers from overheating and the state's tax incentives may further contribute to the appeal.[13]

In the first five months of 2025, twelve additional data centers were established in North Dakota.[14] Regardless of whether the state becomes home to additional data centers, which would accompany the now nineteen existing North Dakota locations, understanding what legal frameworks are in place to ensure individuals' right to privacy and comply with data breach laws is crucial for this state's practitioners.[15] Awareness of data breach notification requirements as legal practitioners is relevant and undoubtedly timely with the continuous evolution of technological advances. Businesses and firms do not need to have employees nor own property in other states to be bound by other states' data breach notification laws.[16] Rather, "[e]ach breach notification law

10. *See generally Burgum: One of World's Largest Data Centers to Locate in Williston Area as Industry Targets Growth in ND*, N.D. OFFICE OF THE GOVERNOR (Jan. 26, 2022, 11:20 AM), https://www.governor.nd.gov/news/burgum-one-worlds-largest-data-centers-locate-williston-area-industry-targets-growth-nd [https://perma.cc/9877-GVFB].

11. Brooke Dudley, *Data Center Boom: A Golden Opportunity for Property Owners in North & South Dakota*, LANDGATE (Apr. 24, 2025), https://www.landgate.com/news/data-center-boom-a-golden-opportunity-for-property-owners-in-north-south-dakota [https://perma.cc/B7G3-L55K] ("At least six additional data centers are in development, as noted by Aaron Birst, Executive Director of the North Dakota Association of Counties."); Georgia Butler, *Two Companies Seek to Develop $125bn AI Data Centers in North Dakota – Report*, DATA CTR. DYNAMICS (Sep. 4, 2024), https://www.datacenterdynamics.com/en/news/two-companies-seek-to-develop-125bnai-data-centers-in-north-dakota/ [https://perma.cc/VZ8H-E2NG] ("Two companies are looking to develop artificial intelligence (AI) data centers in North Dakota.").

12. *See generally Energy and Natural Resources*, N.D. DEP'T OF COM., https://www.commerce.nd.gov/economic-development-finance/energy-and-natural-resources [https://perma.cc/RK5V-RW23] (last visited May 14, 2025).

13. *See generally Building Business: Why Midco is Ready to Help Big Tech Go Beyond in North Dakota*, MIDCO BUS.: INSIGHT CTR. (Sep. 13, 2024), https://business.midco.com/insight-center/2024/september/building-business-why-midco-is-ready-to-help-big-tech-go-beyond-in-north-dakota/ [https://perma.cc/BBP2-897A]; Laura Simmons, *Data Centers Love North Dakota. Should North Dakota Love Them?* DAILY YONDER (Aug. 21, 2023), https://dailyyonder.com/data-centers-love-north-dakota-should-north-dakota-love-them [https://perma.cc/D29A-3KRS].

14. *See generally* Niva Yadav, Teton Digital Gets Go-Ahead for 100MW Data Center in North Dakota, DATA CENTER DYNAMICS (Feb. 20, 2025), https://www.datacenterdynamics.com/en/news/teton-digital-gets-go-ahead-for-100mw-data-center-in-north-dakota (noting that seven data centers existed in North Dakota when this article was written in February 2025).

15. *See generally North Dakota Data Centers*, DATA CTR. MAP, https://www.datacentermap.com/usa/north-dakota/ [https://perma.cc/HP3N-9CX3] (last visited May 14, 2025) (North Dakota's total of nineteen data centers are located in Bismarck (1), Fargo (4), Grand Forks (2), Williston (8), Ellendale (3), and Jamestown (1)).

16. *See* JEFF KOSSEFF, CYBERSECURITY LAW 46 (John Wiley & Sons, Inc. 3d ed. 2023).

applies to the unauthorized acquisition of information belonging to that state's residents, provided that the company conducts business in the state—a low threshold."[17]

A. WHAT IS A DATA BREACH?

The 2023 Internet Crime Report provides, "[a] data breach in the cyber context is the use of a computer intrusion to acquire confidential or secured information, . . . not includ[ing] computer intrusions targeting personally owned computers, systems, devices, or personal accounts such as social media or financial accounts."[18] However, breaches of protected data are not only the result of malicious acts. Rather, data breach notification laws may be triggered by any unauthorized acquisition of personal information, "whether due to a cyberattack, a corporate error, or other incident."[19] Even the innocent mistake of sending an email containing personal information to the wrong email address may trigger data breach notification laws. Regardless of how the data is acquired, information obtained by the wrong person can result in serious consequences. With access to sensitive data, someone would be able to imitate the owner of the information or manipulate the data for personal gain, potentially leading to identity theft, fraud, and financial loss.[20]

B. WHAT IS PERSONAL INFORMATION?

Statutes vary across jurisdictions as to what data is considered personal information for breach purposes.[21] Considering this variation, breached data may be deemed personal information warranting notification in one state but may not be considered as such across state lines.[22] However, for a majority of states, personal information includes "an individual's first name or initial and last name, in combination with at least *one* of the following categories of information: (1) Social Security number; (2) driver's license or state identification number; or (3) account number, credit card number, or debit card number" and associated passcodes.[23] North Dakota is among the states that recognize the commonly associated categories of private information, such as Social Security identification and financial account information.[24]

17. *Id.*

18. FED. BUREAU OF INVESTIGATION, *supra* note 1, at 30.

19. *See* Emily Stackhouse Taetzsch, Note, *Privacy Purgatory: Why the United States Needs a Comprehensive Federal Data Privacy Law*, 50 J. LEGIS. 121, 130-31 (2024).

20. *See generally* IBM, *supra* note 4, at 12 ("PII . . . can be used in identity theft and credit card fraud.").

21. *See* KOSSEFF, *supra* note 16, at 48.

22. *See generally id.* at 48-49.

23. *Id.* at 48.

24. *See generally* N.D. CENT. CODE § 51-30-01(4) (2015).

However, compliance concerns arise out of a lack of national uniformity in what is deemed personal information as states include or exclude specific definitions from their notification statutes.[25]

C. STATES' JURISDICTIONAL CLAIMS OVER THEIR RESIDENTS

When a business discovers an unauthorized acquisition of personal information has occurred, it must act quickly to begin data breach remediation.[26] The laws of the state in which the compromised data's owner resides govern the breached entity's notification protocol.[27] For example, if an entity is doing business within the state of North Dakota and engages in business with a non-resident of the state, the North Dakota entity will be subject to following the requirements of the client's home state if the North Dakota business experiences a data breach and the client's unencrypted personal information is compromised.

D. WHAT IS ENCRYPTION?

All fifty states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands explicitly exempt personal information that has been encrypted from triggering the breach notification laws if the data is compromised.[28] Generally, encryption means that the information has been altered to be unusable without a compatible "confidential process or key."[29] However, "[m]ost of these laws do not provide technical specifics for encryption" and "many of the state encryption exceptions apply only if the encryption key was not accessed."[30] These variations amongst state laws may further add to the compliance concerns of breach notification obligations.

As defined by South Dakota, and similarly across the Eighth Circuit, encryption means that computerized data "is rendered unusable, unreadable, or

25. *See generally* KOSSEFF, *supra* note 16, at 48-49.

26. *See generally Data Breach Response: A Guide for Business*, FED. TRADE COMM'N (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business [https://perma.cc/N63A-XNHP].

27. *See* KOSSEFF, *supra* note 16, at 46.

28. *See generally id.* at 49 ("No state data breach notification laws require notification of the breach of personal information that is encrypted."); D.C. CODE § 28-3851(1)(B) (2020); P.R. LAWS ANN. tit. 10, § 4051(a) (2005); 9 GUAM CODE ANN. § 48.20(a) (2009); V.I. CODE ANN. tit. 14, § 2208(a) (2005).

29. *See* JAY P. KESAN & CAROL M. HAYES, CYBERSECURITY AND PRIVACY LAW IN A NUTSHELL 108 (2019) (citing OHIO REV. CODE ANN. § 1347.12(A)(4) (West 2023)).

30. KOSSEFF, *supra* note 16, at 49. *See generally* KESAN & HAYES, *supra* note 29, at 108 ("The states in this category [encryption exemption] all follow the general rule of defining encryption as a transformation of data so it cannot be used 'without use of a confidential process or key.'" (citing OHIO REV. CODE ANN. § 1347.12(A)(4) (West 2023))).

indecipherable without the use of a decryption process or key . . . ."[31] Encryption is illustratively comparable to protecting data behind a locked door.[32] When data is encrypted, the door serves as a barrier to the public that cannot be unlocked unless someone possesses the compatible key to unlock the door and get inside. When data is not encrypted, the door is unlocked and anyone who stumbles upon it could open the door and view the intimate details of what lies inside.[33]

Section 51-30-01(1) of the North Dakota Century Code identifies a data breach as an unauthorized acquisition of personal information that has *not been encrypted*.[34] Pursuant to the North Dakota statute, the state breach notification requirements are triggered "when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases *unreadable* or *unusable*."[35]

II. DATA BREACH REQUIREMENTS AND COMPLIANCE CONCERNS FOR THE NORTH DAKOTA PRACTITIONER

Absence of uniformity in data breach notification requirements may seem like a speculative concern, but a breach of personal information has become a real issue for numerous North Dakota residents.[36] This is an area of law that applies to every legal practitioner, regardless of practice area, as data breach compliance is paramount to protecting client data.[37] "Regardless of an attorney's clients or practice areas, as long as the Internet still exists and people still use computers throughout their personal and professional lives, data security will be an underlying concern in virtually everything that the attorney does."[38] To be prepared, practitioners should remain current on breach notification laws to best understand the applicability of the main categories of compliance: what is considered personal information, when and to

31. *See* S.D. CODIFIED LAWS § 22-40-19(2) (2018); *see also, e.g.*, IOWA CODE § 715C.1(5) (2018); NEB. REV. STAT. § 87-802(3) (2024).

32. *See generally* KESAN & HAYES, *supra* note 29, at 108.

33. Data breach notification statutes may be triggered when unencrypted data is compromised by an unauthorized source, meaning that the door is unlocked and now accessible to someone who does not have permission to view it. Additionally, some states' data breach notification statutes are triggered when encrypted data is compromised by an unauthorized source with to the compatible key, meaning that the door is locked but accessible to someone who does not have permission to view it *and* that person also has obtained the key to unlock the door. *See generally id.*

34. *See* N.D. CENT. CODE § 51-30-01(1) (2015).

35. *Id.* (emphasis added).

36. *See generally Data Breach Notices,* N.D. OFFICE OF ATTORNEY GENERAL, https://attorneygeneral.nd.gov/consumer-resources/data-breach-notices/ [https://perma.cc/E8B7-G3G5] (last visited May 15, 2025).

37. KESAN & HAYES, *supra* note 29, at 2.

38. *Id.*

whom notice must be provided, exceptions to providing notice, and whether civil actions may be commenced by an affected party.[39]

A. NORTH DAKOTA'S DATA BREACH NOTIFICATION REQUIREMENT

Under Section 51-30-01(1) of the North Dakota Century Code, a "[b]reach of the security system" occurs when there has been an "unauthorized acquisition of computerized data when access to *personal information* has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable."[40] Further defined by Section 51-30-01(4)(a), "[p]ersonal information" is any information containing:

> an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) [t]he individual's social security number; (2) [t]he operator's license number assigned to an individual by the department of transportation . . . ; (3) [a] nondriver color photo identification card number assigned to the individual by the department of transportation . . . ; (4) [t]he individual's financial institution account number, credit card number, or debit card number [and] . . . any required security code, access code, or password that would permit access to an individual's financial accounts; (5) [t]he individual's date of birth; (6) [t]he maiden name of the individual's mother; (7) [m]edical information; (8) [h]ealth insurance information; (9) [a]n identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or (10) [t]he individual's digitized or other electronic signature.[41]

Once made aware that personal information has been compromised, the breached entity must notify "any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person."[42] The methods of notice include (1) written notice; (2) electronic notice; or (3) substitute notice, which is permissible in circumstances where the notification cost would either exceed $250,000.00, more than 500,000 individuals need to be notified as a result of the breach, or the breached entity lacks sufficient contact information to otherwise notify

39. *See id.* at 95.
40. N.D. CENT. CODE § 51-30-01(1) (2015) (emphasis added).
41. *Id.* § 51-30-01(4)(a).
42. *See id.* § 51-30-02.

affected individuals.[43] Substitute notice under this chapter permits breach notification via electronic mail if the breached entity has email addresses for affected individuals, "[c]onspicuous posting of the notice" on the breached entity's webpage if it exists, and "[n]otification to major statewide media."[44]

Additionally, notice must be given by mail or email to the North Dakota Attorney General in any instance where a security breach affects more than 250 individuals.[45] All notification "must be made in the most expedient time possible and without unreasonable delay," except where notification is delayed for legitimate law enforcement investigatory purposes.[46] If the acquired information is encrypted or otherwise unreadable or useable, the breached entity is exempt from the notification procedures.[47]

The threshold for data to qualify as personal information under the North Dakota statute's definition is relatively low, and any unauthorized acquisition of such data requires notification to the state's affected residents.[48] Every year, data breaches affect "[c]orporations, legal and other firms, nonprofit organizations, academic institutions and government agencies[,]" and North Dakota entities are no exception.[49] Legal practitioners assisting in breach remediation must be able to identify the state residency of affected individuals and understand how each states' breach notification requirements differ in order to abide lawfully.[50]

B. COMPLIANCE DIFFICULTIES WITH OTHER STATES' BREACH NOTIFICATION REQUIREMENTS

When it comes to a data breach, there are numerous situations that may challenge a North Dakota practitioner when attempting to conform with the applicable notification laws across state lines. While several states' notification laws are comprised of similar language, others have unique provisions that North Dakota attorneys must be cognizant of in order to abide lawfully.[51] The first of the key differences is that notification of a breach is not necessary in certain states where a breach has not resulted, or is unlikely to result in, a

43. *Id.* § 51-30-05(1)-(3).

44. *See id.* § 51-30-05(3)(a)-(c).

45. *Id.* § 51-30-02.

46. *See id.* §§ 51-30-02, 51-30-04.

47. *See id.* §§ 51-30-01(1), 51-30-02.

48. *See generally id.* §§ 51-30-01(4)(a), 51-30-02.

49. Megan Silverman, *Data Breach Trends and Tips for Reducing Impacts*, ABA (Mar. 29, 2023), https://www.americanbar.org/groups/business_law/resources/business-law-today/2023-april/data-breach-trends-tips-for-reducing-impacts/. *See generally supra* text accompanying note 3.

50. *See* Taetzsch, *supra* note 19, at 130-31 ("State breach notification laws vary substantially regarding the precise method of notification to residents, the type of data that triggers notification, and next steps if sensitive data is exposed." (footnotes omitted)).

51. *See generally id.*

substantial risk to the individual.[52] However, North Dakota's breach notification laws do not include a "risk-of-harm provision[] and therefore require notification regardless of whether [a] company concludes that the breach is likely to lead to harm to individuals."[53]

Other states have identified distinct pieces of personal information that North Dakota does not protect under its breach notification statute.[54] Specifically, Puerto Rico protects work-related evaluations as personal information when compromised in combination with the individual's name or first initial and surname.[55] Additionally, in Wyoming, "[a] birth or marriage certificate" is protected as "personal identifying information" under its data breach notification laws.[56] Even if North Dakota does not deem certain data to be personal information, if unencrypted data is compromised and the affected individual is a resident of a state which recognizes it as personal information, the resident state's breach notification laws will be triggered and the North Dakota entity must comply anyways.[57] For example, if a North Dakota entity or law firm experiences a data breach through which someone has wrongfully obtained personal information belonging to a Wyoming resident, Wyoming's state data breach notification statute will govern how the entity responds to the Wyoming resident's breached data.[58]

The collection of biometric data may also put a North Dakota practitioner at odds if such information is compromised, as states have started to recognize this data as personal information.[59] Biometrics are "physical properties inherent in the human body" collected for identification purposes, such as fingerprints and retina scans.[60] In Iowa, Illinois, Nebraska, and South

52. *See* KOSSEFF, *supra* note 16, at 49 ("In most states, companies can avoid notification obligations if, after investigating the breach, they determine that the incident did not create a risk of harm for individuals whose personal information was exposed.").

53. *See generally id. Compare* MICH. COMP. LAWS § 445.72(1) (2011) ("Unless the person or agency determines that the security breach has not or is not likely to cause substantial loss or injury to, or result in identity theft with respect to . . . ."), *with* N.D. CENT. CODE § 51-30-02 (2015) ("Any person . . . shall disclose any breach of the security system following discovery or notification of the breach in the security of the data to any resident of the state whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.").

54. *See generally supra* note 52 and accompanying text.

55. *See* P.R. LAWS ANN. tit. 10, § 4051(a)(7) (2005).

56. *See* WYO. STAT. ANN. §§ 6-3-901(b)(x), 40-12-501(a)(vii) (2015).

57. *See generally* Taetzsch, *supra* note 19, at 125, 131 (2024) ("State breach notification laws vary substantially regarding the precise method of notification to residents, the type of data that triggers notification, and next steps if sensitive data is exposed." (footnotes omitted)); KOSSEFF, *supra* note 16, at 49 ("No state data breach notification laws require notification of the breach of personal information that is encrypted.").

58. *See generally* discussion *supra* Section I.C.

59. *Compare* N.D. CENT. CODE § 51-30-01 (2015), *with* IOWA CODE § 715C.1(11)(a)(5) (2018), 815 ILL. COMP. STAT. 530/5(1)(F) (2017), NEB. REV. STAT. § 87-802(5)(a)(v) (2016), *and* S.D. CODIFIED LAWS § 22-40-19(4)(e) (2018).

60. KESAN & HAYES, *supra* note 29, at 257.

Dakota, biometric data that is breached in combination with an individual's "first name or first initial and last name" is considered personal information that would warrant application of the states' respective notification requirements for their affected residents.[61] Though North Dakota has not yet added biometric data to its list of personal information criterion, obtaining such data is becoming a more common occurrence and practitioners would nonetheless be expected to comply with applicable state laws for those that do recognize it as such, if the information were to be compromised.[62]

Further differences in state data breach notification requirements include variations of who must be notified, how an affected person may be notified, and when the notification must be made.[63] While North Dakota requires notice to consumers and disclosure to the Attorney General if more than two hundred fifty individuals are affected by a data breach, other states have differing notification policies that may require an entity to provide notice to additional persons.[64] For example, Minnesota's statute provides that a breach requiring notice to more than five hundred Minnesota residents also requires notification "within 48 hours" to "all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis."[65]

The current patchwork of laws creates compliance concerns as legal practitioners may need to look to more than fifty statutes to understand what information is of concern, to what extent the information must be wrongfully acquired, and who must be notified when a breach occurs.[66] Noncompliance with state data breach requirements may result in civil penalties, as "[t]hirteen states allow residents to file civil actions against the breached entities, as well as DC, Puerto Rico, and the Virgin Islands."[67] With no federal laws to resolve numerous conflicts among states, consistency and uniformity is desperately needed as data breaches become a more impending threat.[68]

---

61. IOWA CODE § 715C.1(11)(a) (2018); *see also, e.g.*, 815 ILL. COMP. STAT. 530/5(1)(F) (2017); NEB. REV. STAT. § 87-802(5) (2016); S.D. CODIFIED LAWS § 22-40-19(4)(e) (2018). *See generally supra* notes 52-53 and accompanying text.

62. *See generally* KESAN & HAYES, *supra* note 29, 257 ("Commercially, many companies are starting to use fingerprint identification in order to cut down on timecard fraud among employees, and secure access to sensitive documents.").

63. *See generally supra* note 52 and accompanying text.

64. *See* N.D. CENT. CODE § 51-30-02 (2015); *see also* KOSSEFF, *supra* note 16, at 483-544.

65. *See* MINN. STAT. § 325E.61(2) (2006).

66. *See generally* KOSSEFF, *supra* note 16, at 46-47.

67. KESAN & HAYES, *supra* note 29, at 107; *see also* KOSSEFF, *supra* note 16, at 46.

68. *See generally* KOSSEFF, *supra* note 16, at 46 ("Although many of the state laws have similar provisions—indeed, some contain identical phrases and requirements—there are important differences."); *supra* notes 1-3 and accompanying text.

III. PROCEDURAL SAFEGUARDS AGAINST DATA BREACHES

There is currently no federal data breach notification legislation, nor is there "a comprehensive federal consumer data protection law that covers all varieties of private data," but there is existing federal legislation protecting certain types of data, such as financial and healthcare.[69] These statutory and regulatory schemes can serve as models in establishing uniformity amongst data breach statutes.

For many sectors, the Federal Trade Commission (FTC) regulates data security "under Section 5 of the FTC Act, which declares illegal 'unfair or deceptive acts or practices in or affecting commerce.'"[70] Under this Section, the FTC may bring a data security-related action against a company for their illegitimate business practices.[71] In addition to the FTC, entities that collect particularly sensitive personal information or deal with national security concerns may be subject to further cybersecurity regulatory measures.[72] Among the regulations and security standards for certain types of information, some notable policies include: the Gramm-Leach-Bliley Act (GLBA) Safeguards Rule that sets specific requirements for financial institutions; the Payment Card Industry Data Security Standard (PCI DSS) for entities that accept credit and debit card purchases to protect card data; and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule that provides requirements for health data.[73]

---

69. *See Consumer Data Privacy Laws*, BL, https://pro.bloomberglaw.com/insights/privacy/consumer-data-privacy-laws/#us-privacy-laws [https://perma.cc/VM32-3SUD] (last visited May 15, 2025); *see also supra* note 62 and accompanying text.

70. KOSSEFF, *supra* note 16, at 1-2 (citing 15 U.S.C. § 45(a)(1) (2006)) ("Many other agencies—including the Department of Health and Human Services, Education Department, and Federal Communications Commission—have jurisdiction to regulate privacy and data security for particular sectors.").

71. KOSSEFF, *supra* note 16, at 2-6. The FTC may bring an action under the *unfair* prong if the business practice goes against public policy, as established by three elements: "(1) 'the injury must be substantial,' (2) 'the injury must not be outweighed by any offsetting consumer or competitive benefits that the sales practice also produces,' and (3) 'the injury must be one which consumers could not reasonably have avoided.'" The FTC may bring an action under the *deception* prong if a business practice misrepresents, omits, misleads a consumer, acting reasonably given the circumstances, on a material fact. *Id.* at 3-5 (citing Fed. Trade Comm'n, FTC Policy Statement on Unfairness, *appended to* FTC v. International Harvester Co., 104 F.T.C. 949, 1070 (1984)).

72. *See id.* at 141.

73. *See generally id.* at 141-70; Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

A. PROPOSED COMPREHENSIVE FEDERAL LEGISLATION: THE AMERICAN PRIVACY RIGHTS ACT OF 2024

Washington Representative Cathy McMorris Rodgers introduced to Congress H.R. 8818, American Privacy Rights Act of 2024 (APRA), a bill seeking "[t]o provide Americans with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement, and for other purposes."[74] The APRA was introduced in the House of Representatives on June 25, 2024, and contemporaneously referred to the House Committee on Energy and Commerce, but has made little to no progress since its introduction.[75] Passage of APRA will not resolve data breach notification issues due to the carve out in the language of the Act.[76] If enacted, the APRA would specifically not preempt state law regarding, among other things, "[p]rovisions of laws, insofar as such provisions address notification requirements in the event of a data breach."[77] Despite the intent of the APRA to create a more uniform approach to data privacy, it does not preempt state laws on data breach and, thus, does not address a lack of uniformity in data breach notification requirements.[78] Accordingly, the current patchwork of more than fifty laws regarding data breach notification requirements would still be of concern.[79]

B. THE PREEMPTORY CHALLENGES WITH FEDERAL LEGISLATION REGARDING DATA BREACH NOTIFICATION

Attempts have been made in the past to create a uniform federal approach to data breach notification, all of which have been unsuccessful.[80] Among others, two noteworthy proposals demonstrate the preemptive challenges in identifying the proper scope of potential federal legislation.

---

74. American Privacy Rights Act of 2024, H.R. 8818, 118th Cong. (2024).

75. *See generally* H.R.8818 – American Privacy Rights Act of 2024, CONGRESS.GOV, https://www.congress.gov/bill/118th-congress/house-bill/8818/all-actions (last visited May 16, 2025).

76. *See generally* H.R. 8818.

77. *Id.* § 118(a)(3)(E).

78. *See generally id.* § 118(a)(3)(E); *supra* text accompanying notes 66-69.

79. Relatively new legislation has emerged across the country as states enact comprehensive data privacy laws in absence of a national standard. These laws provide broader consumer protections as to how data is collected, managed, and accessed. Among the states with enacted or pending comprehensive consumer privacy laws, Minnesota, Iowa, and Nebraska are the first three states of the Eighth Circuit to adopt such legislation. These and other states have taken the initiative to adopt a comprehensive data privacy law to uniformly protect consumer information at the state level. *See generally* Taetzsch, *supra* note 19, at 124-25, 132-33; *Which States Have Consumer Data Privacy Laws?* BL (Apr. 7, 2025), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/#map-of-state-privacy-laws [https://perma.cc/WY5T-JXRJ].

80. *See generally* Data Breach Notification Act, S. 139, 111th Cong. (2d Sess. 2010); Data Security and Breach Notification Act of 2015, S. 177 114th Cong. (1st Sess. 2015).

Proposed in 2010, the Data Breach Notification Act sought to set a national standard for notifying individuals affected by a data breach.[81] Under this proposed legislation, "[a]ny agency, or business entity engaged in interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the agency or business entity does not own or license . . . " would have been required to notify affected individuals if their personal information was, or was reasonably believed to have been, compromised.[82] Among other provisions, the Data Breach Notification Act would "supersede any other provision of Federal law or any provision of law of any State relating to notification by a business entity engaged in interstate commerce or an agency of a security breach . . . ."[83]

Similarly, the Data Security and Breach Notification Act of 2015 sought to require security practices and provide a nationalized breach standard.[84] However, the preemption of state laws was much broader than that of the 2010 legislation.[85] Pursuant to the Data Security and Breach Notification Act of 2015, this proposed legislation would have superseded, among other things, any state law that expressly "(A) requires information security practices and treatment of data containing personal information similar to any of those required under section 2; or (B) requires notification to individuals of a breach of security . . . ."[86] Regarding preemption, the language of the Data Breach Notification Act of 2010 would have broadly superseded both state law and federal laws regarding breach notification, and the Data Security and Breach Notification Act of 2015 would have superseded a wide-range of preexisting state legislation.[87] Striking the appropriate balance between federal oversight and state deference regarding data breach notification poses an additional challenge to establishing uniformity of data breach regulations.

IV. HOW NORTH DAKOTA SHOULD RESPOND UNTIL FEDERAL LEGISLATION ESTABLISHES UNIFORMITY IN BREACH NOTIFICATION REQUIREMENTS

Until the inconsistencies in data breach notification requirements can be resolved, North Dakota must be proactive about this problem. Because of the reasons above, the following courses of action should be taken to maximize

81. *See* S. 139.
82. *See id.* § 2(b)(1).
83. *Id.* § 10.
84. *See* S. 177.
85. *Compare id.* § 7(a)(1), *with* S. 139 § 10.
86. S. 177 § 7(a)(1).
87. *See generally* Data Breach Notification Act, S. 139, 111th Cong. (2d Sess. 2010); Data Security and Breach Notification Act of 2015, S. 177 114th Cong. (1st Sess. 2015).

protection of North Dakota residents' personal information. First and foremost, North Dakota practitioners must be diligent in their efforts of protecting personal information and understanding the variations of each states' breach notification statutes. Additionally, North Dakota's breach notification statute should be amended to expand upon the provisions in an effort to provide greater protection and transparency to its residents.

A. UNDERSTANDING ETHICAL AND LEGAL OBLIGATIONS TO PROTECT PERSONAL INFORMATION

Pursuant to the North Dakota Rules of Professional Conduct, a lawyer has an ethical obligation to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[88] For law firms in particular, data security is crucial due to the high volume of protected information entrusted to legal practitioners.[89] Law firms collect large amounts of sensitive information, "such as trade secrets, intellectual property, personally identifiable information (PII), and confidential attorney-client-privileged data" that make them a target for cyberattacks.[90] "To protect client information, attorneys increasingly have to take active steps to protect data, not just refrain from making disclosures."[91] Recommended steps to protect a law firm's data include implementing a data security policy, continued education for staff relating to data risk, utilizing password protection measures, encrypting sensitive information, securing communications, and proactively planning to respond to a data breach.[92]

Attorneys who represent businesses or individuals who collect sensitive information should also be conscious of data breach compliance concerns. Any company experiencing a data breach must act quickly and begin remediation in a timely fashion to prevent further harm and comply with breach notification requirements.[93] Legal practitioners should be notified immediately by their clients of a potential data breach or cyberthreat, and must not

88. N.D.R. Prof. Conduct. 1.6(d); *see also* Silverman, *supra* note 49.

89. *See generally* Clio, *Ensuring Security: Protecting Your Law Firm and Client Data*, ABA (May 9, 2024), https://www.americanbar.org/groups/law_practice/resources/law-technology-today/2024/ensuring-security-protecting-your-law-firm-and-client-data; John Simek, *2023 Cybersecurity TechReport*, ABA (Dec. 18, 2023), https://www.americanbar.org/content/aba-cms-dotorg/en/groups/law_practice/resources/tech-report/2023/2023-cybersecurity-techreport/.

90. Clio, *supra* note 89.

91. KESAN & HAYES, *supra* note 29, at 1.

92. *See* Clio, *supra* note 89.

93. *See Data Breach Response: A Guide For Business*, FED. TRADE COMM'N (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business [https://perma.cc/E3AR-NSVD]; Silverman, *supra* note 49.

delay in beginning remediation efforts.[94] Once an attorney is made aware of the concern, they should recommend "their organizations or clients to consider retaining a third-party digital forensics expert to verify the risk is contained and that it is safe to conduct business."[95] Even though a data breach is identified, it may not be fully resolved and the assistance of digital forensics can ensure there is no further risk of additional or continuing threats.[96] Once the threat is contained, notification should commence in a timely fashion to adhere to state-specific requirements.[97] A remediating attorney must identify in which states the affected individuals reside and should promptly look to those states' breach notification statutes to understand their legal obligations.[98]

For companies of all sizes, the FTC recommends good cybersecurity practices to protect against cyberattacks.[99] To protect documents and data, the FTC recommendations include updating software, securing files, requiring passwords, encrypting devices and data that contains personal information, and requiring multi-factor authentication.[100] Additionally, securing wireless network routers and utilizing network encryption can help ensure that data shared while connected to the network would be unusable to an outside party.[101]

B. AMENDMENTS TO NORTH DAKOTA'S BREACH NOTIFICATION STATUTE TO BRIDGE GAPS WITHIN THE EIGHTH CIRCUIT

In an effort to provide greater protections and transparency to North Dakota residents, the state's breach notification statute should be amended. The need for practitioners to conform with other states' breach notification laws is not exclusive to North Dakota—it applies to legal practitioners remediating a breach in every jurisdiction.[102] Therefore, expanding upon certain provisions of the North Dakota breach notification statute will afford the state's

94. *See* Silverman, *supra* note 49.

95. *See id.*

96. *See id.*

97. *See Data Breach Response: A Guide For Business*, FED. TRADE COMM'N (Feb. 2021), https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business [https://perma.cc/E3AR-NSVD].

98. *See* Taetzsch, *supra* note 19, at 130-31. *See generally* discussion *supra* Section I.C.

99. *See Cybersecurity for Small Business: Cybersecurity Basics*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/attachments/cybersecurity-basics/cybersecurity_sb_cyber-basics.pdf [https://perma.cc/U2ME-E49J] (last visited May 15, 2025) (citing the following agencies: Federal Trade Commission, National Institute of Standards and Technology, U.S. Small Business Administration, and Homeland Security.).

100. *See id.*

101. *See id.*

102. *See generally* discussion *supra* Section I.C.

residents with additional guarantees when their personal data is compromised, regardless of where the breach occurs.[103] Additionally, clarifications can be made to the current language of the North Dakota breach notification statute to ensure compliance requirements are clear to any legal practitioner needing to provide notice to a North Dakota resident.[104] Specifically looking to other Eighth Circuit states' breach notification statutes, the following proposed amendments would benefit North Dakotans while remaining consistent with requirements of other circuit states.[105]

Minnesota, Iowa, and South Dakota breach notification statutes define a breach to include encrypted data that has been compromised along with the encryption key, which makes the secured data readable or usable.[106] Following suit, North Dakota's definition of "[b]reach of the security system" should be amended to include an unauthorized acquisition of encrypted data and the encryption key.[107] Furthermore, similar to the Nebraska breach notification statute, North Dakota's "[b]reach of the security system" definition should be amended to clarify that acquisition of personal information pursuant to a court order or legitimate governmental purpose is not a breach.[108] Currently, the North Dakota definition limits a non-breach to the "good-faith acquisition of personal information by an employee or agent."[109] In sum, Section 51-30-01(1) of the North Dakota Century Code should read as follows:

> "Breach of the security system" means unauthorized acquisition of computerized data when access to personal information has not been secured by encryption or by any other method or technology that renders the electronic files, media, or databases unreadable or unusable**,** *or when access to personal information was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired through the breach of security*. Good-faith acquisition of personal information by an employee or agent *for a legitimate purpose* of the person is not a breach of the security system, if the personal information is not used or subject to

103. *See generally supra* text accompanying notes 14-15.

104. *See generally* discussion *supra* Section II.B.

105. Eighth Circuit states include Arkansas, Iowa, Minnesota, Nebraska, North Dakota, and South Dakota. *See generally* ARK. CODE ANN. § 4-110-103 (West 2019); IOWA CODE § 715C (2018); MINN. STAT. § 325E.61 (2006); NEB. REV. STAT. § 87-802 (2016); N.D. CENT. CODE § 51-30-01 (2015); S.D. CODIFIED LAWS § 22-40-19 (2018).

106. *See* MINN. STAT. § 325E.61(1)(e) (2006); IOWA CODE § 715C.1(11)(a) (2018); S.D. CODIFIED LAWS § 22-40-19(1) (2018).

107. *See generally* N.D. CENT. CODE § 51-30-01(1) (2015); S.D. CODIFIED LAWS § 22-40-19(1) (2018). *See also* discussion *supra* Section II.A.

108. *See generally* NEB. REV. STAT. § 87-802(1) (2016); N.D. CENT. CODE § 51-30-01(1) (2015).

109. *See* N.D. CENT. CODE § 51-30-01(1) (2015).

> further unauthorized disclosure. *Acquisition of personal information pursuant to a subpoena or order of a state agency is not a breach of the security system*.[110]

A similar amendment should be made to Section 51-30-01(4)(a) as follows:

> "Personal information" means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted *or are encrypted and the encryption key was also acquired*;[111]

Moreover, Arkansas, Iowa, Nebraska, and South Dakota breach notification statutes include as personal information a variation of biometric data.[112] North Dakota's definition of personal information should be expanded to include biometric data when compromised, in addition to the individual's first name or first initial and last name.[113] Thus, Section 51-30-01 should be amended to include the following proposed definition:

> *"Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voice print, retina or iris image, or any other unique biological characteristics of a person if the characteristics are used by the owner or licensee to uniquely authenticate the person's identity when the individual accesses a system or account.*[114]

Provided a definition of biometric data is added to Section 51-30-01 of the North Dakota Century Code as stated above, Section 51-30-01(4)(a) should be amended to include "Biometric data" as a data element.[115]

Further expanding upon the protected data elements, North Dakota should require notification of breach for unauthorized acquisition of data that is similar to South Dakota's "[p]rotected information."[116] Considering IBM's Cost of a Data Breach Report 2024 noted that forty-six percent of breaches involved acquisition of PII, which is defined to include email addresses, North Dakota's breach notification requirements should be amended to require notification to residents if such information is compromised.[117] Thus,

---

110. *See generally id.* (emphasis added for proposed amendments).

111. *See generally id.* § 51-30-01(4)(a) (emphasis added for proposed amendments).

112. *See generally* ARK. CODE ANN. § 4-110-103(7)(E) (West 2019); IOWA CODE § 715C.1(11)(a)(5) (2018); NEB. REV. STAT. § 87-802(5)(a)(v) (2016); S.D. CODIFIED LAWS § 22-40-19(4)(e) (2018). *See also supra* text accompanying notes 59-60.

113. *See generally* ARK. CODE ANN. § 4-110-103(7)(E) (West 2019).

114. *See generally* N.D. CENT. CODE § 51-30-01 (2015) (emphasis added for proposed amendments).

115. *See generally id.* § 51-30-01(4)(a).

116. *See generally* S.D. CODIFIED LAWS § 22-40-19(5) (2018).

117. *See generally* IBM, *supra* note 4, at 6, 12.

Section 51-30-01 should be amended to include the following proposed definition:

> *"Protected information" means a username or email address, in combination with a password, security question answer, or other information that permits access to an online account.*[118]

V. CONCLUSION

Moving forward, data security will always be a concern to legal practitioners.[119] Attorneys have a legal and ethical obligation to prevent disclosure of or unauthorized access to client information, and understanding the intricacies of data breach compliance is at the forefront of this responsibility.[120] In the absence of federal uniformity on responding to data breaches, coupled with increased cyberthreats and usage of digital storage, North Dakota practitioners must be cognizant of how data breach compliance varies across state lines and what can be done until federal legislation resolves this problem.[121] Although all fifty states, the District of Columbia, Puerto Rico, Guam, and the Virgin Islands have laws on data breach notification requirements, provisions vary amongst jurisdictions, which could put a legal practitioner in a challenging situation when remediating a breach.[122] Without a uniform federal standard on breach notification, North Dakota's statute should be amended to align with its circuit states and afford greater protections to North Dakota's residents. Due to technological advances and the potential for incoming data centers to North Dakota, being proactive about data security and data breach compliance is crucial for the North Dakota attorney—now more than ever.

Taylor House[*]

118. *See generally* N.D. CENT. CODE § 51-30-01 (2015) (emphasis added for proposed amendments).

119. *See* KESAN & HAYES, *supra* note 29, at 2.

120. *See* N.D.R. Prof. Conduct. 1.6(d); *see also* Silverman, *supra* note 49.

121. *See generally* discussion *supra* Sections I & IV.

122. *See generally* discussion *supra* Section II.B.

[*] 2026 J.D./M.B.A. Candidate at the University of North Dakota School of Law. Thank you to the NORTH DAKOTA LAW REVIEW for their efforts and support in preparing this piece for publication. I would also like to thank my friends and family, especially my parents, for their endless love and encouragement. Additionally, I extend my heartfelt appreciation to Professor Blake Klinkner for his guidance and mentorship throughout my law school journey.