

# **Exploring Notification Readability: Understanding Customer Inaction in Response to Data Breaches**

**Early stage paper**

**Meng 'Leah' Li**  
Mississippi State University  
ML1850@msstate.edu

**Merrill Warkentin**  
Mississippi State University  
mw156@msstate.edu

## **ABSTRACT**

A data breach notification letter is crucial for informing affected parties about the incident, the potential risks involved, and the measures the organization is implementing to minimize the impact. This necessity arises from the legal requirements set forth by data breach notification laws across all 50 states in the United States. Our study suggests that notifications with low readability may inadvertently cause users to underestimate the negative effects of data breach incidents. This research aims to understand customer inaction following the receipt of data breach notification letters. Specifically, we explore how the readability of these letters and normalcy bias influence customers' protection motivation intention, considering the mediating role of perceived risk, through the lens of Impression Management Theory. Our insights are intended to benefit managers and lawmakers striving to safeguard users' information.

## ***Keywords***

Data breach notification, readability, normalcy bias, perceived risk, impression management theory

## **INTRODUCTION**

Data breaches pose a substantial risk of identity theft to those affected (Verizon, 2022). From January to June 2024, exclusively within the United States, there have been 658 publicly disclosed

incidents leading to the compromise of 700 million known records across sectors such as finance, telecommunications, healthcare, and professional services (IT Governance USA, 2024). To address the severe consequences of such breaches, numerous countries have enacted data breach notification laws mandating companies to inform impacted consumers based on the United Nations Office on Drugs and Crime (2020). In the United States, all 50 states have enacted breach notification laws mandating the notification of state residents in the event of a security breach involving highly sensitive information, such as Social Security numbers<sup>1</sup> and credit card details. Prior to regulation, some companies opted not to inform their customers, leaving them unprotected. Though subsequent regulations have reduced the risk exposure, can we truly rest without any anxiety?

Since these laws have been enacted, companies face a post-breach dilemma: they must notify customers while also minimizing negative consequences such as brand damage and loss of trust (Buckman *et al.*, 2019). Thus, companies may adopt response strategies to downplay the seriousness of the accidents (Nikkhah and Grover, 2022). The purpose of these reputation management strategies is to protect market value and ensure customers loyalty and trust (Gwebu *et al.*, 2018), rather than actively guide users in taking protective actions. However, this risk reduction strategy contrasts with encouraging customers to take action that minimizes their risk; there is a natural tension between the goals of the company and their customers. To illustrate, consider a serious statement in the data breach notification letter, such as “You may suffer significant financial loss if you don’t take the following actions.” This might increase customers’

---

<sup>1</sup> A Social Security number (SSN) is a nine-digit number issued by the Social Security Administration (SSA) to U.S. citizens, permanent residents, and eligible nonimmigrant workers.

anxiety, prompting them to change their passwords or monitor their bank activities and credit scores. But this can also amplify customers' feelings of dissatisfaction and harm companies' perceived legitimacy. Conversely, if such a serious statement is excluded from the notification message, negative reputational consequences may be reduced, but customers may not grasp the severity of incidents and thus may not adopt an appropriate set of actions.

In the context of these contrasting motivations, the *readability* of the notification plays a key role in achieving the final goals, allowing the affected consumers to take preventative measures to safeguard their financial accounts and deter identity theft. Readability includes the rhetorical choice of wording (Johnston *et al.*, 2023), the framing of the message, the clarity of language, conciseness, and comprehensibility. It refers to the ease and effectiveness with which a message can be understood relative to its writing style (Jackson, 2019). Each state law comprises a unique set of notification requirements, and much discretion is left to the breached company regarding the elements, readability, and format. Table A1 (Appendix) summarizes the data breach notification laws across all 50 states. These laws vary, but all highlight key aspects such as notification timing, authority notification, mass notification thresholds, and penalties. However, none of these laws mandate the inclusion of details about the severity of data breach incidents or required customer actions. This lack of specificity leaves room for companies to potentially lower the readability of the notifications, either intentionally or unintentionally.

To effectively encourage individuals to protect themselves, data breach notification letters and emails must be clear, concise, and easily understandable, ensuring that all customers comprehend not only what happened but also the necessary actions they should take. However, the readability of data breach notifications has been found to be problematic (Zou *et al.*, 2018). Message readability has been widely addressed in privacy policy statement research (e.g., Bailey

et al., 2021; Pownell et al., 2020; Wagner, 2022). It has been found that these policies are often poorly drafted, excessively long, and difficult for users to understand. In some cases, data breach notifications also have poor readability. For example, research indicates that the text in these letters typically demands reading abilities at a 10th-grade level, exceeding the recommended level for materials aimed at the general public (typically seven to nine-grade levels) (Zou and Schaub, 2019). This challenge in comprehension often arises from wordiness, the inclusion of technical jargon, vague statements, and an overload of information. Jackson (2019) proposed three possible explanations for the complexity of notifications that are bad writing, information assumption, and impression management. It has been noted that business managers may employ techniques, such as impression management, to conceal negative information related to severe data breaches. This is achieved by manipulating the structure and language of data breach notification letters, rendering the message complex and difficult for recipients to grasp (Jackson, Vanteeva and Fearon, 2019). For example, the use of hedge terms like “maybe” or “likely” in data breach notification obscures the true impact of the breach. Moreover, some companies qualify the 'no evidence' assertion, as seen in the statement: "At this time, we have no evidence that your personal information has been or is likely to be misused" (Pershing, LLC). These strategies not only create uncertainty but also diminish customers' perceived risk, leading them to underestimate the seriousness of the situation and fail to take protective measures even after receiving a data breach notification. Thus, we argued that this lack of action can be attributed to shortcomings (e.g., readability) in the notifications themselves, contributing to customer uncertainty and confusion.

Indeed, a minority of consumers take significant measures to safeguard their privacy and identities following receipt of a data breach notification based on a report by the Identity Theft Resource Center and research firm DIG.Works (Mello, 2021). The research claimed that more

than half perceived the risk of data breach as none or very little (Mayer *et al.*, 2023). Prior research also showed that customers rarely take recommended protective measures even though they are aware of the breach (Zou *et al.*, 2018). Many studies have delved into the effective strategies of data breach notification to maintain customer loyalty and trust (e.g., Guo *et al.*, 2024; Gwebu *et al.*, 2018; Masuch *et al.*, 2021). However, very few studies have explored the customer behaviors or behavioral intentions in response to such notification letters. We contend that investigating how notification letters influence customers' behavioral intentions is of paramount importance since the main goal of these letters is (or should be) to serve as warning signals, prompting customers to take proactive measures to safeguard themselves and reduce the likelihood of future data breaches.

Individual consumers often make choices based on nonrational thinking. Though various prominent theories, such as Deterrence Theory (DT) (Beccaria, 1963) and Protection Motivation Theory (PMT) (Rogers, 1975) assume individuals are logical and rational, reality often sees individuals making decisions based on habits, nonrational cognitive processes, and numerous sources of bias. Our study delved into how varying levels (low vs. high) of readability in data breach notification letters influence an individual's protection motivation intention. We also explored the impact of cognitive bias on outcomes. These objectives align closely with the principles of behavioral economics theory, an area that has extensively investigated these phenomena. We believe that normalcy bias plays a pivotal role in shaping customer responses in our context. Normalcy bias is a cognitive bias that causes individuals to underestimate the severity of a threat and the need for immediate action. It can cause people to underestimate the potential impact of a data breach on their lives; they tend to believe that things will continue as usual even when security warning signs are present. This bias is particularly concerning as it hampers individuals' ability to prepare adequately and respond effectively to potential risks. For example,

normalcy bias can lead individuals to believe that life will continue as usual, even in the face of health warnings, such as irregular dizziness. This bias may cause them to delay seeking medical help until their condition becomes severe and significantly impacts their daily lives. Similarly, in the realm of Information Security (IS), people exhibit this bias by disregarding device security warnings until they experience significant data breaches or financial losses.

We currently lack an understanding of (1) how data breach notification readability influences customers' protection motivation intention; (2) how customers' perceived risk influences the relationship between data breach notification quality and customers' protection motivation intention; and (3) how the normalcy bias influences the relationship between customers' perceived risk and their protection motivation intention. The understanding of the decision-making process of customers on data breaches after receiving a notification remains a notable gap. We utilized the Impression Management Theory as the theoretical framework to underpin our exploration of the relationship. Figure 1 is the research model.

Our study makes three significant contributions to the existing literature. First, we enrich the theoretical discourse by establishing a connection between the readability of notification letters and customers' intention to protect themselves. This adds depth to our understanding of how communication clarity influences individuals' motivation to safeguard their information. Second, our research contributes to the ongoing discussion regarding the impact of notification readability on customers' intentions. By examining how the ease of understanding in these communications affects individuals' likelihood to take protective actions, we shed light on a crucial aspect of information security communication strategies. Last, we delve into the exploration of normalcy bias within the realm of information security. Investigating how individuals with varying levels of normalcy bias respond to data breach notifications provides valuable insights into the

psychological factors influencing their perception of threats and subsequent protective behaviors. This contributes to a more comprehensive understanding of human behavior in the face of cybersecurity risks.

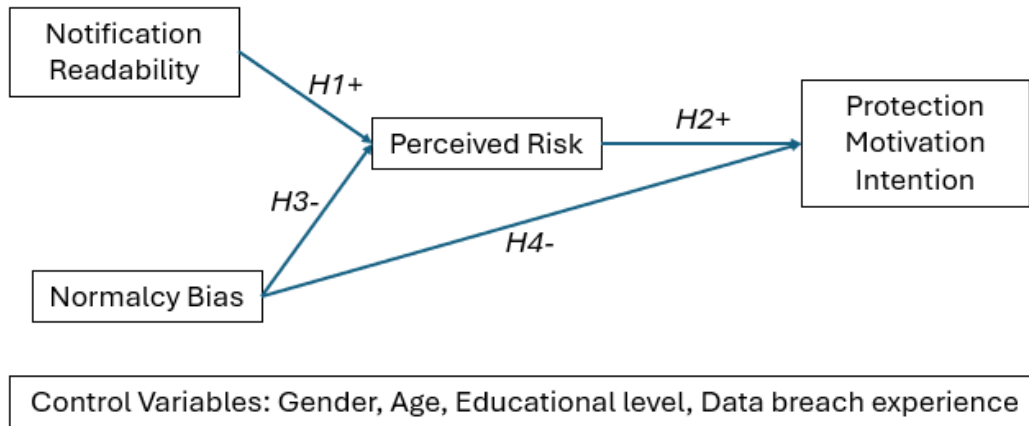


Figure 1 Research Model

## THEORETICAL BACKGROUND & HYPOTHESES DEVELOPMENT

The heading of a section should be Times New Roman 14-point bold, all caps, left justified (Heading 1 Style in this template file).

### Impression Management Theory

Impression management, also termed as self-presentation, involves the deliberate or subconscious efforts of individuals, using both verbal and non-verbal cues, to influence how others perceive them, a situation, or an object (Jackson et al., 2019). It's not uncommon for organizations to also adopt this approach. Research has demonstrated that companies often have lower readability in their annual reports when disclosing "bad news" (Courtis, 1998) than when reporting good news. In this study's context, organizations may use verbal cues in the data breach notification letter and lower the readability of the letters in order to mitigate the potential negative publicity when a data

breach happens (Jenkins et al., 2014). On the one hand, risk communication presents a challenge for companies as they don't want to exaggerate risks and harm customers' business interests (Zou & Schaub, 2019). They may downplay the severity of the breach and obscure critical information through poor readability of notifications, leading readers to underestimate the associated risks. When individuals struggle to grasp the implications due to poor communication, their perception of risk diminishes. The low probability of negative effect words such as "may be involved" or "unlikely to be affected" sugarcoat the severity of the breach. On the other hand, companies are motivated to maintain customer loyalty and trust. They avoid guiding customers or pressuring them into taking protective actions. This approach can backfire by giving customers the impression that no action is necessary on their part. This unintended message can undermine the urgency of addressing the breach's potential consequences. Thus, we have the following.

*H1: Data breach notification letter's readability is positively related to customers' perceived risk.*

Perceived risk refers to an individual's subjective assessment or evaluation of the potential negative consequences or uncertainties. In this study, we don't distinguish the difference between perceived risk and threat. Thus, the relationship between perceived risk and protection motivation intention is aligned with Protection Motivation Theory (PMT) in that the increase of threat appraisal increases protection motivation (Boss et al., 2015; Johnston & Warkentin, 2010). When individuals perceive the risk of an event as low, they often lack the motivation to take proactive measures to protect themselves. Research has demonstrated that risk communication has both direct and indirect effects on protective behaviors during the COVID-19 outbreak, primarily mediated by changes in risk perception (Heydari et al., 2021). Therefore, the hypothesis is developed as follows.

*H2: Customers' perceived risk is positively related to customers' protection motivation intention.*



There is a lack of research regarding normalcy bias, particularly concerning its impact on individuals' responses to data breach notification letters. It stands to reason that individuals with a high normalcy bias tend to normalize threats, leading to a diminished level of concern and lower intentions to take protective measures. In the context of data breach notification letters, individuals with a high normalcy bias may perceive the breach as a routine occurrence or downplay its significance, believing that such events are part of modern digital life. Consequently, they may not feel a strong sense of urgency or concern, leading to a reduced intention to take proactive steps to protect their personal information or digital assets. Thus, we have the following hypothesis.

*H3: Normalcy bias is negatively related to customers' perceived risk.*

*H4: Normalcy bias is negatively related to customers' protection motivation intention.*

## **METHODOLOGY**

### **Participants and Procedures**

To investigate our hypotheses, we will conduct a survey targeting users residing in the United States via the Prolific survey platform. The construct development for normalcy bias following MacKenzie et al. (2011), since there is no existing scale. Each item is rated on a seven-point fully-anchored agreement scale (where 1 = strongly disagree, 7 = strongly agree). To ensure the scales' reliability and validity, we will first conduct an expert panel review and a pilot study.

Prior to data collection, this study will receive approval from the Institutional Review Board (IRB) at our academic institution. Qualified participants must meet the following criteria: be residents of the United States, have a prior approval rate on Prolific of at least 99%, and have submitted over fifty previous entries on the platform. These criteria are established as best practices in data collection to ensure the integrity and quality of the data collected (Nehme et al., 2024). Moreover,

in adherence to established research norms, all participants will be required to be of legal adult age, set at a minimum of 18 years old. These measures are enacted to maintain the rigor and reliability of our study's findings.

Prior to engaging with the survey questions, participants will be presented with a consent form, to which they assent if they choose to participate. Subsequently, participants will be provided with clear definitions of the context-specific terms pertinent to this study. We will employ covariance-based structural equation modeling (CB-SEM) to examine our research model. Initially, we will validate our measurement model through confirmatory factor analysis (CFA) and assess all constructs' reliability, convergent validity, and discriminant validity. Then, we estimate our structural model. Also, the common method bias will be assessed.

## **CONTRIBUTION**

First, this paper theoretically and empirically explores the relationship between the readability of notification letters and customers' intention to protect themselves. This adds depth to our understanding of how communication clarity influences individuals' motivation to safeguard their information. Second, this research can practically contribute by suggesting that lawmakers consider incorporating mandatory elements, such as outlining potential consequences, into the law. Last but not least, the practical contribution of this research suggests that companies should pay close attention to the balance of their data breach notifications. When customers are empowered to actively protect their information, it not only benefits them by enhancing their security but also contributes to improving the overall security posture of the company.

## **LIMITATION**

Common method bias poses a significant limitation in our project due to the concurrent collection of data using the same method at the same time. This bias can distort the relationships between variables by inflating correlations and making unrelated factors appear more strongly related than they are. It can also obscure the true causality between variables and reduce the ability to distinguish between different constructs, impacting the validity and interpretability of our findings. Although we utilized marker variable techniques in the survey and the inclusion of a latent common method factor to control common method bias.

## **CONCLUSION**

Our research underscores the critical importance of readability in data breach notification letters and its impact on customers' protection motivation intention. By examining the relationships between readability, normalcy bias, and protection motivation intention through the lens of Impression Management Theory, we provide valuable insights for both academic and practical applications. We expect that clearer, more comprehensible notifications can significantly enhance individuals' motivation to protect their information, thus mitigating the adverse effects of data breaches. This study advocates for legislative measures mandating explicit communication of potential consequences in data breach notifications and emphasizes the need for companies to craft balanced and effective communications. Ultimately, empowering customers to take protective actions not only enhances their personal security but also strengthens the overall security framework of organizations.

## REFERENCES

- Bailey, R. *et al.* (2021) ‘Disclosures in privacy policies: Does" notice and consent" work?’, *Loy. Consumer L. Rev.*, 33, p. 1.
- Beccaria, C. (1963) *On crimes and punishments*. New York, NY: Transaction Publishers.
- Buckman, J. *et al.* (2019) ‘Fool me twice? data breach reductions through stricter sanctions’, *Data Breach Reductions Through Stricter Sanctions (July 19, 2019)* [Preprint]. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3258599](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3258599).
- Guo, Y., Wang, C. and Chen, X. (2024) ‘Functional or financial remedies? The effectiveness of recovery strategies after a data breach’, *Journal of Enterprise Information Management*, 37(1), pp. 148–169.
- Gwebu, Kholekile L., Wang, J. and Wang, L. (2018) ‘The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management’, *Journal of Management Information Systems*, 35(2), pp. 683–714. Available at: <https://doi.org/10.1080/07421222.2018.1451962>.
- Gwebu, Kholekile L., Wang, J. and Wang, L. (2018) ‘The role of corporate reputation and crisis response strategies in data breach management’, *Journal of Management Information Systems*, 35(2), pp. 683–714.
- IT Governance USA (2024) *Data Breaches and Cyber Attacks in 2024 in the USA*. Available at: <https://www.itgovernanceusa.com/blog/data-breaches-and-cyber-attacks-in-2024-in-the-usa>.
- Jackson, S. (2019a) ‘How readable are data breach notifications?’, *Computer Fraud & Security*, 2019(5), pp. 6–8. Available at: [https://doi.org/10.1016/S1361-3723\(19\)30051-X](https://doi.org/10.1016/S1361-3723(19)30051-X).
- Jackson, S. (2019b) ‘How readable are data breach notifications?’, *Computer Fraud & Security*, 2019(5), pp. 6–8. Available at: [https://doi.org/10.1016/S1361-3723\(19\)30051-X](https://doi.org/10.1016/S1361-3723(19)30051-X).
- Jackson, S., Vanteeva, N. and Fearon, C. (2019) ‘An investigation of the impact of data breach severity on the readability of mandatory data breach notification letters: Evidence from US firms’, *Journal of the Association for Information Science and Technology*, 70(11), pp. 1277–1289.
- Johnston, A. *et al.* (2023) ‘Seeking rhetorical validity in fear appeal research: An application of rhetorical theory’, *Computers & Security*, 125, p. 103020.
- Masuch, K., Greve, M. and Trang, S. (2021) ‘What to do after a data breach? Examining apology and compensation as response strategies for health service providers’, *Electronic Markets*, 31, pp. 829–848.
- Mayer, P. *et al.* (2023) ‘Awareness, Intention, (In)Action: Individuals’ Reactions to Data Breaches’, *ACM Transactions on Computer-Human Interaction*, 30(5), pp. 1–53. Available at: <https://doi.org/10.1145/3589958>.
- Mello, J. (2021) *Many Consumers Fail To Protect Privacy After Receiving Data Breach Notice*. Available at: <https://www.technewsworld.com/story/many-consumers-fail-to-protect-privacy-after-receiving-data-breach-notice-87346.html>.
- Nikkhah, H.R. and Grover, V. (2022) ‘An empirical investigation of company response to data breaches’, *MIS Quarterly*, 46(4), pp. 2163–2196.
- Pownell, J.M. *et al.* (2020) ‘Using readability to explore data privacy statements within mobile health applications’, *CIN: Computers, Informatics, Nursing*, 38(5), pp. 217–223.
- Rogers, R.W. (1975) ‘A Protection Motivation Theory of Fear Appeals and Attitude Change’.
- United Nations Office on Drugs and Crime (2020) ‘Data breach notification laws’. Available at: <https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/data-breach-notification-laws.html>.

- Verizon (2022) *Data Breach Investigations Report*. Available at: <https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf>.
- Wagner, I. (2022) ‘Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996–2021’, *arXiv preprint arXiv:2201.08739* [Preprint].
- Zou, Y. *et al.* (2018a) “‘I’ve Got Nothing to Lose’: Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach’.
- Zou, Y. *et al.* (2018b) “‘I’ve Got Nothing to Lose’: Consumers’ Risk Perceptions and Protective Actions after the Equifax Data Breach’.
- Zou, Y. and Schaub, F. (2019) ‘Beyond Mandatory: Making Data Breach Notifications Useful for Consumers’, *IEEE Security & Privacy*, 17(2), pp. 67–72. Available at: <https://doi.org/10.1109/MSEC.2019.2897834>.

## APPENDIX

Table A1 Summary of the 50 State Data Breach Notification Laws by State

State	Year Enacted	Trigger for Notification	Notification Timing	Authority Notification	Threshold for Mass Notification	Penalties for Non-Compliance
Alabama	2018	Unauthorized access of unencrypted personal info	Without unreasonable delay	Attorney General if > 1,000 affected	> 1,000 individuals	Up to \$500,000 per breach
Alaska	2009	Unauthorized acquisition of unencrypted personal info	Without unreasonable delay	Attorney General	> 1,000 individuals	\$500 per individual up to \$50,000
Arizona	2006	Unauthorized acquisition causing material compromise	Most expedient time possible	Attorney General	> 1,000 individuals	Up to \$500,000 per breach
Arkansas	2005	Unauthorized access to personal info	Most expedient time possible	Attorney General	> 1,000 individuals	Up to \$150,000 per breach
California	2003	Unauthorized access of personal info	Most expedient time possible	Attorney General if > 500 affected	> 500 individuals	Up to \$3,000 per individual
Colorado	2006	Unauthorized acquisition causing harm	Most expedient time possible	Attorney General	> 500 individuals	\$500 per individual up to \$50,000
Connecticut	2005	Unauthorized access of personal info	Most expedient time possible	Attorney General	> 1,000 individuals	Up to \$500,000 per breach
Delaware	2005	Unauthorized acquisition causing harm	Most expedient time possible	Attorney General	> 500 individuals	Up to \$500,000 per breach
Florida	2006	Unauthorized access of personal info	Without unreasonable delay	Attorney General	> 500 individuals	Up to \$500,000 per breach

Georgia	2007	Unauthorized access of personal info	Without unreasonable delay	Attorney General	> 1,000 individuals	Up to \$500,000 per breach
Hawaii	2006	Unauthorized access of personal info	Most expedient time possible	Attorney General	> 1,000 individuals	Up to \$500,000 per breach
Idaho	2006	Unauthorized acquisition of personal info	Most expedient time possible	Attorney General within 24 hours	> 1,000 individuals	Up to \$25,000 per breach
Illinois	2005	Unauthorized acquisition of personal info	Most expedient time possible	General Assembly report for state agencies	> 1,000 individuals	None specified
Indiana	2005	Unauthorized acquisition of personal info	Without unreasonable delay	Attorney General	> 1,000 individuals	Up to \$150,000 per violation
Iowa	2008	Unauthorized acquisition of personal info	Most expeditious manner possible	Consumer Protection Division if > 500 affected	> 1,000 individuals	None specified
Kansas	2006	Unauthorized acquisition of personal info	Without unreasonable delay	None specified	> 1,000 individuals	None specified
Kentucky	2014	Unauthorized acquisition of personal info	Without unreasonable delay	None specified	> 1,000 individuals	None specified
Louisiana	2005	Unauthorized acquisition of personal info	Without unreasonable delay, no later than 60 days	Consumer Protection Section of Attorney General's Office	> 1,000 individuals	Up to \$5,000 per day; civil actions for actual damages
Maine	2005	Unauthorized acquisition of personal info	Without unreasonable delay	Attorney General	> 1,000 individuals	\$500 per violation, up to \$2,500 per day

Maryland	2007	Unauthorized acquisition of personal info if misuse likely	As soon as reasonably practicable, no later than 45 days	Attorney General	> 1,000 individuals	None specified
Massachusetts	2007	Unauthorized acquisition creating substantial risk of ID fraud/theft	Without unreasonable delay	Attorney General and Director of Consumer Affairs and Business Regulation	> 1,000 individuals	None specified
Michigan	2006	Unauthorized acquisition	Without unreasonable delay	No	Yes (if > 1,000 individuals)	Up to a maximum fine of \$750,000 per breach
Minnesota	2005	Unauthorized acquisition	Without unreasonable delay	No	Yes (if > 500 individuals)	None specified
Mississippi	2010	Unauthorized acquisition	Without unreasonable delay	No	No	None specified
Missouri	2009	Unauthorized acquisition	Without unreasonable delay	Attorney General	Yes (if > 1,000 individuals)	None specified
Montana	2006	Unauthorized acquisition	Without unreasonable delay	Attorney General	No	None specified
Nebraska	2006	Unauthorized acquisition	Without unreasonable delay	No	No	None specified
Nevada	2005	Unauthorized acquisition	Without unreasonable delay	No	Yes (if > 1,000 individuals)	None specified



New Hampshire	2006	Unauthorized acquisition	As soon as possible	Attorney General	Yes (if > 1,000 individuals)	None specified
New Jersey	2005	Unauthorized access	Without unreasonable delay	Division of State Police	Yes (if > 1,000 individuals)	None specified
New Mexico	2017	Unauthorized acquisition	No later than 45 days	Attorney General	Yes (if > 1,000 individuals)	None specified
New York	2005	Unauthorized acquisition	Without unreasonable delay	Multiple agencies	Yes (if > 5,000 individuals)	None specified
North Carolina	2005	Unauthorized acquisition	Without unreasonable delay	Attorney General	Yes (if > 1,000 individuals)	None specified
North Dakota	2005	Unauthorized acquisition	Without unreasonable delay	Attorney General	Yes (if > 250 individuals)	None specified
Ohio	2005	Unauthorized acquisition	No later than 45 days	No	Yes (if > 1,000 individuals)	None specified
Oklahoma	2008	Notify affected individuals of breaches involving unencrypted /unredacted personal information likely causing risk.	Without unreasonable delay	Notification may be delayed for law enforcement	No	Up to \$150,000 per breach
Oregon	2007	Notify affected individuals of unauthorized acquisition of unencrypted /unredacted personal information.	No later than 45 days after discovery	Notify Attorney General if >250 individuals	Notify consumer reporting agencies if >1,000 individuals	Compliant with GLBA/federal regulations deemed compliant

Pennsylvania	2006	Notify affected individuals of unauthorized acquisition of unencrypted/unredacted personal information.	Without unreasonable delay	Notification may be delayed for law enforcement	Notify consumer reporting agencies if >1,000 individuals	Compliant with Federal Interagency Guidance deemed compliant
Rhode Island	2006	Notify residents of unauthorized access to unencrypted personal information posing risk of identity theft.	No later than 45 days after confirmation of breach	Notification may be delayed for law enforcement	Notify Attorney General and credit reporting agencies if >500 residents	Compliant with GLBA/HIPAA/federal regulations deemed compliant
South Carolina	2008	Notify residents of unauthorized access to unencrypted/unredacted personal information with risk of harm.	Without unreasonable delay	Notification may be delayed for law enforcement	Notify Consumer Protection Division and consumer reporting agencies if >1,000 individuals	Up to \$1,000 per affected resident
South Dakota	2018	Notify affected individuals of unauthorized acquisition of unencrypted personal information.	Within 60 days of discovery	Notification may be delayed for law enforcement	Notify Attorney General if >250 individuals	Up to \$10,000 per day, per violation
Tennessee	2005	Notify residents of unauthorized acquisition of unencrypted personal information.	No later than 45 days from discovery	Notification may be delayed for law enforcement	Notify consumer reporting agencies if >1,000 individuals	Compliant with GLBA deemed compliant
Texas	2007	Unauthorized acquisition of personal info	As quickly as possible	No	10,000 individuals	\$2,000-\$50,000 per violation

Utah	2006	Unauthorized acquisition of personal info	Without unreasonable delay	No	No specific threshold	Up to \$100,000 aggregate
Vermont	2006	Unauthorized acquisition of personal info	Without unreasonable delay	Within 14 days	1,000 individuals	Not specified
Virginia	2008	Unauthorized acquisition of personal info	Without unreasonable delay	Yes	1,000 individuals	Up to \$150,000 per breach
Washington	2005	Unauthorized acquisition of personal info	No later than 45 days	Yes	500 individuals	Not specified
West Virginia	2008	Unauthorized access/acquisition of info	Without unreasonable delay	No	1,000 individuals	Not specified
Wisconsin	2006	Unauthorized acquisition of personal info	No later than 45 days	No	1,000 individuals	Not specified
Wyoming	2007	Unauthorized acquisition likely to cause harm	Without unreasonable delay	No	No specific threshold	Not specified