
# From Blame to Accountability: Evaluating Responsibility-Taking Language and Class-Action Lawsuits in Data Breach Crises through Stakeholder Theory

Maximilian Antonio Braun

Dissertation written under the supervision of professor Ekin Ilseven

Dissertation submitted in partial fulfilment of requirements for the MSc in Management with Specialization in Strategy, Entrepreneurship and Impact, at the Universidade Católica Portuguesa, 05.01.2025.

**Abstract (English)**

Organizations today operate in a landscape of heightened stakeholder scrutiny and regulatory complexity. Crises compel organizations to demonstrate accountability, with responsibility-taking narratives playing a critical role in rebuilding trust. This thesis investigates how evolving regulatory frameworks, such as the California Consumer Privacy Act (CCPA), shape organizational responsibility narratives and influence stakeholder-imposed punitive actions, thereby offering empirical evidence for how organizations depend on their consumers. Leveraging an empirical quantitative analysis, this study analyzes pre- and post-CCPA data breach notifications from the California Attorney General's database and class-action lawsuit records from ClassAction.org. Linguistic analysis quantifies responsibility-taking and deflective language in breach notifications, while a Difference in Differences methodology evaluates regulatory impact. The relationship between crisis severity and class-action lawsuits is examined through matched data from the two databases, exploring the interplay of narratives and legal outcomes. Results show a significant increase in responsibility-taking language and a decrease in deflective communication post-CCPA. However, breaches involving highly sensitive data reduced responsibility-taking narratives, highlighting the moderating role of severity. Despite these shifts, no consistent evidence was found that responsibility-taking alone reduced the likelihood of lawsuits or that severity had a clear moderating role. This study reveals how regulatory frameworks influence corporate crisis communication, shaping responsibility-taking narratives. While these narratives support trust rebuilding and mitigate reputational damage, their effectiveness in reducing punitive actions remains inconsistent. The findings emphasize the need for organizations to adopt context-specific strategies, integrating narrative adjustments with comprehensive crisis management to meet stakeholder expectations and address legal risks effectively.

**KEYWORDS:** responsibility narrative - crisis communication - stakeholder trust - CCPA - data breach

**TITLE:** From Blame to Accountability: Evaluating Responsibility-Taking Language and Class-Action Lawsuits in Data Breach Crises through Stakeholder Theory

**AUTHOR:** Maximilian Antonio Braun

**Abstract (Portuguese)**

As organizações atuais operam num cenário de maior escrutínio por parte das partes interessadas e de crescente complexidade regulatória. Crises obrigam as organizações a demonstrar responsabilidade, com narrativas de assunção de responsabilidades desempenhando um papel crucial na reconstrução da confiança. Esta tese investiga como estruturas regulatórias em evolução, como o California Consumer Privacy Act (CCPA), moldam narrativas de responsabilidade organizacional e influenciam ações punitivas impostas por stakeholders. Utilizando uma abordagem de métodos mistos, o estudo analisa notificações de violações de dados pré- e pós-CCPA no banco de dados do Procurador-Geral da Califórnia e registos de processos coletivos do ClassAction.org. Uma análise linguística quantifica a linguagem de assunção de responsabilidade e de defesa nas notificações, enquanto uma metodologia de Diferença-em-Diferenças avalia o impacto regulatório. A relação entre a gravidade das crises e os processos coletivos é examinada através de dados combinados das duas fontes, explorando a interação entre narrativas e resultados legais. Os resultados mostram um aumento significativo na linguagem de assunção de responsabilidade e uma redução na comunicação defensiva após o CCPA. No entanto, violações envolvendo dados altamente sensíveis diminuíram as narrativas de responsabilidade, destacando o papel moderador da gravidade. Apesar dessas mudanças, não foram encontradas evidências consistentes de que a assunção de responsabilidade reduza a probabilidade de ações judiciais ou que a gravidade desempenhe um papel moderador claro. Este estudo destaca como os quadros regulatórios moldam a comunicação em crises, realçando a necessidade de estratégias contextuais que integrem ajustes narrativos e gestão de crises eficaz.

**PALAVRAS-CHAVES:** narrativa da responsabilidade - comunicação de crise - confiança das partes interessadas - CCPA - violação de dados

**TÍTULO:** Da culpa à responsabilização: Avaliar a linguagem de assunção de responsabilidades e as acções judiciais colectivas em crises de violação de dados através da teoria das partes interessadas

**AUTOR:** Maximilian Antonio Braun

**Acknowledgments**

With the completion of this thesis, not only do my studies at Católica Lisbon School of Business & Economics come to a close, but so does my entire educational journey. I am deeply grateful to everyone who supported me along this extensive and winding path, those who were there from the very beginning and those who joined along the way, always ready to lend a hand when needed. My heartfelt thanks especially go to my parents, whose unwavering support made this academic journey possible. None of my achievements over the past five years would have been possible without you.

I would also like to extend my heartfelt gratitude to my tutor, Professor Ekin Ilseven, for his exceptional guidance throughout the demanding process of formulating a research question, conducting the research and finally putting it down on paper. His genuine personal interest and unwavering support were evident at every step, and I am profoundly grateful for the opportunity to learn under his mentorship. He challenged me to push beyond my perceived limits, fostering both personal and professional growth in ways I had not thought possible as part of my master thesis.

I will always cherish my time at CLSBE in Lisbon! Thank you for this opportunity.

**Table of Contents**

## 1. Introduction

In 2015 it was revealed that Volkswagen had intentionally installed software to manipulate emissions tests - this incident became known as the Volkswagen emissions scandal, also called the “Dieselgate”, one of the most significant corporate crises in modern history, which resulted in major shockwaves through global markets and shattered consumer trust (Bowen et al., 2018). The following months and years were characterized by a myriad of punitive actions, regulatory scrutiny and reputational damage for Volkswagen, culminating in billions of dollars in fines and a lasting damage on the company’s image worldwide (Wang & Wanjek, 2018). At the center of the Dieselgate was a fundamental negligence in responsibility-taking, later described as a failure that not only impacted the trust of stakeholders, but also highlighted the fragility of stakeholder relationships in regard to ethical questions (Bowen et al., 2018). Incidents like this, where stakeholder relationships and consumer trust are challenged are frequent and result from a wide array of different situations. They give rise to questions such as how organizations can rebuild and sustain trust in the aftermath of crises, particularly through the development and adaptation of narratives. Trust is the cornerstone of any stakeholder relationship and seems to be increasingly under strain in a complex world where corporate actions are scrutinized more than ever (Freeman, 1984; Hillenbrand et al., 2013). In crises, stakeholders expect not only acknowledgment of wrongdoings but also the proposal and implementation of specific actions that demonstrate accountability and a commitment to mutual benefit (Donaldson & Preston, 1995; Freeman et al., 2010). It is imperative to understand that this problem is not abstract; it is a pressing, real-world issue that affects every organization’s ability to operate sustainably in the modern business environment. Stakeholders, whether consumers, investors, employees, or policymakers, demand greater transparency and accountability, especially during crises (Freeman, 1984). Trust, once broken, is exceptionally difficult to rebuild, and failing to address this can have severe long-term consequences, including reduced market value, increased legal risks, and weakened stakeholder loyalty (Hegner et al., 2016).

Despite its significance, much of the existing research relies on theoretical frameworks (Coombs, 2007a; Jamali, 2008) or small-scale studies (Kim et al. 2017; Chen & Jai, 2019), which are capable of showing a minor picture of existing dynamics, however, raising the question of transferability to capture the full complexity.

I seek to contribute to gaps in the literature by analyzing real-world data over an extended period, in order to offer a perspective on how organizations adapt their responsibility-taking narratives in response to crises and regulatory frameworks.

To investigate this, I analyze responsibility-taking narratives as a strategic response to data breach incidents. Specifically, I leverage data breach notifications considering the impact of regulatory shifts, such as the California Consumer Privacy Act (CCPA) (Van Nortwick & Wilson, 2022) as an exogenous event, increasing consumer power. By employing linguistic analysis, which entails measures of responsibility-taking language, I evaluate how organizations assume responsibility in their crisis communication. Specifically, I employ a Difference in Differences (DiD) methodology to examine the impact of regulatory changes on organizational narratives, paired with further quantitative analysis to explore the relationship between these narratives and punitive consumer actions (Qin et al., 2024). My analysis reveals that organizations increasingly emphasize responsibility-taking language after the enforcement of the CCPA, demonstrating that heightened consumer power can effectively influence organizational behavior as a consequence of the implementation of regulatory frameworks. I also show that severity has a moderating role: Severe breaches involving sensitive information show to slightly decrease responsibility-taking language. Furthermore, I analyzed if responsibility-taking language leads to a lower likelihood of encountering punitive consumer actions in form of class action lawsuits and if this relationship is also moderated by severity; however, the findings challenge the assumption that responsibility-taking narratives alone can reduce legal risks, suggesting instead that they must be part of a broader array of variables influencing crisis management; nevertheless, the results are inconclusive here, which will be discussed in great detail later on.

This thesis makes two key contributions to the literature on corporate responsibility (Wartick, 1992; Hegner et al., 2016) and stakeholder management (Freeman, 1984; Donaldson & Preston, 1995). First, by providing empirical evidence from large-scale, longitudinal data I show how increased consumer power through regulatory frameworks like the CCPA influences corporate communication strategies at scale. The results demonstrate that not only compliance is affected but also responsibility-taking narratives seem to be shaped by it (Mulgund et al., 2021). Hence, I'm able to offer another perspective on how regulations can drive transparency and accountability. The thesis also gives hints that responsibility-taking narratives are not universally applied but instead adapted based on the nature of the crisis,

providing a foundation and inspiration for more context-specific approaches in stakeholder theory and crisis management.

The second contribution deepens the understanding of crisis communication by highlighting the moderating role of crisis severity (Coombs & Holladay, 2002; Jin et al., 2007).

## 2. Theoretical Background

### 2.1 Stakeholder Theory

Stakeholder theory, first articulated by Freeman (1984), states that organizations should consider the interests of all individuals and entities affected by the organization's operations, including customers, employees, suppliers, and communities, rather than prioritizing shareholders alone, hence calling for value creation through ethical and balanced engagement. Generally speaking, a stakeholder is defined as any group that can influence or be influenced by an organization's actions (Bryson, 2004). In later research, stakeholder theory was extended by highlighting its application in strategic management and business ethics (Freeman et al., 2010). Here it was argued that sustainable business success depends on fostering trust and cooperation with stakeholders. Going one step further Donaldson & Preston (1995) introduced a normative perspective to the theory, asserting that stakeholder theory is grounded in moral obligations, not just pragmatic considerations. For instance, Mitchell et al. (1997) proposed the salience model, categorizing and prioritizing stakeholders based on their power, legitimacy, and urgency, which underscores the need to dynamically manage stakeholder relationships, especially during crises (Nikkhah & Grover, 2022). Stakeholder emotions responding to a crisis range from anger and trust erosion to forgiveness (Jin et al., 2007). The salience model approach becomes particularly relevant in crisis scenarios, where addressing the concerns of critical stakeholders has the potential to save the organizational reputation (Mitchell et al.; 1997). It has been shown that organizations that integrate these principles into their strategic framework are better equipped to build resilient stakeholder relationships, ensure sustainable success and enhance their reputations (Mitchell et al., 1997). Syed (2019) defines enterprise reputation *"as an aggregate evaluation or perception of an enterprise's ability to meet the publics' expectations of securing customer information."* (p.257). She bases her definition in turn on Wartick (1992), who describes enterprise reputation as the stakeholders' collective assessment of how effectively an organization has fulfilled their expectations, grounded in its past actions.

Trust represents another critical element in managing stakeholder relationships and is fundamental to the long-term sustainability of any organization (Freeman, 1984). Trust is fostered over time by transparent (Auger, 2014), ethical (Donaldson & Preston 1995), and consistent actions (Hillenbrand et al., 2013), trust also ensures that stakeholders remain supportive even during crisis (Freeman et al., 2010). Hence as a result, organizations exhibiting accountability, integrity, and a dedication to mutual benefit to its stakeholders are better equipped to foster these relationships (Donaldson & Preston, 1995; Freeman et al., 2010). Also, transparent communication about organizational goals, decisions, and outcomes helps mitigate uncertainty and in turn facilitates trust building in sharing both successes and failures (Auger, 2014). Delivering consistently on promises enhances reliability and reinforces stakeholder confidence, a concept central to Donaldson & Preston's (1995) theory on organizational credibility. In general, ethical behavior, aligned with norms and regulatory standards, provides a strong foundation for trust (Williams, 2005). Building upon the foundation of trust, corporate responsibility is another essential mechanism for aligning corporate behavior with stakeholder expectations (Wartick, 1992). Trust creates a platform for stakeholders to evaluate organizational actions, while responsibility-taking solidifies and enhances this trust through accountability and proactive measures (Hillenbrand et al., 2013). Organizations that acknowledge their failures and implement corrective actions not only shield their reputation but once again are able to strengthen stakeholder relationships (Kim et al., 2017). In reference to that, it was shown that timely solutions to rectify issues (Jamali, 2008), further indicate an organization's commitment to learning from mistakes and safeguarding stakeholder interests.

An example of the importance of stakeholder relationships and its interconnection to reputation and trust is the Rana Plaza collapse of 2013 in Bangladesh, which brought intense scrutiny to global brands like Primark, Zara, H&M and others that were linked to the garment factories operating within the facility. These companies faced severe reputational damage as stakeholders demanded greater accountability (Beyer & Arnold, 2020). In the aftermath they prioritized stakeholder welfare, seeking to not only repair their reputations but also reinforcing the importance of building trust and ensuring long-term sustainability in their operations to their stakeholders (Beyer & Arnold, 2020). Overall, this exemplary case helps to corroborate the notion that for companies mitigating reputational damage and financial losses by leveraging stakeholder theory turns into a crucial focal point (Kim et al., 2017).

## 2.2 Crises and Framing

Crises are characterized by their unexpected nature, the significant threat they pose to organizational goals, and the need for immediate decision-making under pressure (Coombs, 2007b). According to Coombs (2007b) a crisis is defined as *"a sudden and unexpected event that threatens to disrupt an organization's operations and poses both a financial and a reputational threat."* (p.164). A crisis can harm stakeholders in a physical, emotional or financial way (Coombs, 2007b).

Hence, framing through narratives plays a central role in how organizations address crisis situations (Coombs, 2007a). Generally speaking, frames refer to how words and images appear in communication, hence frames support interpreting information and determine the way problems, their causes and solutions are specified, while allowing the assignment of responsibility (Druckman, 2001). Consequently, crisis types can also be defined as frames, allowing different interpretations based on the type, as shown before (Coombs & Holladay, 2002). Hence, leveraging frames is imperative when influencing public perceptions and stakeholder reactions in times of crisis (Coombs, 2007a). For example, during the MH370 crisis, where a Boeing 777 of Malaysia Airlines disappeared without a trace, the company leveraged both rational and emotional framing strategies to address public concerns and manage stakeholder expectations fairly successful (Ahmad et al., 2017). By combining factual updates about the ongoing investigation with empathetic messaging that acknowledged the emotional burden of affected family members, the airline aimed to frame the crisis as one of shared tragedy rather than negligence from their side (Ahmad et al., 2017). Qin et al. (2024) extend the notion of framing crises a certain way, by showing how the absence of framing, corporate silence, can become a destructive form of implicit communication. Using a DiD analysis, they measured the repercussions of failing to provide a frame during Blackout Tuesday, highlighting the risks of leaving stakeholder expectations unmet. Generally, this aligns with Druckman (2001) framing principles by assigning responsibility while fostering understanding and trust, showcasing how carefully crafted narratives can influence perceptions during high-stakes situations (Ahmad et al., 2017).

## 2.3 Situational Crisis Communication Theory

In the context of trust building and responsibility-taking behavior it is also important to take into account Attribution Theory, outlined by Weiner (1985), as it serves as a foundational theoretical groundwork for framing: The theory posits that individuals seek to understand the causes of events, particularly negative ones like a crisis, by attributing responsibility to internal or external factors (Weiner, 1986). The lens of Attribution Theory in turn establishes the foundation for Situational Crisis Communication Theory (SCCT), developed by Coombs (2007a). The theory operationalizes Attribution Theory to anticipate stakeholder reactions regarding potential reputational threats connected to a crisis, furthermore, to enable optimizing the outcome of a crisis. According to Coombs (2007a) a threat refers to the potential harm that could be caused to the reputation if it remains unaddressed. Moreover, it provides practical strategies for managing crises by explaining that organizational reputation is influenced both directly and indirectly by three situational attributes: initial crisis responsibility, crisis history and prior reputation (Coombs, 2004; Coombs, 2007a).

SSCT proceeds by clustering crises depending on their type into a victim, accidental and preventable cluster (Coombs & Holladay, 2002). As the name already implies, the victim cluster is characterized by organizations being victims of the crisis themselves (e.g natural disasters or malevolence), the accidental cluster is characterized by organizational actions causing a crisis unintentionally (e.g technical errors) and the preventable cluster is also characterized by organizational actions causing a crisis, however in this case intentionally by inappropriate actions (e.g management misconducts or misdeeds leading to injuries) (Coombs & Holladay, 2002; Coombs, 2007a). Moreover, according to SCCT, response strategies affect stakeholders' perceptions of a crisis and in a second step influence the reputation perceived of the organization having lived through this crisis. By carefully framing their crisis communication strategies, organizations can mitigate reputational damage, rebuild trust, and minimize punitive consumer actions (Coombs, 2007b; Kim et al., 2017; Kuipers & Schonheit, 2022). As mentioned beforehand, staying silent not only fails to address stakeholder concerns but can also be interpreted as an implicit stance, often harming the organization (Qin et al., 2024). As Qin et al. (2024) further argue, organizations that remain silent during moments of societal or organizational crises risk alienating stakeholders, intensifying reputational damage even more.

According to SCCT response strategies range from denial over diminish to rebuild, whereas research suggests that it is recommended to reduce negative effects by generally adjusting information through expressing concern for victims and strategies evolving around the rebuild strategy, furthermore when paired with compensation or a full apology, anger can be mitigated even more effectively (Coombs, 2007a) and are more likely to restore trust in consumers and reduce the likelihood of punitive actions (Klein & Dawar, 2004). This notion is corroborated by recent research that shows that by emphasizing recovery-focused narratives and transparent communication, companies can address dissatisfaction and foster empathy among stakeholders (Nikkhah & Grover, 2022).

Another approach to response tactics has been categorized into defensive, moderate and accommodative strategies, reflecting varying levels of remorse (Gwebu et al., 2018). Defensive strategies, such as denial or minimization, aim to deflect blame and protect reputation with minimal accountability. Moderate strategies involve partial acknowledgments or neutral responses, balancing reputation preservation with limited responsibility. Accommodative strategies demonstrate high remorse through apologies, corrective actions, and full responsibility to rebuild trust and repair stakeholder relationships (Gwebu et al., 2018).

Summarizing, SCCT suggests that stakeholders' responses are shaped by the attribution of crisis responsibility (Coombs, 2007a). Stakeholder theory reinforces the notion that narratives must reflect ethical engagement and align with stakeholder expectations to build trust (Donaldson & Preston, 1995; Freeman et al., 2010) and not create unmet expectations that in turn lead to emotional responses (Coombs, 2007b). Therefore, it is hypothesized that organizations increasingly adopt responsibility-taking narratives as a strategic response to meet heightened accountability demands under strengthened consumer rights frameworks (Coombs, 2007b; Kim et al., 2017; Kuipers & Schonheit, 2022).

**Hypothesis 1:** *Organizations are more likely to assume greater responsibility in their narratives when consumer rights are strengthened, as stronger rights increase the need for accountability.*

I also explore whether punitive consumer actions are less likely when a company takes greater responsibility. Stakeholder theory argues that organizations have a moral obligation to align

their responses with stakeholder expectations, thereby building trust and ensuring long-term sustainability (Donaldson & Preston, 1995; Freeman et al., 2010).

As Coombs and Holladay (2002) highlight, punitive actions serve as external amplifiers of reputational threats, especially in high-responsibility crises. These crises, often categorized as preventable within the framework due to intentional wrongdoing or gross negligence, frequently lead to public demands for accountability, shaping emotional responses such as anger or betrayal, particularly in cases of widespread harm (Jin et al., 2007; Romanosky et al., 2013). Also considering that emotional betrayal and expectancy violation lead to heightened emotional responses (Martin, 2017; Nikkhah & Grover, 2022). Preventable crises (Coombs & Holladay, 2002), characterized by deliberate or reckless organizational behavior, are most likely to provoke regulatory and legal repercussions due to the perceived breach of stakeholder trust (Coombs, 2007a). For example, widespread harm resulting from such crises has been empirically linked to increased litigation and regulatory scrutiny, as demonstrated by Romanosky et al. (2013). The demand for responsibility-taking narratives is particularly heightened in environments where consumer rights are robustly enforced. Failure to meet these expectations not only intensifies reputational damage but can also result in more severe punitive actions as stakeholders, empowered by stronger rights frameworks, seek to hold organizations accountable for violations of trust (Coombs, 2007b).

Furthermore, punitive actions are not merely financial or legal repercussions; they also serve as symbolic reminders of the importance of ethical engagement (Freeman et al., 2010). Research in the field demonstrates that trust is preserved through transparent and ethical communication, as stakeholders are less likely to pursue punitive measures when they perceive an organization is proactively addressing harm (Hillenbrand et al., 2013; Auger, 2014). This alignment is particularly crucial in preventable crises, where public perception often demands visible and authentic responsibility-taking efforts (Coombs, 2007a). The Dieselgate from the introduction section illustrates how preventable corporate crises can lead to severe punitive consumer actions. Volkswagen's deliberate installation of software to falsify emissions test results resulted in fines, settlements, and compensation globally. Legal actions from regulators and consumers, alongside class-action lawsuits, highlighted the financial risks of unethical practices (Bowen et al., 2018). The scandal provoked widespread consumer outrage and regulatory scrutiny, further heightened by Volkswagen's initial denials. While the company eventually adopted corrective actions such as public apologies and compensation programs, the reputational and legal consequences serve as a reminder of the

cost of betraying consumer trust (Wang & Wanjek, 2018). Hence, in this thesis it is hypothesized that the more responsibility an organization assumes, the less likely punitive consumer actions are.

**Hypothesis 2:** *The extent to which organizations assume responsibility in their narratives is negatively correlated with the likelihood of punitive consumer actions.*

Another important factor of SCCT for this thesis is when severity as a contextual factor that amplifies the reputational threat posed by a crisis comes into play (Coombs 2007a). In high-severity crises, stakeholders are more likely to experience intense emotions, such as anger or fear (Romanosky et al., 2013; Martin, 2017), increasing the demand for the organization to adopt responsibility-taking strategies, such as apologies or reparations, causing the reputational stakes to rise proportionally with the severity, requiring tailored communication to rebuild trust, even in accidental crises (Jin et al., 2007; Nikkhah & Grover, 2022). Empirical research by Coombs & Holladay (2002) further supports the moderating role of severity. Their study demonstrates that severity interacts with crisis responsibility, intensifying stakeholders' reactions and influencing the perceived adequacy of the organization's response (Coombs & Holladay, 2002; Jin, 2007).

Revisiting framing according to Druckman (2001), severity acts as a salient framing cue, emphasizing the magnitude of harm and directing stakeholders' attention toward the organization's response. This framing compels organizations to prioritize responsibility-taking narratives to meet heightened expectations. This emotional dimension complements SCCT's categorization of crisis types, as severity acts as a multiplier of reputational threats and potential punitive consumer actions, even in crises with lower perceived organizational responsibility (Coombs & Holladay, 2002). Johnson & Johnson's response to the 1982 Tylenol crisis exemplifies how severity amplifies reputational threats and the necessity for robust rebuild strategies (Trujillo & Toth, 1987; Seeger et al., 1998). The crisis, involving cyanide-laced capsules leading to fatalities, was marked by high severity, as it generated widespread fear and a profound loss of consumer trust. Johnson & Johnson effectively employed responsibility-taking narratives, prioritizing stakeholder safety through immediate product recalls and the introduction of tamper-proof packaging, which significantly mitigated reputational damage (Trujillo & Toth, 1987). Their strategy aligns with Coombs and Holladay's (2002) findings, demonstrating how high-severity crises demand tailored responses that acknowledge harm and offer corrective actions. By framing their response

around consumer safety and corporate accountability, Johnson & Johnson not only met heightened stakeholder expectations but also set a benchmark for crisis communication (Seeger et al., 1998). Consequently, I hypothesize the moderating role of severity on responsibility-taking.

**Hypothesis 3a:** *The severity of a data breach positively moderates the extent to which organizations assume responsibility, with higher severity leading to a greater likelihood of responsibility-taking.*

Even when responsibility-taking measures are employed, high-severity breaches may result in significant punitive actions due to heightened scrutiny and amplified stakeholder expectations (Hegner et al., 2016), as also described above in more detail. Hence the moderating role of severity on punitive consumer actions is also expected to affect this relationship.

**Hypothesis 3b:** *The severity of a data breach moderates the likelihood of punitive consumer actions, with higher severity increasing the probability of consumer backlash, regardless of responsibility-taking.*

**Figure 1**

*Theoretical Model*


## 3. Empirical Context

### 3.1 Data Breaches

In this thesis I investigate the responsibility-taking behavior of organizations after a crisis-like event that jeopardizes the relationship with their stakeholders in the context of data breaches. For the purpose of this thesis, I analyze publicly available breach notifications from the Attorney General of California and class action lawsuit data, in order to uncover whether

taking greater responsibility influences the fallout of data breaches, ultimately contributing to understanding of how organizations can build and maintain stakeholder trust, in the light of crisis situations (Coombs 2007a; Freeman et al., 2010). To corroborate the relevance of my data breaches focus in my analysis, an overview of relevant data concerning the topic results to be useful: In the third quarter of 2024 alone, approximately 422.61 million data records were leaked globally (Statista, 2024), affecting millions of individuals with 46% of breaches involving the theft of sensitive personal information, such as tax identification numbers and home addresses (Bonnie, 2024). As a result, the financial repercussions of data breaches are enormous; the average cost of a data breach reached an all-time high of $4.88 million in 2024, marking a 10% increase from 2023 (IBM, 2024).

However, this only seems to be the tip of the iceberg as cybercrime is projected to cost $10.5 trillion by 2025, growing at a rate of 15% annually globally (IBM, 2024). The escalating frequency and impact of data breaches underscore the critical importance of robust cybersecurity measures: In an era where data breaches have become a pressing concern for organizations and consumers alike, the question of how organizations communicate their accountability and create trust among shareholders has taken center stage (Hillenbrand et al., 2013). With consumer data protection rights becoming more elevated and robust in many jurisdictions around the world, organizations face increasing pressure to address breaches transparently and responsibly (Mulgund et al., 2021). Simultaneously, the severity of breaches and the sensitivity of the compromised data often shape public perception and consumer response, posing challenges for organizations striving to maintain trust and mitigate backlash as seen above (Coombs & Holladay, 2002). Although data breach research covers a wide field, from technical (Nemec Zlatolas et al., 2024) to financial (Cavusoglu et al., 2004), to managerial (Kuipers & Schonheit, 2022) and legal aspects (De Hert & Papakonstantinou, 2016), the dynamic nature of data breaches necessitates interdisciplinary approaches.

Data breaches represent a modern, pervasive and online form of crisis that pose a threat to organizational stability and reputation caused by several factors, such as lax data handling policies, system vulnerabilities, internal misuse and/or human flaws (Kuipers & Schonheit, 2022). When a data breach occurs, the interests and trust of various stakeholders are compromised (Diers-Lawson et al., 2021). Hence, stakeholder theory (Freeman, 1984) is an apt framework for understanding and managing the impact of a crisis-like event, such as a data breach. In this case the crisis is fueled once a data breach compromises confidentiality, integrity, and availability of organizational data (Aldossary & Allen, 2016), due to disrupted

organizational operations and exposed sensitive information, such as customer financial records, intellectual property theft, or large-scale identity theft, which often affect thousands or even millions of stakeholders (Kuipers & Schonheit, 2022), as seen above.

Research suggests that data breaches are dynamic phenomena and cannot easily be attributed to one of the clusters proposed by SCCT (Kim et al., 2017). However, data breaches also have been described as the result of human errors, such as careless employees, outdated security programs, and a lack of proper training, which are characterized as preventable factors implying that organizations bear responsibility due to their controllability over these elements (Ayyagari, 2012). Consequently, data breaches go beyond mere technical failures and can be understood as crises requiring robust responses (Cavusoglu et al., 2004; Kelly, 2005) for a wide array of stakeholders, each and every one with their own vulnerabilities and expectations (Syed, 2019). Hence, stakeholders of an organization are directly or indirectly impacted by data breaches, with varying levels of vulnerability. For example, consumers whose financial information is compromised may face economic losses, while investors may suffer from devaluation of organizational stock (Choi et al., 2022).

In the context of data breaches, stakeholders evaluate the extent to which the organization had control over the breach and whether it demonstrated negligence (Chatterjee et al., 2019). Similarly, Hegner et al. (2016) highlighted that breaches caused by preventable or internal failures evoke heightened distrust and punitive intentions, particularly when stakeholders perceive the organization as having failed to uphold expected security standards. In terms of data breaches Expectancy Violation Theory (EVT) highlights the profound emotional and cognitive impacts of such violations on relational trust and accountability (Martin et al., 2017; Nikkhah & Grover, 2022). It explains how individuals form expectations based on social norms and contextual cues, and how deviations from these expectations can provoke strong emotional and behavioral responses (Afifi & Metts, 1998). Typically, stakeholders anticipate that companies will safeguard their private information (Nikkhah & Grover, 2022), but when this expectation is violated, particularly in cases of preventable or internally caused breaches, it can lead to dissatisfaction, distrust, and punitive actions, as stakeholders perceive the organization as having failed to meet its foundational obligations (Afifi & Metts, 1998; Nikkhah & Grover, 2022). Chipotle's 2015 E. coli outbreak exemplifies how expectancy violations can provoke strong stakeholder reactions when norms of safety and trust are disrupted (Zhao et al., 2018). Customers, who previously associated Chipotle with high-quality and safe food, experienced a sharp contrast between expectations and reality, leading

to significant dissatisfaction and reputational harm. The violation of these expectations aligns with EVT, as the intensity of stakeholder emotions, including anger and fear, increased due to the unexpected nature of the crisis (Zhao et al., 2018). By transparently addressing the crisis, implementing enhanced safety protocols, and launching a robust marketing campaign, Chipotle managed to rebuild customer trust and recover from the reputational damage, demonstrating the critical role of effective post-crisis communication in managing expectancy violations (Nikkhah & Grover, 2022)

### 3.2 Regulation as Empirical Identification Strategy

To investigate how organizations take responsibility in their narratives towards their stakeholders in the aftermath of a crisis, I take advantage of a regulatory change that increases the consumer protection rights in data breach cases, as already mentioned before. Due to the exogenous nature of this regulation to organization strategies, this allows me to find causal support to my hypotheses. Nevertheless, in order to get a full picture of how organizations navigate stakeholder trust and public perception after data breaches, it is necessary to dive deeper into this particular regulation. In the US-state of California, data privacy is regulated by the CCPA, enacted in 2018 and fully enforceable by 2020. This regulation establishes the framework under which data breaches must be handled, including data breach notifications. As this thesis compares pre- and post-CCPA breach notifications, it is essential to understand the regulatory landscape prior to its enforcement.

Historically, data privacy regulation in the United States has been fragmented, with state-specific laws addressing breaches inconsistently. Many focused narrowly on specific data types, such as Social Security numbers or financial information, leaving other personal data unregulated (Van Nortwick & Wilson, 2022). This lack of uniformity allowed organizations significant discretion in disclosing breaches, often resulting in minimal transparency and a focus on reputation management over consumer protection (Van Nortwick & Wilson, 2022). In addition to that, organizations operating in this fragmented system develop breach narratives that can be reactive by fulfilling minimal legal obligations (Acquah et al., 2024), avoiding the broader implications of systemic vulnerabilities in their data protection practices (Hosseini et al., 2024).

The CCPA brought significant changes, creating a uniform standard for businesses collecting personal information about California residents (Cal. Civ. Code § 1798.82, 2023). It expanded

the definition of personal information to include categories such as internet browsing history, geolocation, and biometric data, alongside traditional identifiers like names and social security numbers (Cal. Civ. Code § 1798.140, 2023). This broader scope ensures that more breaches fall under notification requirements, compelling businesses to reevaluate data-handling practices and enhance transparency.

Under California Civil Code § 1798.82 (2023), a data breach is defined as the *"unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a business."* Additionally, the act provides a private right of action for breaches resulting from inadequate security measures, enabling individuals to seek statutory damages (Cal. Civ. Code § 1798.150, 2023). Together, these provisions have shaped how businesses approach breach disclosures, compelling organizations to provide clear and detailed notifications to affected individuals. For example, notifications must include the categories of personal information compromised and steps affected individuals can take to mitigate potential harm (Cal. Civ. Code § 1798.82(d), 2023). This has heightened the stakes for organizations, incentivizing stronger data security measures and more thorough breach disclosures (Acquah et al., 2024).

The introduction of the CCPA has elicited mixed reactions among organizations. Fear arose from the risk of lawsuits and financial penalties, prompting businesses to rapidly adopt compliance measures (Mulgund et al., 2021). Frustration has stemmed from navigating the fragmented regulatory landscape and the costs of compliance (Jurcys & Lampinen, 2020). However, for some, the CCPA presented an opportunity to strengthen consumer trust by improving transparency and data protection practices (Mulgund et al., 2021).

Existing literature on data breaches, such as Gwebu et al. (2018) emphasize the importance of crisis response strategies and corporate reputation in mitigating data breach impacts, however they do not address the influence of regulatory framework. Similarly, Syed (2019) highlights the role of responsibility attribution in escalating reputational damage on social media, additionally, Chen & Jai (2019) provide insights into how corporate responsibility narratives influence consumer trust and revisit intentions, moreover Carre et al. (2018), explore consumer perceptions of corporate responsibility. Nevertheless, this thesis positions responsibility-taking between regulatory shifts and punitive consumer actions in the form of class action lawsuits, hence offering a framework that bridges regulatory, corporate, and consumer dimensions, hereby striving to address gaps in the existing literature.

## 4. Methodology

Methodologically, Qin et al. (2024) present a compelling approach by leveraging social media data to assess consumer engagement patterns pre- and post-crisis. Their experiment design serves as a useful reference for understanding how stakeholder reactions to crises can be quantified using digital metrics.

### 4.1 Data Extraction and Preprocessing

The data used in this thesis stems from two sources: I extracted the information about data breaches from the website of the Attorney General of California (State of California - Department of Justice - Office of the Attorney, n.d.), as it provides an unique comprehensive list of data breaches and data breach notifications issued by organizations that suffered a data breach, whenever affecting more than 500 California residents for very entry starting 2020 (Cal. Civ. Code § 1798.82). The key advantage of this database lies in its extensive coverage of data before and after the enforcement of the CCPA, allowing for a detailed analysis of its impact. Moreover, it provides the opportunity to examine organizational narratives and derive responsibility markers, crucial to answer H1 and H3a. Its uniquely comprehensive and structured format further simplifies the extraction of information. Although the list dates back to 2012, for the purpose of this thesis, I extracted all data breach cases and corresponding notifications between 01.01.2017 and 11.11.2024. This period allowed me to have sufficient data before and after 01.01.2020, the day the CCPA was enforced, which is an exogenous shock to the strength of consumer rights.

To gather data on class action lawsuits, I utilized a publicly accessible database of U.S. class action cases provided by ClassAction.org (2024). The database is optimal for the purpose of measuring punitive actions of consumers through its extensive list of class action lawsuits, which allows it to employ it in order to analyze H2 and H3b. By employing keywords related to data breaches, such as "data breach," "unauthorized access," "cybersecurity," and "information theft", a total of 1,956 cases involving data breaches were identified and extracted. I matched data breach cases between the first and second databases through a two-step process. First, the names of organizations in both databases were standardized to ensure consistency. Next, I identified the matches by comparing organization names and aligning dates. Specifically, a 12-month timeframe was established between the initial reporting of the data breach to the Attorney General and the filing of the lawsuit.

Fuzzy matching was used as part of this process to account for variations in organization names, such as spelling errors, abbreviations, or formatting differences. Fuzzy matching assigns a similarity score to pairs of strings, allowing for approximate matches rather than requiring exact correspondence (Navarro et al., 2001). However, this process only allowed to match 14 class action lawsuit cases for the time period before 2020 and 67 class action lawsuit cases starting 2020; the implications of this imbalance will be discussed later on.

### 4.2 Variables

First, a binary variable called “CCPA” was created, where 0 refers to a data breach incident before 01.01.2020 and 1 to a data breach incident starting 01.01.2020. For more information on the exact amount of data breach notifications extracted please refer to Table 1 and Figure 2. The variable functions as the treatment indicator in a DiD design, capturing the temporal variation introduced by the CCPA enforcement. This allows for causal analysis of its impact on the organization's narratives.

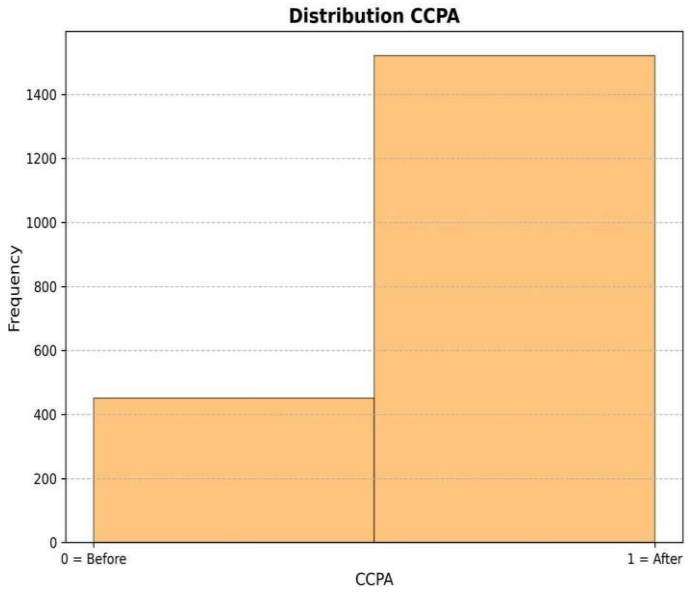
**Table 1**

*Breach Notifications Overview*

| CCPA | General | Documents extracted | Documents apt for analysis |
|---|---|---|---|
| **0** (01.01.2017 - 31.12.2019) | x | 818 | 451 |
| **1** (01.01.2020 - 11.11.2024) | x | 2473 | 1521 |
| **Total** | 4271 | 3291 | 1972 |

**Figure 2**

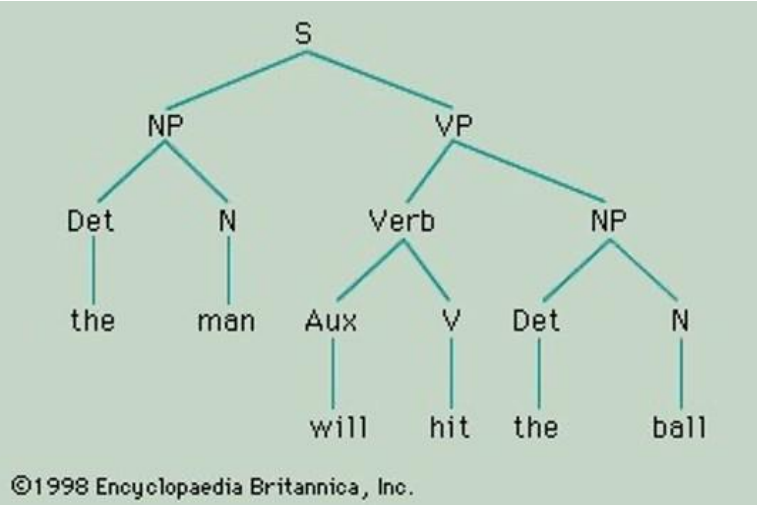
*Distribution CCPA*




All data breach notifications from the Attorney General dataset follow a similar structure, with consistent phrasing of headings across documents. The following sections were extracted from each notification: *"What happened?"* (What Happened?), *"What information was involved?"* (Information Involved), *"What we are doing."* (Action Taken) and *"What you can do."* (Recommendations). Please refer to Appendix A for an example of a data breach notification document. After manually revising and cleaning the entries, the word count for the variables Action Taken and Recommendations was calculated, with non-ASCII characters, URLs, and numbers excluded from the analysis. In a second step, the we + verb count for the Action Taken variable and the you + verb count for the recommendations variable were calculated using Part of Speech (PoS) tree analysis. PoS analysis is a method used to identify and categorize words in a text based on their grammatical roles, such as nouns, verbs, or pronouns. This approach is suitable because it ensures accurate identification of specific word combinations, (here; "we + verb" or "you + verb"), by focusing on their grammatical structure rather than just matching words, which helps avoid errors caused by similar but irrelevant phrases (Marantz, 2020). Please refer to Figure 3 for a simple overview of the process.

**Figure 3**

*PoS tree example*




*Note.* Marantz, (2020). *Understanding sentences – NYU MorphLab*.

https://wp.nyu.edu/morphlab/2020/06/23/understanding-sentences-part-1/

Furthermore, by simply dividing the length through the pronoun + verb count two new variables called “Company Responsibility” and “Consumer Responsibility” were added to the dataset. Moreover, a formula for score measuring responsibility was defined as

*Responsibility Score = (we_verb_count / we_length) - (you_verb_count / you_length)*

The variables Company Responsibility and Consumer Responsibility are employed as dependent variables in H1, however Responsibility Score serves both, as dependent variable (H1, H3a) and independent variable (H2, H3b).

Next, keywords from the “Information Involved” column were utilized to create categories of data compromised in the data breach incidents; the ten categories, in addition to the keywords, can be consulted in Appendix B for more information. These categories have two functions in this analysis: Firstly, to serve as control variables, and secondly, to create the Severity variable, employed in H3a and H2. These severe categories include PII, Financial Information, Authentication Credentials, Health and Medical Information, and Government-Issued Identification and can be considered severe because they involve sensitive data that can

directly lead to identity theft, financial loss, or privacy violations. Compared to less critical categories like Digital Footprints or Miscellaneous Data, breaches of these data types pose immediate and tangible risks to individuals' security, privacy, and well-being, making them more consequential in public perception and regulatory scrutiny. However, it turned out that according to this measure of severity there is an imbalance between severe (1725) and not severe (249) cases, which must be taken into account when analyzing the results presented below. Lastly, another binary variable called "Lawsuit" was created, which functioned as the dependent variable in order to answer H2 and H3b, where 0 indicates no matched class action lawsuit and 1 that there is a match. The implications of the discrepancy between the amounts will be discussed in more detail later on.

## 5. Empirical Analysis & Results

As a start, I visualized the newly computed variables in an array of graphs. Keeping in mind that the dataset isn't evenly distributed between CCPA = 0 and CCPA = 1, a look at the distribution of Consumer Responsibility and Company Responsibility in Figure 4 and 5, as well as the comparison between the ratios in Figure 5 and 6 reveals an increase in Company Responsibility for CCPA = 0 and little to no change in Consumer Responsibility. To underscore this first impression of the data a cumulative distribution function graph (Figure 8) confirms that the changes in Consumer Responsibility and Company Responsibility are relatively small but systematic, with a more pronounced decrease in Consumer Responsibility and a modest increase in Company Responsibility in the after period. This supports the conclusion that the distribution might have evolved between the time periods, reflecting shifts in language use.

**Figure 4**

*Distribution Company Responsibility*

**Figure 5**

*Distribution Consumer Responsibility*

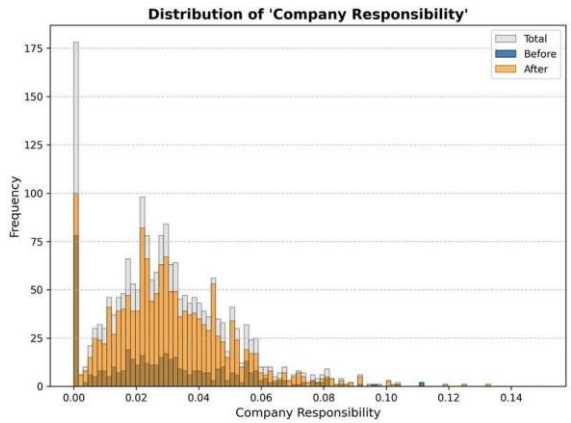



**Figure 6**

*Responsibilities comparison, CCPA=0*

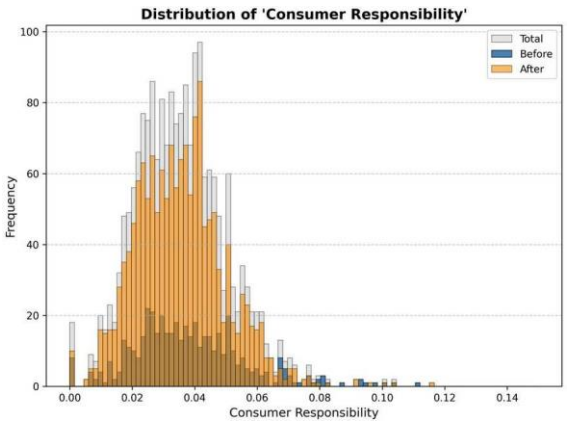
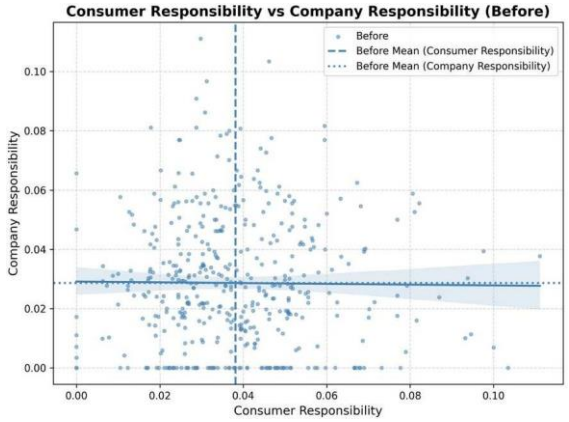



**Figure 7**

*Responsibilities comparison, CCPA=1*



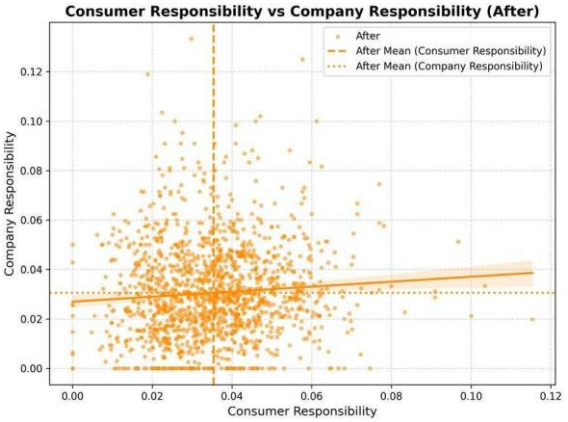
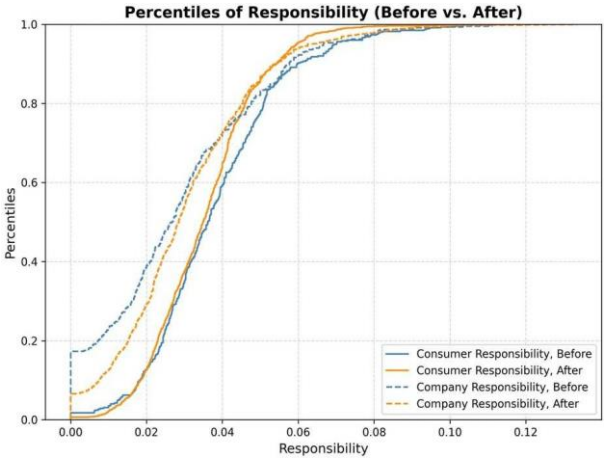




**Figure 8**

*Percentiles comparison, CCPA & Responsibilities*




Although the graphs show a tendency towards an increase in responsibility taking language in data breach notifications after the enforcement of the CCPA and little to no movement in responsibility deflecting language, inferential statistics are needed to confirm these

observations. Consequently, as a first step a t-test was performed (Table 2), which reveals a first indication towards a significant (p-value < 0.01) decrease (-0.0028) in Consumer Responsibility for CCPA = 1, while the increase (0.0019) in Company Responsibility is only significant for a threshold of p-value < 0.1. These findings provide first evidence of a shift in the use of Consumer Responsibility and Company Responsibility over time, however the change in Consumer Responsibility appears to be more conclusive.

The following regression models leverage a DiD approach, with CCPA representing the treatment effect of the CCPA enforcement. The regression results from models 1 and 2 in Table 3 show that CCPA has a significant but small effect on both variables. For Company Responsibility, there is a weak significant (p-value < 0.1) effect, indicating a slight increase (0.002) over time, while for Consumer Responsibility, there is a highly significant (p-value < 0.01) negative effect (-0.003), showing a small but clear decrease over time. To corroborate this effect in a regression analysis in Table 4 revealed a highly significant (p-value < 0.01) positive effect (0.005) of CCPA on Responsibility Score. This suggests that over time, organizations have increasingly adopted a higher responsibility-taking narrative in their data breach notifications. Together, the results indicate a clear temporal shift: the Company Responsibility (responsibility taking) has slightly increased, Consumer Responsibility (responsibility deflecting) has decreased, and overall Responsibility Score has risen, reflecting a growing tendency for organizations to assume more responsibility in response to breaches. In order to further back up the observed effect I added the data breach categories (Appendix B) to the regression analysis. Including these variables is logical as different data types carry varying levels of sensitivity and perceived risk, which likely influence how companies frame their responses. While the significant effect of CCPA on Company Responsibility (p-value < 0.05; 0.002) and Consumer Responsibility (p-value < 0.01, -0.002) remains consistent, one can observe that categories, such as PII significantly (p-value < 0.05) minimally reduce both Company Responsibility and Consumer Responsibility. In contrast, Financial Information (p-value < 0.01; 0.002) and Authentication Credentials (p-value < 0.05, 0.001) significantly increase Company Responsibility, while Sensitive Data shows a significant (p-value < 0.05) positive effect (0.002) on Consumer Responsibility. Other data types, such as Health and Medical Information and Digital Footprints, do not exhibit statistically significant effects (p-value > 0.1) as seen in model 3 and 4 in Table 3. The results from the diverse analysis presented allow the conclusion that H1 can be supported.

**Table 2:**

*t-test CCPA*

| Variable | t-Statistic | p-value | Mean Difference |
|---|---|---|---|
| **Consumer Responsibility** | 3.4184 | 0.0006 *** | -0.0028 |
| **Company Responsibility** | -1.7859 | 0.0743 * | 0.0019 |

**Table 3**

*Regressions Company Responsibility & Consumer Responsibility*

| Regression (OLS) | (1) DV: Company Responsibility | (2) DV: Consumer Responsibility | (3) DV: Company Responsibility | (4) DV: Consumer Responsibility |
|---|---|---|---|---|
| **Const** | 0.029*** (0.027, 0.030) | 0.038*** (0.037, 0.040) | 0.029*** (0.026, 0.031) | 0.038*** (0.036, 0.040) |
| **CCPA** | 0.002* (-0.000, 0.004) | -0.003*** (-0.004, -0.001) | 0.002** (0.000, 0.005) | -0.002*** (-0.004, -0.001) |
| **Personal Identifiable Information** | | | -0.000** (-0.001, -0.000) | -0.000** (-0.001, -0.000) |
| **Financial Information** | | | 0.002*** (0.001, 0.003) | 0.001** (0.000, 0.002) |
| **Authentication Credentials** | | | 0.002*** (0.001, 0.003) | 0.001** (0.000, 0.002) |
| **Health and Medical Information** | | | 0.001 (-0.000, 0.002) | 0.000 (-0.000, 0.001) |
| **Employment Information** | | | 0.002 (-0.002, 0.005) | -0.001 (-0.004, 0.001) |
| **Government-Issued Information** | | | -0.003** (-0.005, -0.000) | 0.001 (-0.001, 0.002) |
| **Digital Footprints** | | | -0.003 (-0.041, 0.036) | -0.002 (-0.032, 0.028) |
| **Sensitive Data** | | | -0.000 (-0.002, 0.001) | 0.002** (0.000, 0.003) |
| **Miscellaneous Data** | | | -0.002 (-0.005, 0.001) | -0.001 (-0.003, 0.001) |
| **System and Account Metadata** | | | -0.004 (-0.017, 0.009) | 0.004 (-0.006, 0.014) |
| Observations | 1972 | 1972 | 1972 | 1972 |
| R2 | 0.002 | 0.006 | 0.019 | 0.017 |
| Adj. R2 | 0.001 | 0.005 | 0.013 | 0.011 |
| Residual Std. Error | 0.020 (df=1970) | 0.015 (df=1970) | 0.020 (df = 1960) | 0.015 (df=1960) |
| F Statistic | 3.189* (df=1; 1970) | 11.686*** (df=1; 1970) | 3.414*** (df=11; 1960) | 3.054*** (df=11; 1960) |
| Note: | | | | *p<0.1; **p<0.05; ***p<0.01 |

**Table 4**
*Regression Responsibility Score & CCPA*

| Regression (OLS) | (1)<br>DV: Responsibility Score |
|---|---|
| **Const** | -0.010***<br>(-0.012, -0.007) |
| **CCPA** | 0.005***<br>(0.002, 0.007) |
| Observations | 4271 |
| R2 | 0.006 |
| Adj. R2 | 0.006 |
| Residual Std. Error | 0.024 (df=1970) |
| F Statistic | 12.821*** (df=1;1970) |
| Note: | *p<0.1; **p<0.05; ***p<0.01 |

As mentioned before, the "Lawsuit" variable indicates whether a class action lawsuit occurred as a consequence of a data breach incident and is a highly relevant variable in order to analyze H3. Initial logistic regression analyses with Lawsuit as the dependent variable and CCPA as well as Responsibility Score as independent variables did not yield significant results (p-value < 0.1) (Table 5).

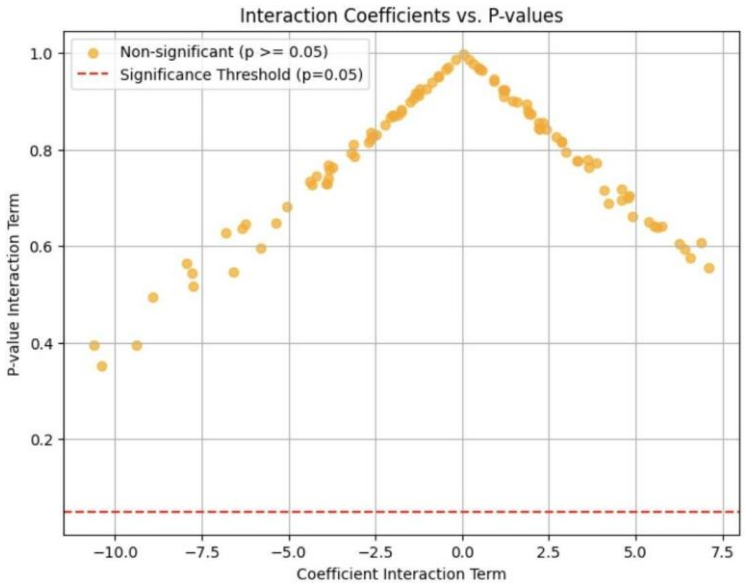
**Table 5**
*Simple Regression Lawsuit Filed*

| Regression (Logit) | (1)<br>DV: Lawsuit Filed |
|---|---|
| **Const** | -3.446***<br>(-3.986, -2.906) |
| **CCPA** | 0.366<br>(-0.222, 0.953) |
| **Responsibility Score** | -0.512<br>(-9.789, 8.765) |
| Observations | 1972 |
| Pseudo R2 | 0.002 |
| Note: | *p<0.1; **p<0.05; ***p<0.01 |

Hence, a second step introduced an interaction term between CCPA and Responsibility Score to test whether the effect of responsibility-taking narratives on the likelihood of lawsuits changes over time. To ensure robustness, due to the imbalanced nature of the Lawsuit variable a series of 100 logistic regressions were performed using random samples each time. Non-lawsuit cases were sampled before (70 cases) and after (335 cases) the time period, which is 5 times the amount of Lawsuit cases respectively, while all lawsuit cases were included in each iteration. The first analysis, visualized in Figure 9, tested a simplified model with only CCPA, Responsibility Score, and their interaction term. On the x-axis one can see the interaction term, whilst on the y-axis lies the corresponding p-value; the dotted red line is a visual marker for p-value < 0.05. The results show no significant interaction effects across all iterations, with p-values consistently above the 0.05 threshold, suggesting no observable relationship.

**Figure 9**

*Iterative Regression Lawsuit*

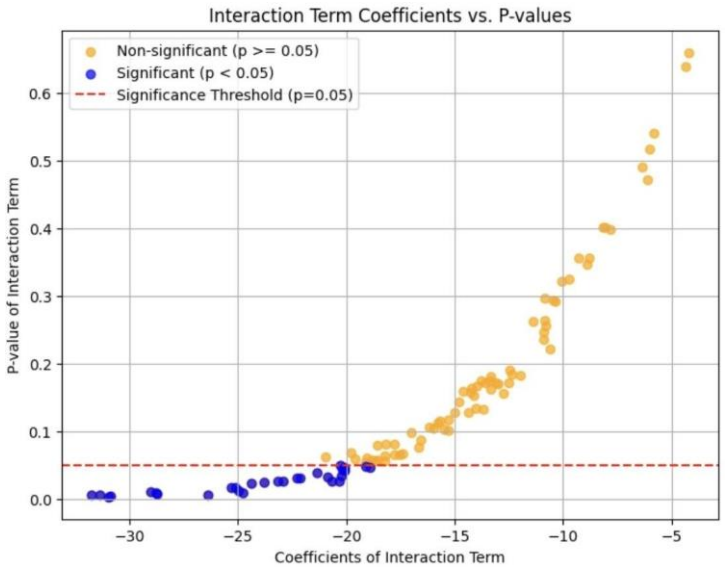



*Note.* Interaction Term = CCPA * Responsibility Score

In a subsequent analysis, the data breach categories, which were introduced above, were included as control variables to account for the influence of breach types on the likelihood of class action lawsuits. The results, visualized in Figure 10, with the interaction term once again on the x-axis and the corresponding p-value on the y-axis, show that while the majority (71 for p-value >= 0.05) of interaction terms remain non-significant, a small number (29 for p-value < 0.05) of iterations produce significant effects ($p < 0.05$). The dotted red line indicates where p-value < 0.05 lies. However, unlike in Figure 9, the sign of all interaction coefficients is aligned with the expectations; more responsibility taking leads to less chances of lawsuits. This indicates that involving the nature of the data breach is essential to reveal the effect of responsibility taking by organizations. Nevertheless, the clustering of p-values around the value 0.15 suggest that these inferred effects remain inconsistent and further analysis is necessary

**Figure 10**

*Iterative Regression Lawsuit 2*




*Note.* Interaction Term = CCPA * Responsibility Score

And lastly, to further investigate, t-tests (Table 6) were conducted to compare Company Responsibility, Consumer Responsibility, and Responsibility Score between lawsuit cases for CCPA = 1. The test also revealed no significant differences (p-value > 0.1) across the key variables, reinforcing the earlier findings that no robust relationship can be established between class action lawsuits

**Table 6** *t-test: CCPA for Lawsuit Filed = 1*

| Variable | t-statistic | p-value | Mean Difference |
|---|---|---|---|
| **Consumer Responsibility** | 0.1453 | 0.8848 | -0.0006 |
| **Company Responsibility** | -0.6663 | 0.5072 | 0.0043 |
| **Responsibility Score** | -0.6474 | 0.5192 | 0.0049 |

Taken together, these results suggest that while the inclusion of data breach categories introduces some variability, neither CCPA, Responsibility Score, nor their interaction consistently influence the likelihood of lawsuits. This highlights that factors beyond the variables analyzed are likely the primary drivers of legal action in response to data breaches. Hence, it can be concluded that there seems to be some support for H3, however not well documented, due to the use of a fairly conservative dataset - more on that can be found in the limitation section.

It was chosen as an apt moderator due to the severity of breached data changing the stakes for organizations and stakeholders. For severe breaches, the higher risk of tangible harm (e.g., financial loss, identity theft) might affect the effectiveness of responsibility-taking narratives. In less severe breaches, where the consequences are lower, responsibility-taking narratives might mitigate more effectively punitive consumer actions, such as class action lawsuits.

In order to test H3a and H3b another binary variable with the name “Severity” was created (0 being not severe and 1 being severe). Consequently, I conducted a regression analysis to test H3a (Table 7). The results indicate that Severity has a weak, significant (p-value < 0.1) negative effect (-0.003) on Responsibility Score in model 1, meaning that when a breach was severe the emphasis on responsibility-taking language was reduced in data breach notifications. In contrast, CCPA has a significant (p-value < 0.01) positive effect (0.004), suggesting that after the introduction of the CCPA, companies have adopted more responsibility-taking narratives, placing greater emphasis on their own actions. When adding an interaction term of both variables to the analysis causes all variables to be above the p-value threshold (p-value > 0.1) , which gives a hint that while time and severity individually influence Responsibility Score, their combined effect does not meaningfully alter the use of responsibility-taking language, leading to a loss of statistical significance.

However, as seen in the regression analysis concerning H1, it was shown that some data breach categories, such as Financial Information, Authentication Credentials, and Sensitive Data, had an effect on the components of the Responsibility Score: Company Responsibility and Consumer Responsibility. Specifically, Financial Information and Authentication Credentials increased Company Responsibility (responsibility-taking language), while Sensitive Data increased Consumer Responsibility (responsibility-deflecting language),

indicating that when looking at severe categories individually, an effect can be observed. Hence, H3a can only be partially supported.

**Table 7**
*Regression Severity (H3a)*

| Regression (OLS) | (1)<br>DV: Responsibility Score | (2)<br>DV: Responsibility Score |
|---|---|---|
| **Const** | -0.006***<br>(-0.010, -0.003) | -0.004<br>(-0.019, 0.011) |
| **Severity** | -0.003*<br>(-0.006, 0.000) | -0.005<br>(-0.021, 0.010) |
| **CCPA** | 0.004***<br>(0.002, 0.007) | 0.002<br>(-0.014, 0.017) |
| **Severity * CCPA** | | 0.002<br>(-0.013, 0.018) |
| Observations | 1972 | 1972 |
| R2 | 0.008 | 0.008 |
| Adj. R2 | 0.007 | 0.007 |
| Residual Std. Error | 0.024<br>(df=1969) | 0.024<br>(df=1968) |
| F Statistic | 8.143***<br>(df=2; 1969) | 5.457***<br>(df=3; 1968) |
| Note: | | *p<0.1; **p<0.05; ***p<0.01 |

Moving on to H3b, the dataset was split into two subsets along the lines of severe and not severe classified data breaches. However, running a regression analysis (Table 8) neither CCPA, Responsibility Score, nor their interaction show significant (p-value > 0.1) effects; for non-severe breaches, the results are similarly inconclusive: none of the independent variables are significant (p-value > 0.1) . These results suggest that neither CCPA nor Responsibility Score meaningfully affect the likelihood of lawsuits here, and their combined interaction does not alter this relationship. Consequently, H3b cannot be supported, and it is highlighted that there's a need to explore alternative factors, such as regulatory environments or breach-specific circumstances, that may better explain variations in legal outcomes, which will be discussed in more detail in the limitations section.

**Table 8**
*Regression Severity (H3b)*

| Regression (Logit) | (1)<br>DV: Lawsuit Filed for "Severe" Dataset | (2)<br>DV: Lawsuit Filed for "Not Severe" Dataset |
|---|---|---|
| **Const** | -3.423***<br>(-3.987, -2.858) | -28.701<br>(-1069005.50, 1068948.09) |
| **CCPA** | 0.359<br>(-0.267, 0.985) | 25.540<br>(-1068951.26, 1069002.34) |
| **Responsibility Score** | -0.486<br>(-19.118, 18.146) | 0.088<br>(-36952972.38, 36952972.56) |
| **CCPA * Responsiblity Score** | 1.474<br>(-20.497, 23.446) | -8.066<br>(-36952980.54, 36952964.40) |
| Observations | 1724 | 248 |
| Pseudo R2 | 0.002 | 0.014 |
| Note: | | *p<0.1; **p<0.05; ***p<0.01 |

Summarizing the results, the findings show clear support for H1, with organizations adopting responsibility-taking narratives for the time period after the enforcement of the CCPA. H3a is partially supported, as severity reduces overall responsibility-taking but varies by data type compromised.

However, H2 is partially supported with only sparse hints to an effect of increased likelihood of class action lawsuits due to the implementation of the CCPA and/ or responsibility taking or responsibility deflecting language when adding data type categories compromised to the analysis. Moreover, H3b is not supported - the dataset doesn't allow a conclusion in terms of data breach severity plays a role in terms of increased or decreased class action lawsuit likelihood

.

## 6. Discussion

The first part of my research question was to examine how increased consumer power through changing regulatory frameworks influences organizations' responsibility-taking narratives following data breaches and whether these narratives reduce the likelihood of punitive consumer actions. Also, I sought to find an answer if and how the severity of data breaches influences the likelihood of adopting responsibility-taking narratives and the likelihood of punitive consumer actions. Drawing on Stakeholder Theory (Freeman, 1984; Donaldson &

Preston, 1995) hypotheses were developed and tested to explore these dynamics. The findings indicate support for H1, suggesting that organizations adopt more responsibility-taking narratives in response to strengthened consumer rights under the CCPA. While severity (H3a) was found to have an impact on responsibility-taking narratives (Coombs & Holladay, 2002; Coombs, 2007a), the effect varied by the data breach type (Hegner et al., 2016; Nikkhah & Grover, 2022). In some cases, a significant effect was found, while in others no such effect could be proven. However, no consistent evidence was found linking responsibility-taking narratives to the likelihood of punitive consumer actions (Romanosky et al., 2013; Syed, 2019), suggesting that additional factors may play a more significant role in shaping legal outcomes (H2). In addition to that there was no significant effect found in terms of data breach severity influencing the likelihood of punitive consumer actions (H3b).

### 6.1 Theoretical Implications

The shift towards responsibility-taking narratives in response to strengthened consumer power facilitated through the CCPA highlights the role of regulatory frameworks in shaping organizational communication strategies. This supports and extends the application of Stakeholder Theory by demonstrating that organizations, which adapt narrative strategies to align with the expectations and power dynamics of increasingly empowered stakeholders, holds particularly true for consumers of the company (Freeman, 1984, Freeman et al, 2010). The lack of consistent results between responsibility-taking narratives and the likelihood of punitive consumer actions, remains inconclusive, however, foregone studies indicate that a relationship between the concepts is likely (Hillenbrand et al., 2013; Auger, 2014). Furthermore, the findings show that the type and severity of the breach play a role in determining narrative choices, with weak findings pointing into the direction that severe breaches cause a decrease in responsibility-taking language. However, this diverges from the assumption that organizations adopt a more conciliatory tone in severe crises (Coombs & Holladay, 2002). In summary, with this thesis I'm able to advance the understanding of responsibility-taking narratives adopted by organizations in crisis situations, such as data breach incidents, by demonstrating their responsiveness to consumer empowerment and the role of crisis severity. Nevertheless, this thesis also invites further investigation of the role of punitive consumer actions and the moderating role of severity in connection to crises and the narratives adopted in these situations.

## 6.2 Practical Implications

The practical implications this thesis offers, differ depending on the party.

The results underscore the findings of foregone studies that strengthened consumer power will lead organizations to recognize the growing importance of responsibility-taking narratives, illustrating how exogenous events can shape communication strategies (Coombs, 2007a; Nikkhah & Grover, 2022; Qin et al., 2024). Hence, the main implication for organizations here is that adopting transparent, accountable language in crisis scenarios, shouldn't be viewed merely to comply with legal requirements but goes beyond and concerns trust building and resilience among stakeholders. This aligns with the notion that accountability is vital for maintaining trust during crises. Responsibility-taking narratives, as suggested by SCCT (Coombs, 2007a), demonstrate organizational commitment to addressing consumer concerns and mitigating harm. Transparent communication about the scope of the crisis, remedial actions, and preventative measures aligns with stakeholder expectations (Freeman, 1984; Donaldson & Preston, 1995), fostering confidence in the organization's ability to manage challenges. Further research shows that clear communication and actions can reduce negative responses and help to maintain trust, although I wasn't able to corroborate this idea here (Hillenbrand et al., 2013, Auger, 2014). The implications of my findings explicitly go beyond consumers, by also entailing employee concerns, financial risks, and other community challenges. Hence, the universality of the implications presented here underscore the strategic importance of aligning organizational behavior with the principles of Stakeholder Theory (Freeman, 1984).

For investors, an organization's approach to handling crises provides insights into its governance quality and long-term risk management capabilities (Cavusoglu et al., 2004). Companies that proactively communicate responsibility demonstrate a higher commitment to ethical practices, which can reduce reputational damage and financial volatility (Kim et al., 2017). Clear disclosures about risks and corrective measures, supported by evidence of ethical practices, reinforce investor confidence and might even reduce financial uncertainty. As this thesis illustrates, narratives that emphasize resilience and proactive recovery align with stakeholder priorities and demonstrate organizational foresight (Ahmad et al., 2017; Nikkhah & Grover, 2022), which in the end allows possible interpretation of performance and investment opportunities for investors.

Policymakers play a crucial role in reinforcing accountability standards and addressing gaps in existing regulations. By tailoring regulations in a way that allows them to address the faults organizations might have in their communication approach towards their stakeholders, they are able to encourage responsibility-taking narratives, they can create an environment where organizations are motivated to prioritize stakeholder trust (Mulgund et al., 2021). The results presented here corroborate the notion of how such frameworks influence organizations to adopt responsibility-taking behaviors, ensuring transparency and proactive engagement (Mulgund et al., 2021). Policymakers can extend these principles across sectors, tailoring regulations to address crises affecting employees, communities, or even the environment. For example, requiring detailed disclosures or mandating stakeholder-centric policies can enhance trust and encourage ethical corporate behavior (Hosseini et al., 2024).

In conclusion, this thesis is able to bridge theory and practice, emphasizing the universal importance of transparency, accountability, and tailored engagement strategies in managing diverse stakeholder relationships, going beyond the mere consumer perspective.

### 6.3 Limitations and Further Research

Limitations of this thesis concern the generalizability of data sources, the methodology, the choice of lawsuits as a proxy for consumer punitive actions. Each aspect has implications for the robustness and applicability of the research outcomes but also opens ways for future exploration.

The California Attorney General's database provides a comprehensive overview of data breach incidents and their corresponding notifications and allows derivations, nevertheless one also encounters limitations. The database solely captures breaches affecting California residents and those meeting the reporting threshold, leaving out incidents in other jurisdictions or below the threshold. To enhance the generalizability of findings, particularly in cross-cultural and global contexts, incorporating data from other US-states or international databases could lead to a broader picture and might alter the findings. For instance, examining organizations operating under the European General Data Protection Regulation (GDPR) would provide insights into another jurisdiction that is often mentioned alongside the CCPA. The GDPR, regarded as one of the strictest global data protection laws, is comparable to the CCPA in its scope and the rights granted to the citizens influenced by the regulation (Van Nortwick & Wilson, 2022). While both regulations emphasize transparency and

accountability, the GDPR applies globally to entities handling EU citizens' data, with a focus on data minimization, privacy by design, and strict breach notification rules (GDPR, 2016, Arts. 5, 33–34). It mandates organizations to notify supervisory authorities within 72 hours of a breach unless the risk is minimal, and to inform affected individuals without undue delay if their rights are at high risk (GDPR, 2016, Arts. 33–34). In contrast, the CCPA is state-specific, prioritizing consumer empowerment and transparency for California residents while permitting broader data practices (Van Nortwick & Wilson, 2022). Studying the interplay between the GDPR and CCPA frameworks could illuminate both how companies in different parts of the world react to increased consumer power and how the same organization navigates differing regulatory landscapes. Such an approach would enhance understanding of data breach dynamics, offering more robust insights into the way international companies react to heightened consumer power in terms of adopting responsibility-taking narratives (De Hert & Papakonstantinou, 2016). In addition to that the database doesn't allow to easily distinguish between industries, which would allow for more complex analysis, hence allowing to introduce further control variables to the regression models. H1, which predicts stronger responsibility-taking narratives in response to strengthened consumer rights, might yield different results under alternative regulatory frameworks or industry specific contexts. In addition to industry, it might be illuminating to expand the scope of analysis to other variables in order to include organization-specific characteristics such as size, reputation, governance, profitability, HQ location, and prior breach history. Having access to such information and including them could provide further meaningful control variables and yield different or new results.

In terms of the methodology applied in this thesis there are a few points worth highlighting, when it comes to limitations. First, the analytical framework employs simplified proxies such as Company Responsibility, Consumer Responsibility and Responsibility Score to capture responsibility-taking narratives. While these proxies resulted to be effective for quantifying language, they may fail to capture subtle dynamics in communication, especially concerning the analysis of H1 and H3a. Future research could address this by employing more sophisticated linguistic analyses, such as sentiment analysis or topic modeling, to better understand the nuances of responsibility-taking narratives. Second, the measurement of breach severity could also be further refined. Severity in this thesis is assessed based on the type of compromised information. However, this approach isn't exhaustive of the broader implications of severity, for example whether the compromised information was misused or

not. For instance, H3a, which links breach severity to responsibility-taking, could be enhanced by including factors such as breach magnitude, duration, and the financial impact on affected individuals. Additionally, analyzing how organizations adjust their language and/ or narratives based on the severity and type of breached data could reveal patterns relevant to H3a and H3b. Furthermore, using lawsuits as the only measure of punitive consumer actions raises the question about generalizability. Class action lawsuits provide only a partial view of the consequences of data breaches, not taking into account broader impacts, such as customer churn, social media backlash, boycotts, and stock price fluctuations. For instance, H2 hypothesizes a negative relationship between responsibility-taking and punitive actions, but class action lawsuits may not fully capture these dynamics. Going beyond that further research might reveal differences between punitive actions employed by consumers, hence I advise to explore these alternative measures to develop a more comprehensive understanding of stakeholder responses. Incorporating other external factors like (social) media coverage, public sentiment, and other regulatory pressures could provide a richer understanding of variations in organization's behavior and stakeholder reactions.

By addressing these limitations, future research can provide a more nuanced understanding of the interplay between organizational communication, stakeholder reactions, and consumer power. Ultimately, this might help companies to develop more effective strategies for navigating crises, particularly data breach incidents.

### 6.4 Conclusion

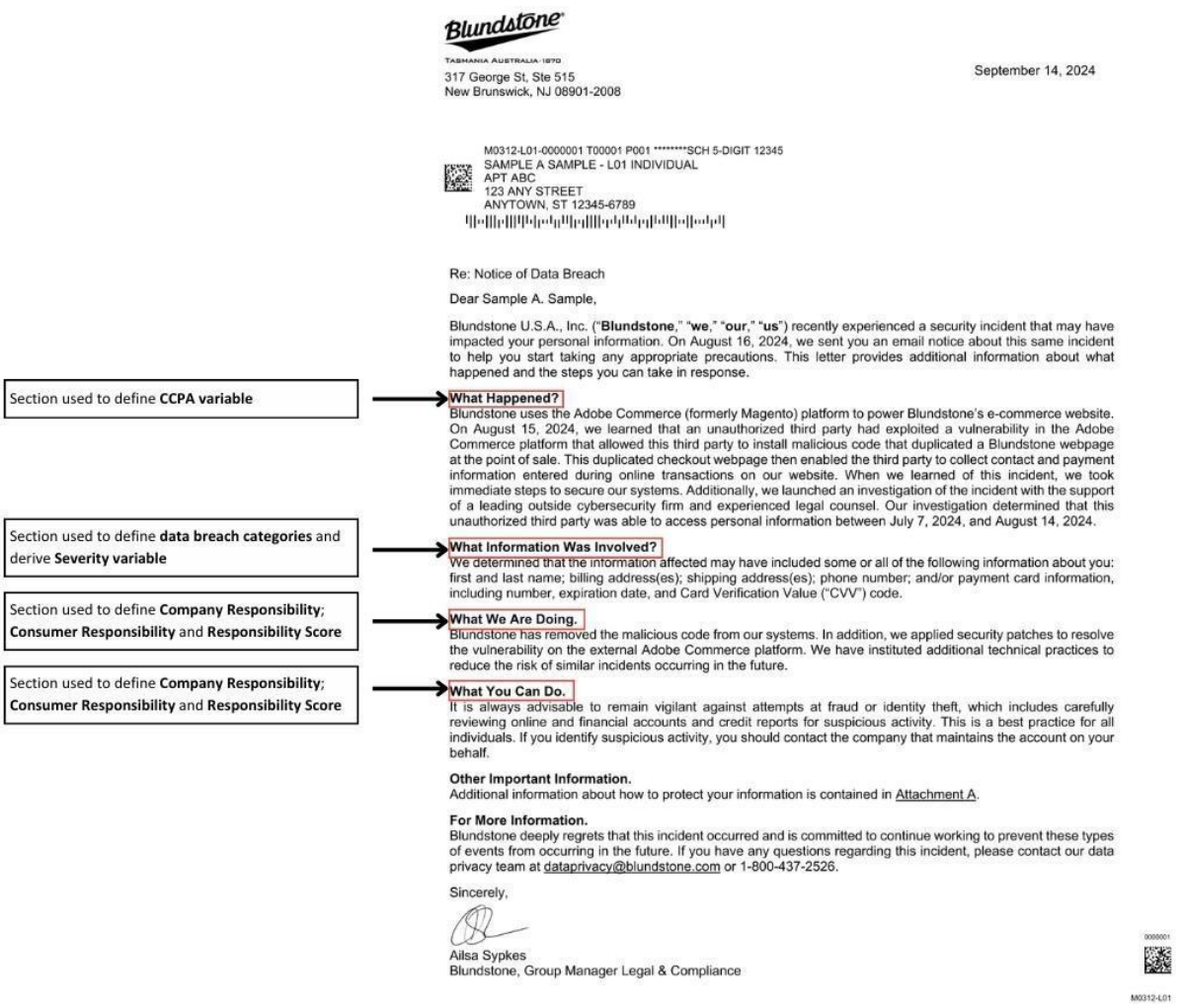
This thesis sought to answer how consumers' strengthened consumer rights influence organizations' responsibility-taking narratives following data breaches and whether these narratives reduce punitive consumer actions. By analyzing large-scale, longitudinal data and employing linguistic and statistical analysis, I demonstrated the influence of heightened consumer power through frameworks like the CCPA on organizational behavior in terms of assuming responsibility. However, while these narratives help rebuild trust and mitigate reputational harm (Coombs, 2007a, Qin et al., 2024), their impact on reducing punitive actions, such as class action lawsuits, remains inconclusive although previous research has conducted research with the effect being present (Hillenbrand et al., 2013; Auger, 2014). The moderating role of severity remains unclear according to my analysis. However, the findings also reveal that crisis severity and the type of compromised data affect responsibility-taking narratives.

This thesis contributes to the field by linking heightened consumer power through regulatory frameworks to corporate behavior, offering empirical evidence that strengthens the theoretical foundations of Stakeholder Theory (Freeman, 1984; Donaldson & Preston, 1995). Additionally, it enhances understanding of crisis communication, showing how responsibility-taking narratives are adapted based on crisis context and severity (Coombs & Holladay, 2002; Jin et al., 2007).

In conclusion, this thesis underscores the critical role of transparency, accountability, and tailored strategies in managing crises and maintaining stakeholder trust. By aligning narratives with stakeholder expectations, organizations can navigate crises effectively and foster resilience in an increasingly scrutinized business environment.

## Appendix A

**Figure 11**
*Excerpt from exemplary Data Breach Notification*




## Appendix B

**Figure 12:**
*Data Breach Types*

**Data breach types and associated keywords**

| Data Breach Type | Keywords associated |
|---|---|
| *Personal Identifiable Information (PII)* | Name, Address, Phone, Email, Gender, Date of Birth, Social Security |
| *Financial Information* | Credit Card, Debit Card, Bank Account, Loan Balance, Payment Card |
| *Authentication Credentials* | Username, Password, PIN, Login, Security Question |
| *Health and Medical Information* | Medical Record, Health Insurance, Diagnosis, Treatment |
| *Employment Information* | Employee ID, Employer, Taxpayer ID |
| *Government-Issued Identification* | Driver's License, Passport, State ID |
| *Digital Footprints* | IP Address, Geographic Location, Online Profile |
| *Sensitive Data* | Wage, Salary, Tax, Financial Transaction, Genotype |
| *Miscellaneous Data* | Insurance Policy, Health Plan, Membership ID, Benefit |
| *System and Account Metadata* | Account Type, Order History, Transaction History, Usage Data |

## List of abbreviations

CCPA..... California Consumer Privacy Act

DiD ..... Difference in Differences

DV ..... Dependent Variable
EVT ..... Expectancy Violation Theory
GDPR ..... General Data Protection Regulation
PoS..... Part-of-speech
SCCT .....Situational Crisis Communication Theory

**List of figures**

**List of tables**

## References

Ahmad, D. A. M. A., Ashari, N. M., & Samani, M. C. (2017). Effect of rational and emotional framing on highly involved audience in severe crisis situation: An experimental study on MH370. *Jurnal Komunikasi: Malaysian Journal of Communication, 33*(2), 89–104. https://doi.org/10.17576/JKMJC-2017-3302-07

Acquah, E., Ganapati, S., & Choi, Y.-J. (2024). Examining the effects of California Consumer Privacy Act (CCPA) on Organizational Data Breach Notification. *Proceedings of the 25th Annual International Conference on Digital Government Research,* 216–223. https://doi.org/10.1145/3657054.3657082

Afifi, W. A., & Metts, S. (1998). Characteristics and consequences of expectation violations in close relationships. *Journal of Social and Personal Relationships, 15*(3), 365–392.

Auger, G. A. (2014). Trust Me, Trust Me Not: An Experimental Analysis of the Effect of Transparency on Organizations. *Journal of Public Relations Research, 26*(4), 325–343. https://doi.org/10.1080/1062726X.2014.908722

Ayyagari, R. (2012). An Exploratory Analysis of Data Breaches from 2005-2011: Trends and Insights. *Journal of Information Privacy and Security*, *8*(2), 33–56. https://doi.org/10.1080/15536548.2012.10845654

Beyer, K., & Arnold, M. (2020). Circular approaches and business model innovations for social sustainability in the textile industry. In J. C. Bocken, P. Ritala, L. Albareda, & R. Verburg (Eds.), *Innovation for sustainability: Business transformations towards a better world* (pp. 341–373). Springer. https://doi.org/10.1007/978-3-030-22018-1_19

Bonnie, E. (2024, December 3). 110 of the Latest Data Breach Statistics [Updated 2024]. *Secureframe*. Retrieved December 8, 2024, from https://secureframe.com/blog/data-breach-statistics

Bowen, M., Freidank, J., Wannow, S., & Cavallone, M. (2018). Effect of Perceived Crisis Response on Consumers' Behavioral Intentions During a Company Scandal –

An Intercultural Perspective. *Journal of International Management, 24*(3), 222–237. https://doi.org/10.1016/j.intman.2017.12.001

Bryson, J. M. (2004). What to do when stakeholders matter: Stakeholder Identification and Analysis Techniques. *Public Management Review*, *6*(1), 21–53. https://doi.org/10.1080/14719030410001675722

California Civil Code § 1798.82, amended by Assembly Bill No. 2828, Chapter 337 (2023). https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.&part=4.&chapter=1.&article=

California Consumer Privacy Act of 2018, Assembly Bill No. 375, Chapter 55, codified as Cal. Civ. Code §§ 1798.100–1798.199 (2023). https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=1.&article=

Carre, J. R., Curtis, S. R., & Jones, D. N. (2018). Ascribing responsibility for online security and data breaches. *Managerial Auditing Journal*, *33*(4), 436–446. https://doi.org/10.1108/MAJ-11-2017-1693

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*, *9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Chatterjee, S., Gao, X., Sarkar, S., & Uzmanoglu, C. (2019). Reacting to the scope of a data breach: The differential role of fear and anger. *Journal of Business Research*,

*101*, 183–193. https://doi.org/10.1016/j.jbusres.2019.04.024

Chen, H. S., & Jai, T.-M. (Catherine). (2019). Cyber alarm: Determining the impacts of hotel's data breach messages. *International Journal of Hospitality Management*, *82*, 326–334. https://doi.org/10.1016/j.ijhm.2018.10.002

Choi, B. C. F., Kim, S. S., & Jiang, Z. (Jack). (2016). Influence of Firm's Recovery Endeavors upon Privacy Breach on Online Customer Behavior. *Journal of Management Information Systems*, *33*(3), 904–933. https://doi.org/10.1080/07421222.2015.1138375

ClassAction.org. (2024, December 10). *Class action lawsuits and settlements: Stay informed and get legal help*. Retrieved December 14, 2024 from https://www.classaction.org/

Coombs, W. T., & Holladay, S. J. (2002). Helping Crisis Managers Protect Reputational Assets: Initial Tests of the Situational Crisis Communication Theory. *Management Communication Quarterly*, *16*(2), 165–186. https://doi.org/10.1177/089331802237233

Coombs, W. T. (2004). Impact of Past Crises on Current Crisis Communication: Insights From Situational Crisis Communication Theory. *Journal of Business Communication*, *41*(3), 265–289. https://doi.org/10.1177/0021943604265607

Coombs, W. T. (2007a). Attribution Theory as a guide for post-crisis communication research. *Public Relations Review*, *33*(2), 135–139. https://doi.org/10.1016/j.pubrev.2006.11.016

Coombs, W. T. (2007b). Protecting organization reputations during a crisis: The development and application of situational crisis communication theory. *Corporate Reputation Review, 10*(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review*, *32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

Diers-Lawson, A., Symons, A., & Zeng, C. (2021). Building crisis capacity with data breaches: The role of stakeholder relationship management and strategic communication. *Corporate Communications: An International Journal*, *26*(4), 675–699. https://doi.org/10.1108/CCIJ-02-2021-0024

Donaldson, T., & Preston, L. E. (1995). The Stakeholder Theory of the Corporation: Concepts, Evidence, and Implications. *The Academy of Management Review*, *20*(1), 65. https://doi.org/10.2307/258887

Druckman, J. N. (2001). The Implications of Framing Effects for Citizen Competence. *Political Behavior*, *23*(3), 225–256.

Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Cambridge University Press.

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & De Colle, S. (2010). *Stakeholder theory: The state of the art*. Cambridge University Press.

Gupta, M., McGowan, D., & Ongena, S. R. G. (2023). The Cost of Privacy. The Impact of the California Consumer Protection Act on Mortgage Markets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4404636

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems*, *35*(2), 683–714. https://doi.org/10.1080/07421222.2018.1451962

Hegner, S. M., Beldad, A. D., & Kraesgenberg, A.-L. (2016). The Impact of Crisis Response Strategy, Crisis Type, and Corporate Social Responsibility on Post-crisis Consumer Trust and Purchase Intention. *Corporate Reputation Review*, *19*(4), 357–370. https://doi.org/10.1057/s41299-016-0007-y

Hillenbrand, C., Money, K., & Ghobadian, A. (2013). Unpacking the Mechanism by which Corporate Responsibility Impacts Stakeholder Relationships. *British Journal of Management*, *24*(1), 127–146. https://doi.org/10.1111/j.1467-8551.2011.00794.x

Hosseini, H., Utz, C., Degeling, M., & Hupperich, T. (2024). A Bilingual Longitudinal Analysis of Privacy Policies Measuring the Impacts of the GDPR and the CCPA/CPRA. *Proceedings on Privacy Enhancing Technologies*, *2024*(2), 434–463. https://doi.org/10.56553/popets-2024-0058

IBM. (2024). *Cost of a data breach report 2024*. Retrieved October 23, 2024, from https://www.ibm.com/reports/data-breach

Jamali, D. (2008). A Stakeholder Approach to Corporate Social Responsibility: A Fresh Perspective into Theory and Practice. *Journal of Business Ethics*, *82*(1), 213–231. https://doi.org/10.1007/s10551-007-9572-4

Jin, Y., Pang, A., Cameron, G.T., 2007. Integrated crisis mapping: Toward a publics-based, emotion-driven conceptualization in crisis communication. *Sphera Publica. 7*, 81–96.

Jurcys, P., & Lampinen, M. (2020). Principles of Data Privacy in California: Study of Industry Reactions and Comments to the Proposed CCPA Regulations and User-Centric Perspectives. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3601948

Kelly, C. (2005). Data security: A new concern for PR practitioners. *Public Relations Quarterly, 50*(2), 25–26.

Kim, B., Johnson, K., & Park, S.-Y. (2017). Lessons from the five data breaches: Analyzing framed crisis response strategies and crisis severity. *Cogent Business & Management, 4*(1), 1354525. https://doi.org/10.1080/23311975.2017.1354525

Klein, J., & Dawar, N. (2004). Corporate social responsibility and consumers' attributions and brand evaluations in a product–harm crisis. *International Journal of Research in Marketing, 21*(3), 203–217. https://doi.org/10.1016/j.ijresmar.2003.12.003

Kuipers, S., & Schonheit, M. (2022). Data breaches and effective crisis communication: A comparative analysis of corporate reputational crises. *Corporate Reputation Review, 25*(3), 176–197. https://doi.org/10.1057/s41299-021-00121-9

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing, 81*(1), 36–58. https://doi.org/10.1509/jm.15.0497

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a Theory of Stakeholder Identification and Salience: Defining the Principle of Who and What Really Counts. *The Academy of Management Review, 22*(4), 853-886. https://doi.org/10.2307/259247

Marantz, A. (2020). *Understanding sentences – NYU MorphLab*. Retrieved January 2, 2025 from https://wp.nyu.edu/morphlab/2020/06/23/understanding-sentences-part-1/

Mulgund, P., Mulgund, B. P., Sharman, R., & Singh, R. (2021). The implications of the California Consumer Privacy Act (CCPA) on healthcare organizations: Lessons learned from early compliance experiences. *Health Policy and Technology*, *10*(3), 100543. https://doi.org/10.1016/j.hlpt.2021.100543

Navarro, G., Baeza-Yates, R., Sutinen, E., & Tarhio, J. (2001). Indexing Methods for Approximate String Matching. *IEEE Data Engineering Bulletin*, *24*(4), 19–27.

Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). Data breaches in healthcare: Security mechanisms for attack mitigation. *Cluster Computing*, *27*(7), 8639–8654. https://doi.org/10.1007/s10586-024-04507-2

Nikkhah, H. & Grover, V. (2022). An Empirical Investigation of Company Response to Data Breaches. *MIS Quarterly*, *46*(4), 2163–2196. https://doi.org/10.25300/MISQ/2022/16609

Qin, M. S., Luo, X., Schifeling, T., & Wang, Y. (2024). When corporate silence is costly: Negative consumer responses to corporate silence on social issues. *Strategic Management Journal*, 1–33. https://doi.org/10.1002/smj.3683

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (2016). Official Journal, L 119, 1-88. ELI: http://data.europa.eu/eli/reg/2016/679/oj

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical Analysis of Data Breach Litigation. *Journal of Empirical Legal Studies*, *11*(1), 74–104. https://doi.org/10.1111/jels.12035

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, Organization, and Crisis. *Annals of the International Communication Association*, *21*(1), 231–276. https://doi.org/10.1080/23808985.1998.11678952

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *Journal of Strategic Information Systems*, *28*(3), 257–274. https://doi.org/10.1016/j.jsis.2018.12.001

State of California Department of Justice, Office of the Attorney General. (n.d.). *State of California Department of Justice, Office of the Attorney General.* Retrieved December 14, 2024, from https://oag.ca.gov/

Statista. (2024). *Number of data breaches worldwide from 2005 to first half 2023*. Retrieved December 7, 2024, from https://www.statista.com/statistics/1307426/number-of-data-breaches-worldwide/

Trujillo, N., & Toth, E. L. (1987). Organizational Perspectives for Public Relations Research and Practice. *Management Communication Quarterly*, *1*(2), 199–231. https://doi.org/10.1177/0893318987001002004

Van Nortwick, M., & Wilson, C. (2022). Setting the Bar Low: Are Websites Complying With the Minimum Requirements of the CCPA? *Proceedings on Privacy Enhancing Technologies, 2022*(1), 608–628. https://doi.org/10.2478/popets-2022-0030

Wang, Y., & Wanjek, L. (2018). How to Fix a Lie? The Formation of Volkswagen's Post-crisis Reputation Among the German Public. *Corporate Reputation Review*, *21*(2), 84–100. https://doi.org/10.1057/s41299-018-0045-8

Wartick, S. L. (1992). The relationship between intense media exposure and change in corporate reputation. *Business & Society*, *31*(1), 33–49. https://doi.org/10.1177/000765039203100104.

Weiner, B. (1985). An Attributional Theory of Achievement Motivation and Emotion. *Psychological Review*, *92*(4), 548–573.

Weiner, B. (1986). *An attributional theory of motivation and emotion*. Springer-Verlag.

Williams, C. C. (2005). Trust Diffusion: The Effect of Interpersonal Trust on Structure, Function, and Organizational Transparency. *Business & Society*, *44*(3), 357–368. https://doi.org/10.1177/0007650305275299

Zhao, X., Zhan, M., & Jie, C. (2018). Examining multiplicity and dynamics of publics' crisis narratives with large-scale Twitter data. *Public Relations Review*, *44*(4), 619–632. https://doi.org/10.1016/j.pubrev.2018.07.004