Corporate Data Transparency

Xin Meng, Arpita Gupta, Tanisha Rahim, Justin Li, Jason Greenberg, Neha Keshan

December 16, 2025

1 Abstract

Data breaches represent a growing threat to us all as consumers. Our privacy concerns lie on the companies who seek to generate the most profit possible. These corporations lack responsibility and accountability yet play an ever-increasing pivotal role in our lives. This paper examines this problem through a case study of the 2024 Ticketmaster data breach. The company's response, widely criticized for delayed disclosure and prioritizing investor relations over consumer protection, highlights systemic failures in the current regulatory environment. We find that the FTC lacks a specific and enforceable national standard. Financial compensation for victims is not required by law and frequently must be addressed in court instead. We conclude that this fragmented system fails to protect consumers.

Building on this diagnosis, we propose a federal baseline policy: (1) automatic, real-time notification of breaches to regulators and users, (2) a strict two-week deadline for detailed disclosure to all affected users, and (3) mandatory user compensation tied to a fixed percentage of the company's prior-year revenue, with a broad and evolving definition of "personal information." This framework is intended to simplify compliance, close loopholes in state-by-state rules, and realign incentives toward accountability and transparency.
Link to our github: https://github.com/Tanishar254/FinalTechReport-Data-and-Society.git

2 The Problem Summary

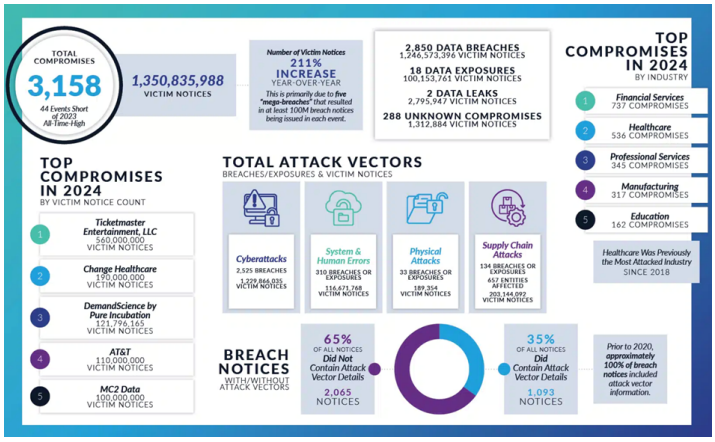

Figure 1: Data breaches in 2024

As shown by figure [1] below, data breaches have become increasingly common and harmful, yet little to no protection is provided for consumers by the government. This is due to breach-notification laws that vary widely between states and the lack of a unified federal standard for these issues. This allows companies to delay disclosure, provide incomplete information, or avoid notifying users altogether by exploiting vague definitions such as "substantial loss." The FTC, while able to punish deceptive security practices, has no explicit authority to enforce a national disclosure timeline or require compensation for affected consumers. This fragmented system leaves millions of consumers vulnerable, uninformed,

and typically uncompensated after their personal information is exposed. This is the problem that we are looking to tackle.

3 Policy Proposal: A National Standard for Data Breach Transparency and Compensation

We considered the problem described above in its depth and breadth, and conducted further research. Based on the weaknesses revealed by our findings about the Ticketmaster data breach and the broader regulatory landscape, we propose a concrete federal policy framework with three main pillars: real-time disclosure, strict timelines for user notification, and mandatory user compensation tied to corporate revenue.

3.1 Automatic Real-Time Notification

Our first recommendation is that breach notification should be built into corporate software systems as an automatic process rather than an ad hoc decision. Specifically:

- As soon as a company detects unauthorized access or signs of hacking into systems containing personal information, it must automatically notify the FTC in real time.
- Users should receive an initial alert (maybe labeled as a potential security incident) as soon as the breach is detected, even if some details are still under investigation.

This would reduce the risk that companies quietly delay disclosure while they assess reputational risk or legal exposure. It also ensures that regulators see incidents as they unfold rather than weeks or months later.

3.2 Two-Week Deadline for Detailed User Notice

Our second recommendation is a strict upper bound on the time companies have to provide full details about the data breach to users. We propose a maximum of 14 days from the date of the breach detection for companies to notify every affected user with:

- What data categories were exposed
- The time window of exposure
- Known or suspected misuse
- Concrete steps the user can take (e.g., credit monitoring, password changes, etc.).

3.3 Revenue-Based User Compensation Rule

Our third recommendation is a simple, scalable compensation formula:

- If there is loss of personal information, the company must set aside 0.015 percent of its previous fiscal year's revenue, to be split among all affected users.

This ties liability to the size and resources of the company, rather than a fixed dollar amount per user. A large company with billions in revenue cannot treat breaches as trivial fines; a smaller company faces a lower absolute liability, but still meaningful relative to its size. The more revenue a company generates from user data, the more it stands to lose from failing to protect the data. Class-action lawsuits and regulatory settlements could still increase compensation in extreme cases (e.g., intentional misconduct), but they would no longer be the only way victims receive any monetary redress.

3.4 Evolving Definition of Personal Information

Our policy starts with a broad baseline definition of the term "personal information" and allows for expansion over time through federal rulings and case law. Initially, personal information would encompass at least:

- Full name
- Date of birth
- Social security number
- Phone number, email address, additional contact information
- Residential Address
- Financial information (payment cards, bank details, transaction histories)
- Health-related information

As new classes of sensitive data become central to digital life such as biometric data, geo-location histories, or behavioral profiles, the definition can be expanded by regulation or precedent from case law. This avoids locking in a narrow definition that quickly becomes outdated.

3.5 Nationwide Rule

Finally, we propose that this policy suggestion function as a nationwide baseline. States could still pass stricter rules (e.g., higher compensation percentages, shorter deadlines, etc) but no state could undercut this federal standard. We decided on a nationwide policy because many companies currently follow the strictest state's rules. Hence, our policy cements that practice and sets a baseline for protecting users.

Today, companies informally follow the strictest state laws regardless of the users impacted, in order to avoid missing compliance requirements and reduce risk; but this approach is not transparent to users. A unified federal baseline would simplify compliance for companies operating in all 50 states. It would reduce confusion for users about their rights and close loopholes where companies exploit weaker state definitions of phrases like "substantial loss" or notification exceptions.

4 Case Study: The 2024 Ticketmaster Data Breach

In May 2024, Ticketmaster, a major online ticket marketplace, detected unauthorized activity in a third-party cloud database containing customer data [6]. The breach, which occurred from early April to mid-May, was only noticed by the public after a group called ShinyHunters later claimed responsibility. They claimed that they allegedly have 560 million user data and asked for a 500,000 dollar ransom for it [8]. Ticketmaster publicly disclosed the incident on May 31, 2024, after the hackers had already made it public.

4.1 Timeline of Detection and Disclosure

Our analysis of public reports and Ticketmaster's own disclosures shows a problematic sequence:

- Early April – Mid-May 2024: Early Detection Ticketmaster detected unauthorized access in a third-party cloud database that stored sensitive customer information and launched a forensic investigation. At this point, regulators and law enforcement were notified, but users were not yet informed.
- Mid-May 2024: Internal Escalation As the investigation confirmed that personal data had likely been accessed at scale, the company continued working with incident-response teams and outside experts. However, details about the scope and the affected population remained opaque to the public.

- Late May 2024: Hacker Group Claims Responsibility The hacker group ShinyHunters publicly claimed responsibility and advertised the stolen data for sale. This meant that malicious actors learned about the breach before many of the actual victims did.
- After May 31, 2024: Official Notice and Delayed User Alerts Ticketmaster's first major public communication focused on investor disclosures and regulatory filings rather than user-facing transparency. User notification emails did not roll out until late July 2024—roughly two months after the breach was confirmed—despite the high stakes for affected consumers.

4.2 How Ticketmaster Handled It and the Feedback

Ticketmaster faced backlash for its slow, investor-focused response and lack of transparency about the breach's impact. Customers were frustrated by the lack of transparency, while cybersecurity experts criticized the company's weak protection and detection. Its limited public statements and claims that the breach had no "material impact" appeared dismissive of consumer concerns. Consequently, a class-action lawsuit was filed against Live Nation Entertainment, Ticketmaster's parent company, for failing to protect user data and promptly disclose the breach. The incident ultimately eroded public trust and became a cautionary example of how delayed disclosure and poor accountability can escalate a security lapse into a reputational crisis.

4.3 Connection to Proposal

Together, these shortcomings illustrate why stronger federal standards are urgently needed. Inconsistencies in disclosure timelines, the absence of required user compensation, and the lack of clear enforcement authority all contribute to an environment in which companies can prioritize their legal and financial interests over the security and the benefit of their users. The 2024 Ticketmaster breach provides a concrete example of how these gaps play out in practice.

5 Federal Disclosure Timeline

Data breaches have become too common. Oftentimes, they're large scale and can impact many people from a variety of locations. Laws are not one-size-fits-all, so the regulations that apply to a data breach typically depend on which state the users reside in. All 50 states in the US have laws requiring private businesses to notify individuals of security breaches of information involving personally identifiable information [7]. 19 out of 50 states have a section in their legislation specifying when notification of a data breach is NOT required [5]. Due to the loose definitions, the state to state law leaves a lot of gray areas up for corporate exploitation. This carve-out is a core part of the problem. Because "substantial loss" is vague and interpreted differently, corporations have room to argue that notification is unnecessary even when sensitive data has been exposed. Combined with state-by-state timelines and thresholds, this creates a patchwork of rules that is hard for consumers to understand and easy for corporations to exploit.

Companies may delay notifying users while they conduct internal investigations, consult legal teams, or weigh reputational risk. As a result, users often learn about breaches through news reports or hacker forums rather than from the company holding their data. Our Ticketmaster case study demonstrates how this ambiguity translates into real-world harm.

6 FTC Regulation

The Federal Trade Commission (FTC) is the main agency to protect consumers from deceptive business acts. Under the FTC Act (15 U.S.C. §§ 41–58), it can punish companies that lie about how they protect user data or fail to keep data safe. However, this law is very general and has no fixed rule about when or how companies must tell users after a data breach [4]. Each state now has its own timeline, so large firms often follow a complex mixture of state rules. In practice, many companies default to whichever state has the strictest requirements to minimize legal risk, but this is still a reactive strategy rather than a proactive, user-centric standard. Because there is no single federal disclosure clock, companies can still delay notifying users while staying technically compliant.

Our analysis of FTC enforcement and guidance shows that the agency can punish "weak or misleading data-security" practices and deceptive statements about security, but it lacks explicit authority to enforce a uniform breach-notification timeline. This gap is one of the central motivations for our policy proposal: giving the FTC a clear mandate to enforce a national disclosure standard that is faster, clearer, and focused on user protection rather than corporate convenience.

7 Federal User Compensation

There are no federal regulation requiring companies to provide user compensation in the case of a data breach. The FTC and the SEC only require companies to notify their users about a security breach and to be transparent about the situation [7]. User compensation is provided in a case by case situation, specifically when a class action lawsuit is filed or during a regulatory settlement.

A well-known example is the Equifax data breach settlement [2]. In 2017, Equifax announced a breach that affected 147 million people. In 2019, the company agreed to a global settlement with the FTC and other agencies, providing up to 425 million dollars to those who were affected. While this sounds large, the per-person compensation was modest and took years of legal and administrative work to deliver [3].

The absence of a federal baseline requirement for compensation means that:

- Many victims never receive any meaningful remediation.
- Companies treat compensation as a legal and PR bargaining chip rather than a predictable cost of failing to protect user data.
- Outcomes vary widely between cases, depending on the strength of legal representation, the visibility of the breach, and the company's willingness to settle.

This reactive, litigation-driven system is neither efficient nor fair. It also fails to create strong ex-ante incentives for companies to invest in robust security and transparent disclosure.

8 Current Updates

We examined the 2024 Ticketmaster breach and how the company responded and communicated with their users. We reviewed state breach-notification laws, FTC enforcement, and SEC disclosure rules to map current timelines. We assessed whether any federal law mandates consumer compensation completed a focused review of FTC regulation.

Since our mid-term report, we extended this analysis into a fully fleshed-out policy recommendation. This included specifying exact disclosure timelines (real-time alerts plus a two-week detailed notice window) and a quantitative compensation formula (0.015 percent of prior-year revenue) to translate abstract "fair compensation" into an enforceable rule.

Additionally, we tracked the ongoing Ticketmaster case and observed that Live Nation has still not clearly disclosed the total number of users affected. This ongoing opacity further reinforced our view that voluntary corporate transparency is not sufficient and must be backed by binding federal standards.

9 Issues Handled

When it came to understanding legal jargon, we used generative AI tools to help us unpack statutes, agency guidance, and case law. For complex class-action lawsuits, reading plain-language summaries before diving into the full opinions made the content more manageable. Additionally, because there was a scarcity of straightforward sources—especially on corporate disclosure decisions that companies prefer to downplay—we had to dig into regulatory filings, news coverage, and technical reports.

10 Hurdles Facing

The legal language used in the documents we researched is dense and hard to understand. Statutory definitions, exemptions, and cross-references required significant effort to interpret correctly. Researching class-action lawsuits was similarly complex: it was often unclear how compensation was defined, negotiated, and ultimately distributed to affected consumers.

Furthermore, there is a scarcity of transparent corporate disclosures. Many firms minimize public documentation of breaches to avoid negative publicity, which limits access to reliable data on timelines, decision processes, and internal deliberations. Live Nation's reluctance to provide a precise count of affected users in the Ticketmaster breach is one concrete example of this opacity.

Designing a simple yet robust federal policy in this context required us to constantly balance legal realism with the need for clarity and enforceability.

11 Expected Results

Initially, we expected to find a clear federal rule that defined what "fair compensation" should look like for users affected by data breaches. Instead, we discovered that no such standard exists. Compensation is determined case by case through class-action lawsuits or regulatory settlements, and these outcomes vary widely in both amount and accessibility. We also anticipated some variation among state laws, but our research showed that the differences are far greater than we had assumed. These differences include notification timelines, harm thresholds, and the basic definition of personal information, which creates confusion for users and inconsistency in how companies respond to breaches.

These findings reinforced the need for a simple and predictable national standard. Without a unified federal rule, companies are able to delay notifications or disclose only limited information while still remaining technically compliant. We expect that implementing our proposed policy, which includes real-time alerts, a strict two-week deadline for detailed disclosure, and revenue-based compensation, would reduce ambiguity and improve both corporate accountability and user protection. Overall, our results confirm that a nationwide framework would provide clearer expectations for companies and stronger safeguards for consumers in every state.

12 Takeaways and Future Plans

Our main takeaway is that the current U.S. approach to data breach regulation is reactive, fragmented, and ultimately misaligned with consumer protection. The Ticketmaster case showed us how easily corporations can comply with the "letter" of state-level rules while still withholding timely, meaningful information from users. Going forward, we hope to refine our proposed federal baseline by examining how different compensation percentages and disclosure timelines would affect firms of various sizes, possibly using simple economic or simulation models. We are also interested in exploring how our framework could be integrated with broader data privacy legislation, such as federal rules on data minimization or data retention. Finally, a key future step is to connect policy design with public education, developing accessible materials that help everyday users understand their rights, recognize breach notifications, and take action when their data is exposed.

13 Collaboration with Other Groups

We collaborated with group 1 who focused on corporate responsibility in handling data. Our discussions centered on how much room there is for malpractice when companies collect and process user data at scale. Their perspective reinforced the idea that "compliance on paper" is not enough when corporate incentives are misaligned.

Additionally, we worked with group 8 who explored the extent to which individuals truly "own" their data online. A key insight was that when you browse or post content, much of the data you "leak" is not legally considered yours anymore. This raised deeper questions about what it means to compensate "owners" of data when the law often treats that data as a corporate asset.

Finally, we work with group 10 who worked on integrating education about data rights and current events into school curriculum. Our conversations highlighted that fragmented policy is only part of the problem; the other part is lack of public awareness. Even the best laws are less effective if everyday users do not understand their rights or how to respond to breaches.

These collaborations helped us situate our policy proposal within a broader ecosystem: corporate governance, digital ownership, and public education. It also strengthened the interdisciplinary case for a federal baseline on data breach transparency and user compensation.

14 Use of Generative AI Tools

Our group used generative AI tools in a limited and clearly defined way to support the writing and research process. Specifically, we used AI to help us clarify and interpret complex legal language from statutes, FTC guidelines, and class-action lawsuits so that we could understand these materials more effectively. We also used AI to help improve grammar, readability, and structural flow in the draft sections of the report, as well as to help outline the policy proposal before writing the final version ourselves. Importantly, we did not use AI to generate research findings, create or fabricate citations, or replace our independent analysis. All factual claims and references in this report were manually researched, reviewed, and created by group members.

15 Group Contributions

Tanisha: : I did the research for the federal user compensation (Section 7) and presented that section. I helped my team flesh out our policy recommendation(section 3). I led the writing in the overleaf report, and contributed to the project experience section such as issues handled(section 9) and takeaways and future plans(section 12). Also, I helped divide work, schedule meetings and kept group moving forward to meet the deadline.

Arpita: I researched, presented, and wrote about the company disclosure and notification timelines (Section 5). Based on this information, I led the creation of our policy recommendation and wrote it out in the report (Section 3). I also led the presentation slides and presentation practice and worked with Tanisha to divide work, schedule meetings, get team members to engage, and kept the group moving forward to meet the deadline.

Xin: I created the Overleaf project for the group to ensure consistent formatting and collaboration. Specifically, I focused on researching and writing on FTC regulations (Section 6) and current updates (Section 8) to our analysis. I also helped to draft and improve Expected Results (Section 11), as well as the paragraph describing our use of generative AI tools (Section 14). In addition, I formatted and standardized the references to meet the required style guidelines. Furthermore, I also implement the acknowledgement (Section 16) as well.

Justin: I worked on the case study part as well as the general formatting of the Overleaf document. More specifically, I did the research and the summary of the case study on Ticketmaster (Section 4), as well as the write-up on how it relates to our proposed solution. I also wrote the problem summary of our group (Section 2), as well as keeping the formatting of the document consistent.

Jason: I was working on the group collaboration slides as well as the information in the report (Section 13). My group did a great job of reaching out and communicating with the other groups, which, once they gave me all that information, I was able to come to conclusions about our work together and how our ideas among groups are similar and rely on each other.

16 Acknowledgment

This work was completed as part of a course project at Rensselaer Polytechnic Institute. We would like to thank our teaching assistant for guidance and feedback throughout the semester. We also thank our classmates for their helpful discussions, questions, and suggestions during presentations and peer review sessions, which contributed to the development of this work.

References

[1] Center, I.T.R.: the fraudian slip podcast: Identity theft resource center – itrc publication on 2024 data breaches highlights eye-opening findings. https://www.idtheftcenter.org/podcast/fraudian-slip-2024-data-breaches/ (May 2025), accessed: November 17, 2025

[2] Consumer Financial Protection Bureau: Cfpb, ftc, and states announce settlement with equifax over 2017 data breach (July 22 2019), https://www.consumerfinance.gov/about-us/newsroom/cfpb-ftc-states-announce-settlement-with-equifax-over-2017-data-breach/, accessed: November 9, 2025

[3] Federal Trade Commission: Equifax data breach settlement: What you should know (January 2024), https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement, accessed: November 9, 2025

[4] Federal Trade Commission: Ftc act: The antitrust laws (2024), https://www.ftc.gov/advice-guidance/competition-guidance/guide-antitrust-laws/antitrust-laws, accessed: November 9, 2025

[5] IT Governance USA Inc: Data breach notification laws by state (2024), https://www.itgovernanceusa.com/data-breach-notification-laws, accessed: November 7, 2025

[6] Law, B.: Snowflake at t: Ticketmaster sued over infostealer breach. Bloomberg Law (2024), https://news.bloomberglaw.com/privacy-and-data-security/snowflake-at-t-ticketmaster-sued-over-infostealer-breach?context=search&index=0, accessed: November 9, 2025

[7] National Conference of State Legislatures: Security breach notification laws (September 29 2023), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws, accessed: November 9, 2025

[8] News, B.: Hackers claim theft of ticketmaster data affecting millions. BBC News (2024), https://www.bbc.com/news/articles/c899pz84d8zo, accessed: November 9, 2025