Cost of a Data Breach Report 2024

Executive Summary

Prepared for Financial Organsiatons

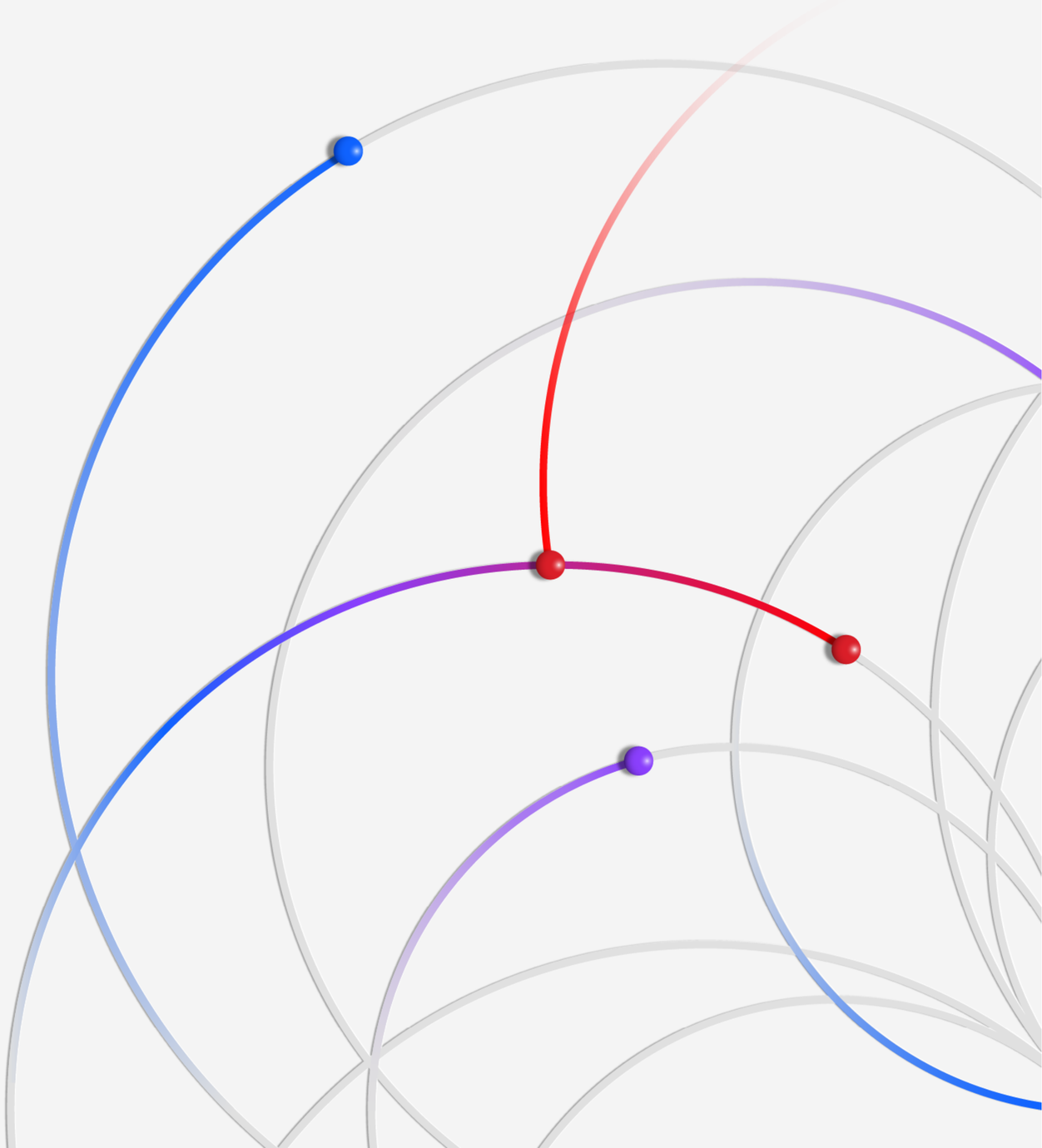


Table of contents

01

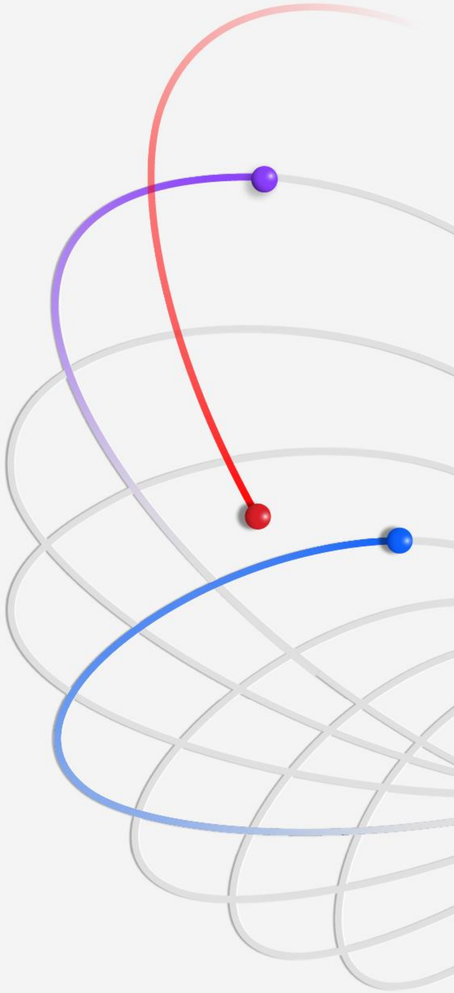
Executive summary

IBM's annual Cost of a Data Breach Report provides IT, risk management and security leaders with timely, quantifiable evidence to guide them in their strategic decision-making. It also helps them better manage their risk profiles and security investments. This year's report—the 19th of the series—reflects changes caused by technological shifts, such as the rise of shadow data, which is data residing in unmanaged data sources, and the extent and costs of business disruption brought about by data breaches.

The report's research—conducted independently by Ponemon Institute and sponsored, analyzed and published by IBM—studied 604 organizations impacted by data breaches between March 2023 and February 2024. Researchers looked at organizations across 17 industries, in 16 countries and regions, and breaches that ranged from 2,100 to 113,000 compromised records. To gain on-the-ground insights, Ponemon Institute researchers interviewed 3,556 security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations.

The result is a benchmark report that business and security leaders can use to strengthen their security defenses and drive innovation, particularly around the adoption of AI in security and security for their generative AI (gen AI) initiatives.

We lead this year's report with 2 major developments. First, the global average cost of a data breach increased 10% over the previous year, reaching USD 4.88 million, the biggest jump since the pandemic. Business disruption and post-breach customer support and remediation drove this cost spike. When asked how they're dealing with these costs, more than half of organizations said they are passing them on to customers. Having customers absorb these costs can be problematic in a competitive market already facing pricing pressures from inflation.



Second, on the defender side of the equation, researchers also found applying security AI and automation is paying off, lowering breach costs in some instances by an average of USD 2.2 million. AI and automation solutions are reducing the lifespan needed to identify and contain a breach and its resulting damage. Put another way, defenders without AI and automation to assist them can expect to take longer to detect and contain a breach, and see costs rise compared to those who use these solutions.

As we've seen across the industry, cybersecurity teams are consistently understaffed. This year's study found more than half of breached organizations faced severe security staffing shortages, a skills gap that increased by double digits from the previous year. This lack of trained security staff is growing as the threat landscape widens. The continuing race to adopt gen AI across nearly every function in the organization is expected to bring with it unprecedented risks and put even more pressure on these cybersecurity teams.

This report provides insights and recommendations from the research to help reduce the potential financial and reputational damages from a data breach.

What's new in the 2024 report

Each year, we continue to evolve the Cost of a Data Breach Report to match new technologies, emerging tactics and recent events. For the first time, this year's research explores:

- Whether companies experienced operational disruption, for example, the inability to process sales orders, a complete shutdown of production facilities, ineffective customer services
- Whether the breach included data stored in unmanaged data sources, otherwise known as shadow data
- To what extent companies are using AI and automation in each of 4 areas of security operations: prevention, detection, investigation and response
- The nature of extortion attacks, for example, extortion and ransomware attacks or extortion and data exfiltration only
- What the mean time was to identify and contain data breaches, as well as to restore data, systems, or services to their pre-breach state
- How long it took companies to report the breach if they were mandated to do so
- Whether organizations that involved law enforcement following a ransomware attack paid the ransom

02

Key findings

The key findings described here are based on IBM analysis of research data compiled by Ponemon Institute.

USD 4.88M

Average total cost of a breach

The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs totaled USD 2.8 million, the highest combined amount for lost business and post-breach activities over the past 6 years.

USD 2.2M

Cost savings from extensive use of AI and automation in prevention

2 out of 3 organizations studied stated they're deploying security AI and automation across their security operations center, a 10% jump from the prior year. When deployed extensively across prevention workflows—attack surface management (ASM), red-teaming and posture management—organizations averaged USD 2.2 million less in breach costs compared to those with no AI use in prevention workflows. This finding was the largest cost savings revealed in the 2024 report.

26.2%

Growth of the cyber skills shortage

More than half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2% increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. Even as 1 in 5 organizations say they used some form of gen AI security tools—which are expected to help close the gap by boosting productivity and efficiency—this skills gap remains a challenge.

Key findings

1 in 3

Share of breaches involving shadow data

35% of breaches involved shadow data, showing the proliferation of data is making it harder to track and safeguard. Shadow data theft correlated to a 16% greater cost of a breach. Researchers found storing data across environments proved to be a common storage strategy, accounting for 40% of breaches. These breaches also took longer to identify and contain. In contrast, data stored in just 1 type of environment was breached less often, whether that environment was public cloud (25%), on premises (20%) or private cloud (15%).

USD 4.99M

Average cost of a malicious insider attack

Compared to other vectors, malicious insider attacks resulted in the highest costs, averaging USD 4.99 million. Among other expensive attack vectors were business email compromise, phishing, social engineering and stolen or compromised credentials. Gen AI may be playing a role in creating some of these phishing attacks. For example, gen AI makes it easier than ever for even non-English speakers to produce grammatically correct and plausible phishing messages.

46%

Share of breaches involving customer personal data

Nearly half of all breaches involved customer personal identifiable information (PII), which can include tax identification (ID) numbers, emails, phone numbers and home addresses. Intellectual property (IP) records came in a close second (43% of breaches). The cost of IP records jumped considerably from last year, to USD 173 per record in this year's study from USD 156 per record in last year's report.

Key findings

USD 1M

Cost savings when law enforcement is involved in ransomware attacks

Two-thirds of organizations that suffered ransomware attacks and involved law enforcement didn't pay the ransom. Those organizations also ended up lowering the cost of the attack by an average of nearly USD 1 million, when excluding the cost of any ransom paid. Involving law enforcement also helped shorten the time required to identify and contain breaches from 297 days to 281 days.

292

Days to identify and contain breaches involving stolen credentials

Breaches involving stolen or compromised credentials took the longest to identify and contain (292 days) of any attack vector. Similar attacks that involved taking advantage of employees and employee access also took a long time to resolve. For example, phishing attacks lasted an average of 261 days, while social engineering attacks took an average of 257 days.

USD 830,000

Largest average cost increase among all industries

The industrial sector experienced the costliest increase of any industry, rising by an average USD 830,000 per breach over last year. This cost spike could reflect the need for industrial organizations to prepare for a more rapid response, as organizations in this sector are highly sensitive to operational downtime. Still, the time to identify and contain a data breach at industrial organizations was above the median industry, at 199 days to identify and 73 days to contain.

Average cost of a data breach in the **financial industry**

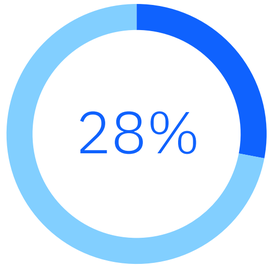
USD 6.08M

2nd highest cost
of 17 industries
studied

22% higher than
the USD 4.88M
global average

3% higher
compared
to 2023

Key statistics

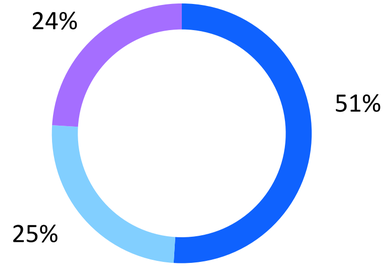


Percentage of financial organizations with extensive use of security AI and automation

USD 1.9M

Cost savings of extensive use of security AI and automation versus no security AI and automation

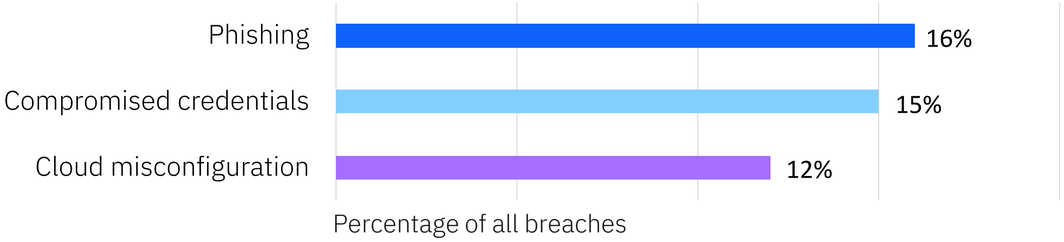
Root causes of a data breach



Malicious attack | IT failure | Human error

Global highlights

Top 3 initial attack vectors



USD 375M

Average total cost of a breach of > 50M records

USD 4.91M

Average cost of a ransomware-related breach

Time to identify and contain

Financial industry

Global average

USD 248K

Average cost savings with incident response (IR) teams and testing versus no IR teams or testing

USD 223K

Average cost savings with identity and access management (IAM) strategy that support hybrid environment and user experience

03

Recommendations to help reduce the cost of a data breach

Our recommendations include successful security approaches that are associated with reduced costs and lower times to identify and contain breaches.

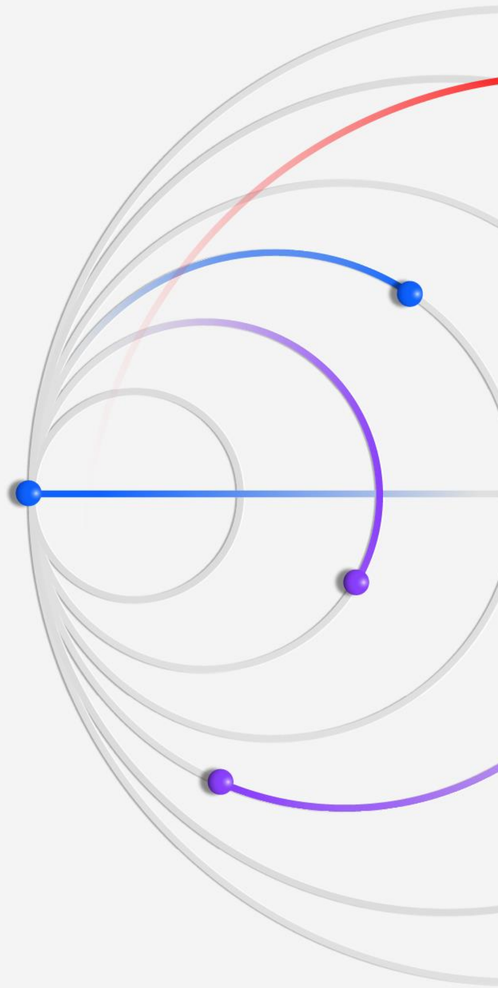
Know your information landscape

Most organizations distribute data across multiple environments, including on-premises data repositories, private clouds and public clouds. However, many organizations have incomplete or out-of-date data inventories, delaying efforts to discover what data has been breached and how sensitive or confidential it is. These delays can complicate the response and raise the cost of a breach.

Security teams should ensure they have comprehensive visibility into all these environments, so they can continuously monitor and protect data regardless of where it resides. Organizations can apply data security posture management (DSPM) and other solutions, such as identity access management and ASM, across all these environments for consistent and comprehensive protection.

Security teams must pay extra attention to hybrid environments and public clouds. 40% of data breaches involved data stored across multiple environments, and when breached data was stored in public clouds, it incurred the highest average breach cost at USD 5.17 million. It’s imperative security teams gain a deeper understanding of the specific risks and controls for each cloud service they employ.

Managing data across environments becomes further complicated by the impact of unmanaged data. More than one-third of data breaches involve shadow data. Security teams must now assume their organizations have unmanaged data sources. Unencrypted data, including data in AI workloads, further exacerbates the risk. Data encryption strategies must consider the types of data, its use and where it resides to lower risk in case of a breach.



Strengthen prevention strategies with AI and automation

The adoption of gen AI models and third-party applications across the organization—as well as the ongoing use of Internet of Things (IoT) devices and SaaS applications—are expanding the attack surface, putting pressure on security teams.

Applying AI and automation that support security prevention strategies—including in the areas of ASM, red-teaming and posture management—can often be addressed by managed security services. Organizations that applied AI and automation to security prevention saw the biggest impact from their AI investments in this year's study compared to 3 other security areas: detection, investigation and response. They saved an average of USD 2.22 million over those organizations that didn't deploy AI in prevention technologies.

Take a security-first approach to gen AI adoption

While organizations are moving quickly ahead with gen AI, only 24% of gen AI initiatives are being secured. The lack of security threatens to expose data and data models to breaches, potentially undermining the benefits that gen AI projects are intended to deliver.

As gen AI adoption continues to scale, organizations need a framework for securing gen AI data, models and usage, along with establishing AI governance controls. They'll need to secure the training data by protecting it from theft and manipulation. Organizations can use data discovery and classification to detect sensitive data used in training or fine-tuning. They can also implement data security controls across encryption, access management and compliance monitoring.

With gen AI, not only are organizations faced with the risk of, and growth in, shadow data, but also shadow models. Organizations must extend posture management to the AI models themselves to protect sensitive AI training data, gain visibility into the use of unsanctioned or shadow AI models, and AI misuse or data leakage.

Securing gen AI model development requires scanning for vulnerabilities in the pipeline, hardening integrations, and enforcing policies and access. To secure the use of gen AI models requires security teams to monitor for malicious inputs, such as prompt injections, and outputs containing sensitive data. They must also deploy AI security solutions that can detect and respond to AI-specific attacks, such as data poisoning, model evasion and model extraction. Developing response playbooks to deny access, and quarantine and disconnect compromised models is essential as well.

Level up your cyber response training

How an organization reacts and communicates during and after a breach—with business leadership, regulators and customers—matters more than ever. 75% of the increase in average breach costs in this year's study was driven by the cost of lost business, including downtime, lost customers and orders, and acquiring new customers. Also included were post-breach response activities, such as setting up a customer help desk, offering credit monitoring to affected customers and paying regulatory fines. The lesson: investing in post-breach response preparedness can help lower data breach costs.

Organizations must supplement technical response capabilities with strategic planning to cover business impact, protect customers and maintain operational continuity. Building governance and making decisions ahead of time can help executives foresee the handling of major business disruption and streamline actions that will benefit the organization in case of an attack.

To enhance their ability to handle high-impact attacks, organizations can build up their muscle memory for breach responses by participating in cyber range crisis simulation exercises. These exercises can include security teams as well as business leaders, so the entire organization improves its ability to detect, contain and respond to breaches. Security leaders should work with their business functions across the organization and communications teams ahead of time to draft response plans and test them. With threat landscapes expanding because of gen AI and other IT initiatives, security training needs to be offered to non-security practitioners. These practitioners include data scientists and data engineers working in machine learning and AI teams and those tasked with continuity of AI workloads across on-premises and cloud assets.

By investing in response preparedness, organizations can help reduce the costly, disruptive effects of data breaches, support operational continuity and help preserve their relationships with customers, partners and other key stakeholders. Moreover, rehearsed response reassures employees and reduces stress, distress and friction internally as the acute stages of an attack are handled, controlled and communicated by a well-prepared leadership team.

04

About IBM and Ponemon Institute

Ponemon Institute
Founded in 2002, Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high-quality empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

Ponemon Institute upholds strict data confidentiality, privacy and ethical research standards and doesn't collect any personally identifiable information (PII) from individuals or company-identifiable information in business research. Furthermore, strict quality standards ensure subjects aren't asked extraneous, irrelevant or improper questions.

If you have questions or comments about this research report, including requests for permission to cite or reproduce the report, contact us by letter, phone call or email:

Ponemon Institute LLC
Research Department
1-800-887-3118
research@ponemon.org

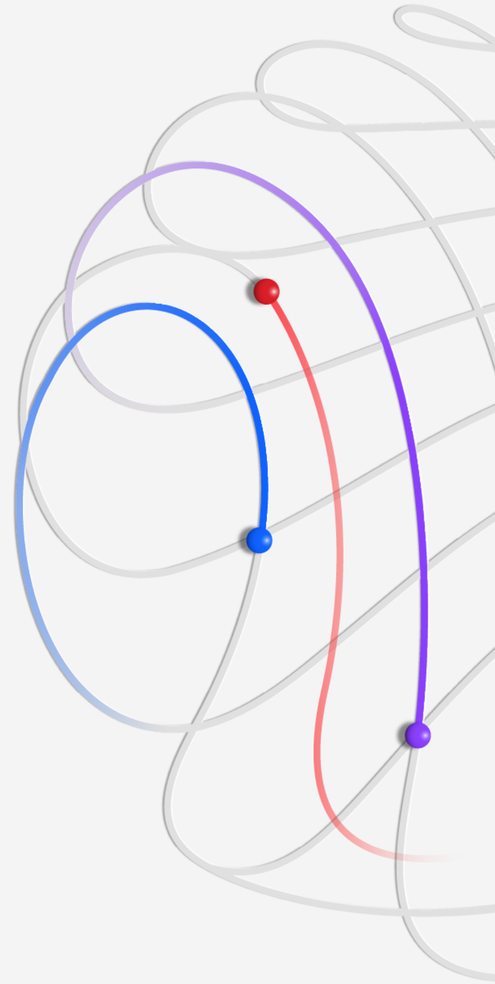
IBM
IBM is a leading global hybrid cloud, AI and business services provider, helping clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs and gain the competitive edge in their industries. All of it is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service. For more information, visit www.ibm.com.

Learn more about advancing your security posture:

Visit ibm.com/security

Join the conversation in the IBM Security Community

Contact your IBM representative to learn more: info@northdoor.co.uk



Thank you

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2024