JANUARY 2024

ITRC | IDENTITY THEFT RESOURCE CENTER

2023 DATA BREACH REPORT

idtheftcenter.org • 1-888-400-5530

Table of Contents

A Letter from the CEO

On July 1, 2003, the world's first law that required consumers to be notified their personal information had been compromised in a data breach went into effect in California. The law only applied to residents of the Golden State and it was primarily aimed at the risk of the time – the exposure of personal information stored in filing cabinets and on disks and drives. Dumpster diving and stolen laptops were the top sources of breaches.

While many businesses were aware of the new law and the need to inform California residents of a loss of their personally identifiable information (PII), most consumers were not. Especially outside California.

That all changed in 2005 when a Georgia-based company sent letters to a small group of California consumers alerting them that their PII had been obtained by a group of organized criminals posing as legitimate businesses. On Valentine's Day, "Data Breach Notice" appeared in the popular lexicon for the first time.

That original notice not only generated intense interest in California, but around the world. Major media outlets in the U.S. and Europe covered the story each day for 30 days and Congress held a series of hearings on the topic of data breaches. Soon, consumers outside California were informed they, too, may have been the victim of the data breach in recognition that criminals and data did not recognize state lines.

By the end of 2005, 156 other organizations had issued breach notices tracked by the ITRC and a handful of states adopted a California-style breach notice law. Fast forward to 2018 when the final two states adopted breach notice requirements, following the lead of 90 other countries, all U.S. territories, and the District of Columbia.

However, Congress did not enact a federal breach notice law. Even in the wake of a single 2017 data breach linked to a Nation/State that compromised the personal information of nearly every adult in the U.S. and millions of adults in other countries. The result was a patchwork of state laws and federal regulations with different definitions of PII, triggers for a notice, methods of notification, time frames for issuing a notice, and penalties for failing to issue a notice.

In the years between 2005 and 2018, technology advanced and identity criminals' skills improved. Paper documents in file cabinets accessible in locked rooms were replaced by cloud environments accessible via the internet. Identity criminals shifted from lone individuals hacking for fun and street cred in their parents' basement to highly sophisticated groups operating out of glass and stone towers in far-away lands. Hollywood shows us people in hoodies while the real identity criminals flash cash, drive Lambos and operate call centers.

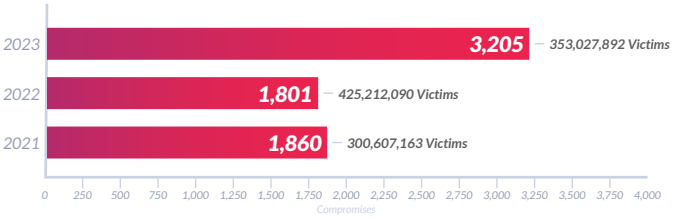
Off-the-shelf hacker tools lowered the barrier to entry for launching attacks and the wealth of personal information available from data breaches and identity scams made it easy to impersonate an individual or business using social engineering. This was the environment in 2021 that created the highest number of data compromises ever tracked by the ITRC – 1,860[1] events impacted an estimated ~300M victims.

The highest, that is, until 2023.

In the pages that follow you'll see the new record high: 3,205 publicly reported data compromises that impacted an estimated 353,027,892 individuals. That's a 72 percent (72%) increase in events over the previous high-water mark and 78 percent (78%) over 2022.

See Figure 1

Figure 1 | *Total Compromises, Year over Year*



Each year we are asked "why the increase in events?" and "what can be done to protect against a data breach?" There's never any one reason why compromises go up or down just as there are no actions that are 100 percent effective in stopping breaches or the identity crimes that result. We do believe there are trends that need to be highlighted and actions that need to be considered if we are to slow or stop the pace of data breaches and exposures.

First, we must acknowledge the significant impact of Supply Chain Attacks and the effect they have on all organizations. A single supply chain attack can directly or indirectly impact hundreds or thousands of businesses that rely on the same vendor. Stronger reporting requirements can help warn other vulnerable businesses of the risk associated with a similar attack. Increased due diligence when it comes to vendors and data protection are also in order.

Second, the two-decade old legislative and regulatory framework designed to alert consumers to breaches is broken. A Supply Chain Attack victim from 2020 confirmed in 2023 what was suspected for years: Businesses under or non-report breaches. We need to bring a level of uniformity to the breach notice process to help protect both consumers and business.

The sheer scale of the 2023 data compromises is overwhelming. Just the increase from the past record high to 2023's number is larger than the annual number of events from 2005 until 2020 (except for 2017). But, we cannot let complacency, frustration, or weariness lead us to surrender the fight to protect identity crime victims. We're not about to give-up or give-in and we hope you will join us as we seek to start a different conversation about protecting identities in 2024.

Eva Velasquez, *CEO*

Identity Theft Resource Center
January 2024

[1]*Audits of 2021 and 2022 compromises resulted in a reduction in the total number of data compromises for those years due to breaches originally reported as separate events later being updated as related events. The total number of compromises in full-year 2021 has been adjusted downward by two (2) events to 1,860 and full-year 2022 adjusted downward by one (1) event to 1,801.*

Glossary of Terms

One of the issues that leads to confusion around data compromises is the fact there is no single definition or set of terms used to describe a data breach that requires a notice in the U.S. Since data breach notices are largely creatures of state law, there are as many definitions and trigger events as there are states, territories and federal districts. Adding to the confusion, Federal government agencies also have their own set of terms and requirements for issuing a data breach notice, many of which have recently changed or are in the process of changing. (See SEC, FTC and FCC rule changes announced in 2023.)

Since 2020, the ITRC has published the definitions we use in compiling and publishing this report. We have updated our terms for the 2023 report.

Data Compromise – The overall term used to refer to events where personal information is accessible by unauthorized individuals and/or for unintended purposes. This includes data breaches, data exposures, and data leaks.

Data Breach – When unauthorized individuals access and/or remove personal information from the place where is it stored.

Data Exposure – When personal information is available for access and/or removal from the place where it is stored, but there is no evidence the information has been accessed by unauthorized individuals. This typically involves cloud-based data storage where cybersecurity protections are incorrectly configured or have not been applied.

Data Leak – When personal information that is publicly available or willingly shared on social media and represents no or low risk when viewed as individual records; however, when aggregated, the sheer volume of personal information available in a single database creates risk to the data subjects and value for identity criminals who specialize in social engineering and phishing. When these databases are left unprotected or otherwise made publicly available, the ITRC classifies these events as Data Leaks.

Identity Crimes – The overall term for a wide variety of state and federal criminal acts that are related to the theft and/or misuse of personal information.

Identity Theft – Taking personally identifiable information (PII) as protected by state or federal laws.

Identity Fraud – Using stolen personally identifiable information (PII).

2023 DATA BREACH REPORT

idtheftcenter.org • 1-888-400-5530

The *Annual Data Breach Report* explores a dramatic increase in reported data compromises and the underlying trends behind the growth. 2023 represented an all-time high for data compromises reported in the United States.

ITRC | IDENTITY THEFT RESOURCE CENTER

Total Compromises in 2023

3,205
TOTAL COMPROMISES

353,027,892
TOTAL VICTIMS

3,122 DATA BREACHES
349,221,481 VICTIMS

25 DATA EXPOSURES
960,700 VICTIMS

2 DATA LEAKS
2,696,728 VICTIMS

56 UNKNOWN COMPROMISES
148,983 VICTIMS

1,400+
PUBLIC DATA BREACH NOTICES
*Did **Not** Contain Information about an Attack Vector*

*This Number Has Nearly **Doubled** Year-Over-Year*

+72 TOTAL COMPROMISES
72 Percentage Point Increase
from All-Time-High in 2021

-16 TOTAL VICTIM COUNT
16 Percentage Point Decrease
from 2022

Top 5 Compromises by Victim Count

T-MOBILE
37,000,000 VICTIMS IMPACTED

XFINITY
35,879,455 VICTIMS IMPACTED

PEOPLECONNECT, INC.
20,221,007 VICTIMS IMPACTED

NATIONSTAR MORTGAGE LLC
14,690,284 VICTIMS IMPACTED

PBI RESEARCH SERVICES – MOVEIT TRANSFER
11,781,156 VICTIMS IMPACTED

Supply Chain Attacks on the Rise

Impacting More Organizations and Victims in 2023

Organizations Impacted Since 2018
+2,600
PERCENTAGE POINTS

Estimated Number of Victims Since 2018
+1,400
PERCENTAGE POINTS

Total Attack Vectors

CYBERATTACKS
2,365 Breaches | 343,338,964 Victims

SYSTEM AND HUMAN ERRORS
729 Breaches/Exposures | 6,715,385 Victims

PHYSICAL ATTACKS
53 Breaches/Exposures | 127,832 Victims

SUPPLY CHAIN ATTACKS
242 Breaches/Exposures | 2,769 Entities Affected
54,432,431 Victims

Top Compromises by Industry

HEALTHCARE	*809 Compromises*
FINANCIAL SERVICES	*744 Compromises*
PROFESSIONAL SERVICES	*308 Compromises*
MANUFACTURING	*259 Compromises*
EDUCATION	*173 Compromises*

Executive Summary

Analysis – 2023 vs 2022

The number of data compromises reported in the United States surpassed two significant milestones in 2023: the highest number of data events reported in a single year and exceeding 2,000 (and ultimately 3,000) events in a single year. The total number of data breaches, exposures, leaks and unspecified events reached 3,205, impacting an estimated 353,027,892 victims, including those affected by multiple compromises. The 2023 compromises represent a 78 percentage point increase over the previous year and a 72 percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

The estimated number of victims impacted represents a 16 percentage point reduction from 2022, when more than half of the total annual victim count was related to three breaches announced late in the previous year. This is consistent with a general trend of the number of estimated victims dropping slightly each year. This is a result of organized identity criminals focusing on specific information and identity-related fraud and scams rather than mass attacks.

Based on publicly reported compromises, the total number of compromises reflects a trend where most industries saw increases, and a handful saw slight decreases in reported attacks. However, three (3) industries reported more than double the number of compromises compared to 2022: Healthcare, Financial Services and Transportation.

Healthcare led all industries in terms of the number of reported compromises in each of the past five (5) years, but Utilities companies led in the estimated number of victims in 2023.

More than nine percent (9%) of the ~3,700 U.S. publicly traded companies issued a data breach notice in 2023, impacting ~143M victims. The 358 notices from publicly traded companies represented 11 percent (11%) of the overall number of compromises. Yet, public companies accounted for 40 percent (40%) of all data compromise victims. That compares to 2,847 data events at all other organizations, impacting ~210M victims during the course of the year.

Analysis of the breach notices also indicated that public companies were more likely to withhold actionable information about their data breach than other entities. Publicly traded companies withheld information about an attack in 47 percent (47%) of notices compared to 46 percent (46%) of private companies, government agencies, education institutions and nonprofit organizations.

As in each of the past five (5) years, the vast majority of data compromises were linked to cyberattacks in 2023. Phishing-related and ransomware attacks were down slightly, while malware and Zero Day attacks jumped significantly compared to previous years.

Compromises related to System and Human errors more than tripled in 2023, led by a 590 percent (590%) increase in data being exposed in emails and correspondence. Breaches involving a physical action – loss of a document, device theft, skimming devices – were relatively flat with single-digit increases. Physical breaches are down 65 percent (65%) since 2018.

The trend toward opaque breach notices discussed in the *2022 ITRC Data Breach Report* accelerated in 2023. The number of breach notices without specific information about the root cause of an attack nearly doubled year-over-year. In the 12 months that just ended, more than 1,400 public breach notices did not contain information about an attack vector compared to 716 in 2022 – a 98 percentage point increase.

Trends in 2023

Two clear trends emerged in 2023 beyond the dramatic rise in overall data compromises: 1) an equally dramatic increase in the number of organizations being impacted by Supply Chain Attacks, and 2) a trend highlighted by the rise in Supply Chain Attacks – the further break-down in the breach notification framework.

Trend 1: Supply Chain Attacks Grow

While the growth in the number of organizations targeted in Supply Chain Attacks has been relatively slow since 2018, the number of organizations impacted has surged by more than 2,600 percent (2,600%) over the same time period. The estimated number of victims has also surged to more than 54M victims, or 15 percent (15%) of the overall number of victims in 2023.

Trend 2: Underlying Flaw in Data Breach Notice Laws

The rise in Supply Chain Attacks where the breached entity may not own the data that is stolen has called into question who is responsible for making the determination of risk and notifying victims of the compromise. The 2020 Supply Chain Attack against Blackbaud illustrates the issues surrounding notification and highlights the fact breaches are under-reported.

According to a settlement agreement reached in late 2023 with 49 state attorneys general, Blackbaud notified more than 13,000 customers about the data breach and the loss of their data but did not notify the individual victims whose personal information was exposed.

Of the 13,000 Blackbaud customers impacted by the breach, only 604 organizations filed public notices tracked by the ITRC, representing an estimated 12.8M victims. The gap between the thousands of organizations that lost data and the hundreds who notified victims is a clear indicator that data breach notice laws and regulations have failed to achieve the original goal of protecting businesses and individuals.

Solutions

The combination of more data from more compromises, along with revolutionary technology, means we must consider significant changes to how we protect personal information and respond when it is compromised. There are three areas where the ITRC suggests action that will help reduce the rate and impact of data breaches on individual and business victims.

Uniform Breach Notice Laws

In the 20 years since California's first-of-its-kind data breach notice law went into effect, nearly 19,000 data breaches have been publicly reported in the United States. In the U.S., there were an average of ~12 (12.3) data breaches reported each business day in 2023, while in the European Union, there were an average of 912 compromises reported each business day in 2022; the last year data was available.

The current patchwork of 50 state laws and expanded federal regulations makes compliance difficult and expensive for businesses. Individual victims (as well as businesses vulnerable to a similar attack) increasingly receive no notice or notices with little or no actionable information.

The ITRC believes that state data breach laws and federal agency regulations can be more helpful to victims by adopting uniform provisions.

Digital Credentials & Facial Comparison Systems

Trillions of U.S. dollars were pumped into the economy in the form of enhanced government cash benefits in 2020 and 2021 to support businesses and individuals during the pandemic. Professional threat actors and their more opportunistic criminal counterparts began to systematically apply for pandemic relief benefits. Identity verification processes used to open and access accounts were no match for the volume or scale of legitimate and illegitimate applications for assistance.

As an organization that operates the largest repository of U.S. data breach information, the ITRC immediately recognized that data alone could no longer be trusted as the sole source of truth about a person's identity in most processes. The ITRC concluded that the expanded use of facial verification and digital credentials is crucial to reducing the number of identity crimes involving the use of stolen personal information.

Facial identity verification is not the same as the controversial facial recognition. The use of a facial biometric as part of a comprehensive identity verification process provides a low-risk, equitable way to help ensure the authenticity of an applicant while lowering the overall value of compromised personally identifiable information to bad actors.

Additionally, given that many legacy identity verification solutions rely on credit data – which does not work well for individuals with little to no credit history – these biometric tools can help reach individuals who might otherwise be excluded from the ability to remotely verify their identity online.

Improve Vendor Due Diligence

Nearly a dozen states have adopted comprehensive state privacy laws, most of which also include some form of cyber risk assessment. Given the rise in Supply Chain Attacks identified earlier in this report, understanding the risk represented by vendors is imperative. Knowing both the breach history of an organization and being able to verify that history is a key to proper due diligence on current and future suppliers. So is knowing when a vendor or a vendors vendor issues a data breach notice.

The ITRC will soon launch a due diligence and alert tool that allows organizations to comply with state and federal requirements to understand the risks within their supply chains. Known as Breach Alert for Business (BA4B), this service will be available for a low annual fee directly from the ITRC. Submit your interest in BA4B by emailing dorinda@idtheftcenter.org.

2023 Analysis

+ *Year-Over-Year*
  - *Compromises and Victims*
  - *Sensitive vs Non-Sensitive Data*
  - *Actionable vs Non-Actionable Notices*
+ *Top 10 Compromises in 2023*
+ *Total Annual Compromises*

The number of data compromises[2] reported in the U.S. surpassed two significant milestones in 2023: the highest number of data events reported in a single year and exceeding 2,000 (and ultimately 3,000) events in a single year.

Year-Over-Year

Compromises and Victims

The estimated number of victims impacted represents a 16 percent (16%) reduction from 2022, when more than half of the total annual victim count was related to three breaches announced late in the previous year. This is consistent with a general trend of the number of estimated victims dropping slightly each year. This is a result of organized identity criminals focusing on specific information and identity-related fraud and scams rather than mass attacks.

See Figure 2

Figure 2 | *Total Compromises, Year-Over-Year*

	Compromises	Victims
2023	3,205	353,027,892
2022	1,801	425,212,090
2021	1,860	300,607,163
2020	1,108	310,235,204
2019	1,279	883,558,186
2018	1,175	2,227,849,622

Statistical information is slow to develop, but cybersecurity researchers increasingly point to anecdotal evidence of identity criminals pairing stolen personal information with Generative AI tools. The result is highly effective phishing and social engineering attacks that target specific businesses or individuals rather than the traditional phishing lures that were riddled with grammar errors and launched with little knowledge of who was receiving the message.

Based on publicly reported compromises, the total number of compromises reflects a trend where most industries saw increases, and a handful saw slight decreases in reported attacks. However, three (3) industries reported more than double the number of compromises compared to 2022: Healthcare, Financial Services and Transportation.

[2]*The ITRC uses the generic term data compromises to describe the various ways personal information is at risk as a result of a cyberattack, system or human error or physical attack. See our Glossary for more information.*

Healthcare led all industries in terms of the number of reported compromises in each of the past five (5) years. However, Utilities companies led in the estimated number of victims in 2023.

See Figure 3

Figure 3 | *Compromises by Industry, Year-Over-Year*

	2023		2022	
	Compromises	Victims	Compromises	Victims
Education	173	~4M	99	~2M
Financial Services	744	~61M	269	~27M
Government	100	~15M	74	~2M
Healthcare	809	~56M	343	~28M
Hospitality	45	~6M	34	~70M
HR/Staffing	10	~239K	–	–
Manufacturing	259	~5M	249	~24M
Mining/Construction	71	~222K	–	–
Non-Profit/NGO	105	~10M	72	~1M
Professional Services	308	~30M	223	~6M
Retail	119	~10M	65	~798K
Social Services	15	~193K	–	–
Technology	167	~65M	87	~249M
Transportation	101	~12M	36	~4M
Utilities	44	~73M	–	–
Wholesale Trade	53	~297K	–	–
Other	81	~4M	250	~12M
Unknown	1	0	–	–
Totals	**3,205**	**~353M**	**1,801**	**~425M**

Sensitive vs Non-Sensitive Data

In late 2023, the U.S. Securities and Exchange Commission adopted new rules for public companies regarding the disclosure of material cyber events, including data breaches. In anticipation of the new regulations, the ITRC added a field to identify an entity as a public or private organization. This additional information pointed to some stark contrasts between how publicly traded and other entities respond to data compromises.

For example, more than nine percent (9%) of the ~3,700 U.S. publicly traded companies issued a data breach notice in 2023, impacting ~143M victims. The 358 notices from publicly traded companies represented 11 percent (11%) of the overall number of compromises. Yet, public companies accounted for 40 percent (40%) of all data compromise victims. That compares to 2,847 data events at all other organizations impacting ~210M victims during the course of the year.

Analysis of the breach notices also indicated that public companies were more likely to withhold actionable information about their data breach than other entities. Public companies withheld information about an attack in 47 percent (47%) of notices compared to 46 percent (46%) of private companies, government agencies, educational institutions and nonprofit organizations.

See Figure 4

Figure 4 | *Public Compromises & Victims, 2023*

	Compromises	Victims
Public	358	143,027,616
Other Entities*	2,847	210,000,276
Total	**3,205**	**353,027,892**

**Other entities include private businesses, government agencies, non-profit organizations, schools, colleges and universities, and other non-publicly traded institutions.*

Compromises involving sensitive personal information remained the most common type of breach in 2023. The number of attacks involving only sensitive information dropped by 10 percentage points but increased in absolute terms in 2023 compared to the previous year. That's because the number of organizations that did not provide information about the nature of the compromised information grew by 3.5x in real terms and doubled in percentage.

See Figure 5

Figure 5 | *Sensitive vs Non-Sensitive Records, Year-Over-Year*

	Compromises Involving Sensitive Records	Percentage	Compromises Involving Non-Sensitive Records	Percentage	Compromises Involving Unknown Records	Percentage
2023	2,427	76%	121	4%	657	20%
2022	1,555	86%	77	4%	169	10%
2021	1,557	84%	116	6%	191	10%
2020	875	79%	118	11%	115	10%
2019	1,089	85%	122	10%	68	5%
2018	1,014	86%	108	9%	53	5%

Actionable vs Non-Actionable Notices

As in each of the past five (5) years, the vast majority of data compromises were linked to cyberattacks in 2023. Based on notices that provide information about the root cause of an attack, Phishing-related and ransomware attacks were down slightly, while Malware and Zero Day attacks jumped significantly compared to previous years.

Compromises related to System and Human errors more than tripled in 2023, led by a 590 percent (590%) increase in data being exposed in emails and correspondence. Breaches involving a physical action – loss of a document, device theft, skimming devices – were relatively flat with single-digit increases. Physical breaches are down 65 percent (65%) since 2018.

See Figure 6

However, the trend toward opaque breach notices discussed in the 2022 ITRC Data Breach Report accelerated in 2023. The number of breach notices without specific information about the root cause of an attack nearly doubled year-over-year. In the 12 months just ended, more than 1,400 public breach notices did not contain information about an attack vector compared to 716 in 2022 – a 98 percent (98%) increase.

Since 2020, the percentage of notices with actionable information that can help companies and individuals take precautions against cyberattacks has dropped from ~100 percent (100%) to 54 percent (54%).

See Figure 7

Figure 6 | *Attack Vectors, Year-Over-Year*

	2023	2022	2021	2020	2019	2018
Cyberattacks	**2,365**	**1,584**	**1,611**	**877**	**928**	**754**
Phishing/Smishing/BEC	438	467	537	383	490	379
Ransomware	246	293	353	159	83	53
Malware	118	73	141	103	112	102
Non-Secured Cloud Environment	14	10	24	51	15	15
Credential Stuffing	29	18	14	17	3	10
Unpatched Software Flaw	–	–	4	3	3	–
Zero Data Attack	110	8	4	1	–	–
Other	30	17	424	159	223	195
Not Specified	1,380	698	110	1	–	–
System & Human Error	**729**	**163**	**179**	**153**	**231**	**261**
Failure to Configure Cloud Security	25	18	54	58	56	49
Correspondence (Email/Letter)	380	55	66	55	89	121
Misconfigured Firewall	19	30	13	4	4	29
Lost Device/Document	53	7	12	5	19	17
Other	220	36	34	31	63	45
Not Specified	32	17	–	–	–	–
Physical Attacks	**53**	**46**	**51**	**78**	**118**	**152**
Document Theft	6	7	9	15	19	25
Device Theft	23	21	17	30	57	57
Improper Disposal	5	5	5	11	14	21
Skimming Device	9	6	1	5	4	12
Other	5	6	19	17	24	37
Not Specified	5	1	–	–	–	–
Data Leak	**2**	–	**7**	–	–	–
Unknown	**56**	**8**	**12**	–	**2**	**8**

Figure 7 | *Actionable vs Non-Actionable Notices, 2023*

	Compromises	Notices with Victim Count and Attack Vector Details	%	Notices with Victim Count and Attack Vector	%	Notices with Victim Count	%
2023	3,205	1,732	54%	1,321	41%	2,540	79%
2022	1,801	1,077	60%	694	39%	1,188	66%
2021	1,860	1,738	93%	1,078	58%	1,134	61%
2020	1,108	1,107	100%	663	60%	665	60%
2019	1,279	1,277	100%	917	72%	918	72%
2018	1,175	1,163	99%	681	58%	685	58%

Top 10 Compromises of 2023

Here are the Top 10 Compromises in 2023. For more information on compromises in 2023 and all compromises of past years, see the Appendix.

Figure 8 | *Top 10 Compromises, 2023*

	Compromises	Victims Impacted
1	T-Mobile	37,000,000
2	Xfinity	35,879,455
3	PeopleConnect, Inc.	20,221,007
4	Nationstar Mortgage LLC, dba Mr. Cooper	14,690,284
5	PBI Research Services – MOVEit Transfer	11,781,156
6	HCA Healthcare, Inc.	11,270,000
7	Weee! Inc.	11,000,000
8	Maximus, Inc. – MOVEit Transfer	11,000,000
9	Perry Johnson & Associates, Inc.	8,952,212
10	Zacks Investment Research, Inc.	8,929,503

Total Annual Compromises Since 2005

The ITRC has been tracking publicly reported data compromises since 2005. You can see the growth in the number of reported breaches as more states adopted mandatory notice laws through 2018. Since then, the growth in compromises has been fueled primarily by cyberattacks.

See Figure 9

Figure 9 | *Total Annual Compromises, 2005 – Present*

	Compromises	Victims
2023	3,205	353,027,892
2022	1,801	425,212,090
2021	1,860	300,607,163
2020	1,108	310,235,204
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935
2016	1,088	2,541,092,072
2015	785	318,276,407
2014	785	147,637,369
2013	617	281,992,032
2012	471	15,808,604
2011	421	22,939,813
2010	662	16,269,861
2009	497	223,598,989
2008	654	35,722,280
2007	446	128,225,343
2006	318	18,439,844
2005	156	66,733,201

Trends

+ *Trend 1: Supply Chain Attacks Grow*
+ *Trend 2: Underlying Flaw in Data Breach Notice Laws*

Two clear trends emerged in 2023 beyond the dramatic rise in overall data compromises: 1) an equally dramatic increase in the number of organizations being impacted by Supply Chain Attacks, and 2) a trend highlighted by the rise in Supply Chain Attacks – the further breakdown in the breach notification framework.

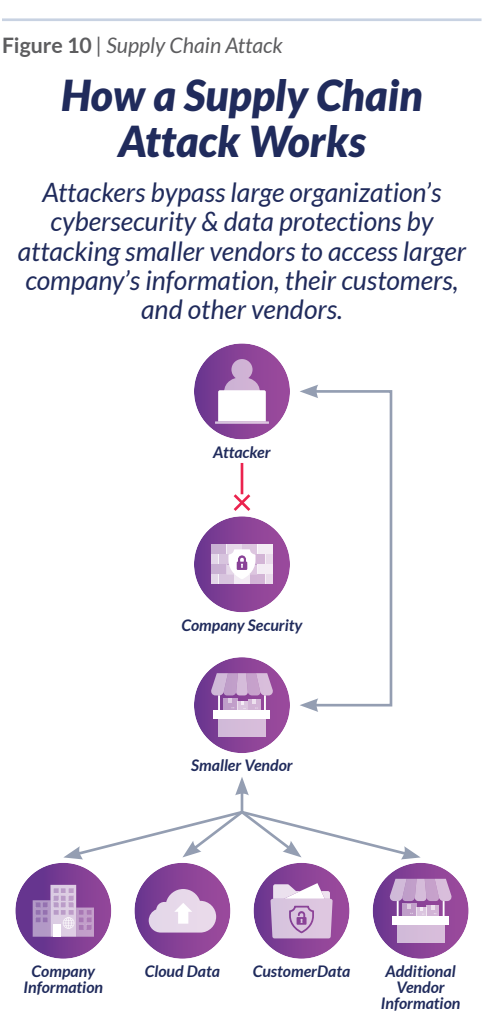
Trend 1: Supply Chain Attacks Grow

Third-Party Vendor Attacks, also known as Supply Chain Attacks, are typically attacks that fall into one of the primary root causes of a compromise, most often a cyberattack such as a phishing-related attack, ransomware or malware. What makes them unique is the target is not data owned by the breached organization but rather the information of the business's customers, clients or other vendors in a supply chain.

Rather than attack a single large organization – a large multi-national corporation with a well-resourced cybersecurity program, for example – identity criminals will attack a smaller vendor with less security protections that supports the same large multi-national company along with many other businesses. A supply chain attack can come in the form of breaching a single organization and stealing information from multiple companies or using flaws in a single product or service used by multiple companies to access the personal information stored in their databases.

See Figure 10

Figure 10 | *Supply Chain Attack*



While the growth in the number of organizations targeted in Supply Chain Attacks has been relatively slow since 2018, the number of organizations impacted has surged by more than 2,600 percent (2,600%) over the same time period. The estimated number of victims has also surged to more than 54M victims, or 15 percent (15%) of the overall number of victims in 2023.

See Figure 11

Figure 11 | *Supply Chain Attacks, Year-Over-Year*

	Third-Party/ Supply Chain Attacks	Entities Impacted
2023	242	2,769
2022	115	1,745
2021	84	521
2020	69	694
2019	104	232
2018	82	101

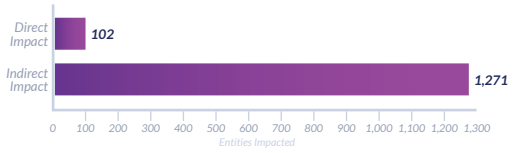
The chart illustrating the growth in Supply Chain Attacks includes organizations impacted by one of the largest third-party vendor attacks ever – a 2023 attack against the company that offers the MOVEit file transfer software and service. Cybercriminals exploited previously unknown flaws in software and cloud versions of MOVEit used by businesses, governments, schools, hospitals and other organizations around the world to securely share documents and information.

While Supply Chain Attacks had been around for many years, the ability to automate and launch the attacks at scale accelerated in 2018. That year, an attack on third parties might impact the company attacked and a handful of other organizations.

Fast forward to today, and the MOVEit attack shows the scope and scale a Supply Chain Attack can have. For instance, 102 entities were directly impacted by threat actors exploiting a MOVEit product. However, 1,271 organizations were indirectly affected when information stored in or accessed by a MOVEit product or service was compromised via a vendor or vendors.

See Figure 12

Figure 12 | *MOVEit Supply Chain Attack, Direct and Indirect Impacts*



Some organizations (25) reported being impacted by multiple vendors that used MOVEit product; more than a dozen (13) organizations reported that a vendor of a vendor experienced the breach. The entire databases of the state motor vehicle agencies in Louisiana and Oregon were compromised, exposing information that can be used to impersonate current or former residents of those states.

Trend 2: Underlying Flaw in Data Breach Notice Laws

The ITRC first identified a significant drop in the number of data breach notices with a distinct lack of actionable information in late 2021.

As noted elsewhere in this report, the opaque nature of data breach notices continued to increase during the past year at a time when the overall volume of public breach notices has grown. This lack of transparency puts businesses and individuals at increased risk of their identities being misused.

Since the earliest days of state breach notice laws, advocates for and against mandatory notices debated if breach laws would be a deterrent to lax policies and protections, and if absent strong penalty provisions, organizations would issue notices at all. For the most part, the organization that is attacked makes the decision if a breach notice is required based on their determination of risk to the data subject. If the organization determines there is no risk of harm to an individual, then no notice is required[3].

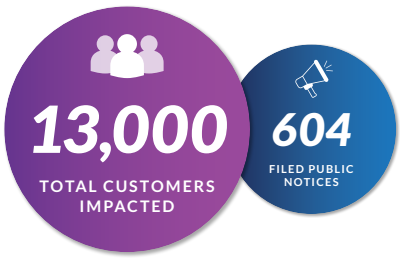
The rise in Supply Chain Attacks where the breached entity may not own the data that is stolen has called into question who is responsible for making the determination of risk and notifying victims of the compromise. The 2020 Supply Chain Attack against Blackbaud illustrates the issues surrounding notification and highlights the fact breaches are under-reported.

In May 2020, Blackbaud, a publicly traded cloud computing provider that serves nonprofit, education, healthcare and other institutional clients, was the target of a cyberattack. The information of roughly one-quarter of the company's customers was compromised and held for ransom. According to a settlement agreement reached in late 2023 with 49 state attorneys general, Blackbaud notified more than 13,000 customers about the data breach and the loss of their data but did not notify the individual victims whose personal information was exposed.

Of the 13,000 Blackbaud customers impacted by the breach, only 604 organizations filed public notices tracked by the ITRC, representing an estimated 12.8M victims. The gap between the thousands of organizations that lost data and the hundreds who notified victims is a clear indicator that data breach notice laws and regulations have failed to achieve the original goal of protecting businesses and individuals.

See Figure 13

Figure 13 | *Blackbaud Supply Chain Attack Notices*



[3]*Oregon, for example, is an exception to the self-determination of risk after a data breach. An organization may consult with law enforcement agencies to make a joint determination if a notice to victims is required*

Solutions

+ *Uniform Breach Notice Laws*
+ *Digital Credentials & Facial Comparison Systems*
+ *Improve Vendor Due Diligence*
+ *Breach Alert for Business*

At the end of 2023, the ITRC issued predictions for 2024, including this:

An unprecedented number of data breaches in 2023 by financially motivated and Nation/State threat actors will drive new levels of identity crimes in 2024, especially impersonation and synthetic identity fraud.

It's a safe bet, too, that Generative AI will also contribute to a rise in the sophistication of phishing attacks and other forms of identity fraud and scams using personal information stolen in data breaches. The availability of compromised consumer data and the use of large language models (LLMs) is already resulting in vastly improved phishing lures and highly effective social engineering attacks that are driving financial losses for businesses and individuals. Still, the greatest risk from Generative AI will continue to be mis- and dis-information because of the ease of automating and scaling the distribution of false information, not voice cloning or deep fake videos used to extort victims.

The combination of more data from more compromises, along with revolutionary technology, means we must consider significant changes to how we protect personal information and respond when it is compromised. There are three areas where the ITRC suggests action that will help reduce the rate and impact of data breaches on individual and business victims.

Uniform Breach Notice Laws

In the 20 years since California's first-of-its-kind data breach notice law went into effect, nearly 19,000 data breaches have been publicly reported in the U.S. In the U.S., there were an average of ~12 (12.3) data breaches reported each business day in 2023, while in the European Union, there were an average of 912 compromises reported each business day in 2022, the last year data was available.

The current patchwork of 50 state laws and expanded federal regulations makes compliance difficult and expensive for businesses. Individual victims (as well as businesses vulnerable to a similar attack) increasingly receive no notice or notices with little or no actionable information. There is wide variability in what triggers a breach notice, how a notice is to be sent, the content of the notice, the time frame in which the notice must be sent and penalties for non-compliance.

The ITRC believes state data breach laws and federal agency regulations can be more helpful to victims by adopting uniform provisions. For example:

- A uniform definition of personally identifiable information that triggers a notice.
- Breach notices should be filed with state and federal agencies of jurisdiction within 24 hours of any data breach.
- Together, breached entities and government agencies should determine if there is potential harm to an individual based on the information that has been compromised. If so, the breached entity should notify impacted individuals within 72 hours of the initial notice to the government of the breach.
- In the event the release of information regarding the data breach is determined to be a threat to national security or of terrorism, the senior state agency official, in consultation with the U.S. government agencies of jurisdiction, may delay notification for no more than 30 days.
- Notices should include detailed information about the organization and the event. Entities should be granted safe harbor from liability for data breaches, if:
    - An entity fully complies with the uniform Act, and;
    - Provides notice to the Identity Theft Resource Center for publication in the ITRC's database of breach notifications for free public access to the information
- Safe Harbor should not be granted in the event of gross negligence or willful misconduct leading to a data compromise. Willful misconduct includes failing to fully fund a data security program equal to the risk of harm.
- Entities found to have violated the provisions of the uniform Act should be fined an amount for each day a violation occurs.

Digital Credentials & Facial Comparison Systems

In November 2023, the ITRC completed a year-long review of emerging methods of identity verification, a key to protecting individuals from identity crimes. Trillions of U.S. dollars were pumped into the economy in the form of enhanced government cash benefits in 2020 and 2021 to support businesses and individuals during the pandemic. Professional threat actors and their more opportunistic criminal counterparts began to systematically apply for pandemic relief benefits. Identity verification processes used to open and access accounts were no match for the volume or scale of legitimate and illegitimate applications for assistance.

As an organization that operates the largest repository of U.S. data breach information, the ITRC immediately recognized that data alone could no longer be trusted as the sole source of truth about a person's identity in most processes. The ITRC concluded that the expanded use of facial verification and digital credentials is crucial to reducing the number of identity crimes involving the use of stolen personal information.

Traditional ID verification is often based on two factors; "something you know," like your SSN, or "something you have," such as a driver's license, smartphone, or security token. Adding a third factor – "something you are" - introduces a biometric which most adults already have (a photo) on file with government agencies thanks to the process they went through to get a driver's license or passport. If someone can prove that their face matches the photo on their government ID, it provides a strong signal that they are the rightful owner of that document.

Facial identity verification is not the same as the controversial facial recognition. The confusion between the two very different uses of facial biometrics threatens the adoption and implementation of beneficial uses of facial verification.

- Facial verification - also known in some circles as "facial comparison" – begins with a consent-based transaction that requires a person to prove they are who they claim to be. In the most robust processes that exist today, a live photo or selfie photo is compared to the photo on a credential that someone already has, like a driver's license.
- Facial recognition is used by law enforcement and intelligence agencies to capture a person's face that is then compared to a file that may contain thousands to millions of other individuals as part of surveillance or an investigation.

The use of a facial biometric as part of a comprehensive identity verification process provides a low-risk, equitable way to help ensure the authenticity of an applicant while lowering the overall value of compromised personally identifiable information to bad actors. Additionally, given that many legacy identity verification solutions rely on credit data – which does not work well for individuals with little to no credit history – these biometric tools can help reach individuals who might otherwise be excluded from the ability to remotely verify their identity online.

Increasing adoption of mobile Driver's Licenses (mDL) also represents an opportunity to reduce the value of stolen personal information and increase the security of personal credentials. Having a standards-based mobile form of digital identity that offers the same trust as a state-issued physical driver's license could be the on ramp to a secure, uniform, consent-based and fraud-resistant identity proofing solutions. A digital credential can be verified with the issuing agency in real-time to ensure the authenticity of the mDL and the identity of the holder, making stolen information far less valuable and useful.

Improve Vendor Due Diligence

Nearly a dozen states have adopted comprehensive state privacy laws, most of which also include some form of cyber risk assessment. Various state and federal regulatory agencies have also adopted a model of requiring organizations to have cybersecurity protections in place that are "equal to the risk" of harm to individuals if their information were compromised in a data breach.

Some states, California and New York for example, have proscribed that an equal-to-the-risk approach includes ensuring vendors (and even vendors' vendors) must have data and security protections in place that meet or exceed the prime organization's criteria. Regular audits are required as part of the compliance regime. New York requires the prime organization to issue a data breach notice even if the breach occurs at an affiliate or vendor.

Given the rise in Supply Chain Attacks identified earlier in this report, understanding the risk represented by vendors is imperative. Knowing both the breach history of an organization and being able to verify that history is a key to proper due diligence on current and future suppliers. So is knowing when a vendor or a vendors vendor issues a data breach notice.

Breach Alert for Business

The ITRC will soon launch a due diligence and alert tool that allows organizations to comply with state and federal requirements to understand the risks within their supply chains. Known as Breach Alert for Business (BA4B), this service will be available for a low annual fee directly from the ITRC.

*Submit your interest in BA4B by emailing **Dorinda Miller**.*

Review the depth and breadth of information available about an organization and its data breaches in the Appendix to this report.

Consumer & Business Resources

The ITRC offers a variety of low-cost identity education, protection, and recovery services for small businesses as well as free victim assistance and education opportunities for consumers. To learn more, email ***Dorinda Miller*** or contact the ITRC by email at ***communications@idtheftcenter.org***.

For Media

For any media-related inquiries, please email ***media@idtheftcenter.org***.

Appendix

+ *Total Compromises, 2005 – Present*
+ *Full Year 2023*
  - *Q1 | Q2 | Q3 | Q4*
+ *Trends, 2018 – 2023*
  - *Total Compromises | Attack Vectors | By Sector | Top 5 Industries*
+ *Public Company vs Other Entity Trends*
+ *Data Map*
+ *Methodology*

Unless otherwise noted, all data reported here was entered into the ITRC notified database between January 7, 2023, through January 6, 2024.

Total Compromises, 2005 – Present

Total Compromises | *2005 – Present*

	Compromises	*Victims*
2023	*3,205*	*353,027,892*
2022	*1,801*	*425,212,090*
2021	*1,860*	*300,607,163*
2020	*1,108*	*310,235,204*
2019	*1,279*	*883,558,186*
2018	*1,175*	*2,227,849,622*
2017	*1,506*	*1,825,413,935*
2016	*1,088*	*2,541,092,072*
2015	*785*	*318,276,407*
2014	*785*	*147,637,369*
2013	*617*	*281,992,032*
2012	*471*	*15,808,604*
2011	*421*	*22,939,813*
2010	*662*	*16,269,861*
2009	*497*	*223,598,989*
2008	*654*	*35,722,280*
2007	*446*	*128,225,343*
2006	*318*	*18,439,844*
2005	*156*	*66,733,201*

Data Compromise Details: Year End, 2023

Number of Compromises

Total Data Compromises:
3,205 Compromises
353,027,892 Victims

Data Breaches:
3,122 Data Breaches
349,221,481 Victims

Data Exposures:
25 Data Exposures
960,700 Victims

Data Leaks:
2 Data Leaks
2,696,728 Victims

Uknown
56 Compromises
148,983 Victims

Attack Vectors, 2023

Cyberattacks:
2,365 Breaches
343,338,964 Victims

+ 438 Phishing/Smishing/BEC
+ 246 Ransomware
+ 118 Malware
+ 110 Zero-Day Attack
+ 29 Credential Stuffing
+ 14 Non-Secured Cloud Environment
+ 30 Other
+ 1,380 NA

System & Human Error:
729 Breaches/Exposures
6,715,385 Victims

+ 380 Correnspondence (Email/Letter)
+ 53 Lost Devices or Documents
+ 25 Failure to Configure Cloud Security
+ 19 Misconfigured Firewalls
+ 220 Other
+ 32 NA

Physical Attacks:
53 Breaches/Exposures
127,832 Victims

+ 23 Device Theft
+ 9 Skimming Devices
+ 6 Document Theft
+ 5 Improper Disposal
+ 5 Other
+ 5 NA

Supply Chain Attacks *(Including Above)*:

+ Cyberattack:
  2.727 Entities Affected
  54,282,305 Victims
+ System & Human Error:
  38 Entities Affected
  148,769 Victims
+ Physical Attack:
  4 Entities Affected
  1,357 Victims

Q1 Data Compromises, 2023

Number of Compromises

Total Data Compromises:
442 Compromises
100,601,357 Victims

Data Breaches:
433 Data Breaches
100,522,430 Victims

Data Exposures:
7 Data Exposures
78,927 Victims

Data Leaks:
0 Data Leaks
0 Victims

Uknown
2 Compromises
Unknown Number of Victims

Attack Vectors, 2023

Cyberattacks:
375 Breaches
96,477,820 Victims

+ 111 Phishing/Smishing/BEC
+ 58 Ransomware
+ 19 Malware
+ 8 Credential Stuffing
+ 5 Non-Secured Cloud Environment
+ 2 Zero-Day Attack
+ 5 Other
+ 167 NA

System & Human Error:
59 Breaches/Exposures
4,033,567 Victims

+ 23 Correnspondence (Email/Letter)
+ 7 Failure to Configure Cloud Security
+ 5 Misconfigured Firewalls
+ 21 Other
+ 3 NA

Physical Attacks:
6 Breaches/Exposures
89,970 Victims

+ 6 Device Theft

Supply Chain Attacks *(Including Above)*:

+ Cyberattack:
  53 Entities Affected
  11,281,517 Victims
+ System & Human Error:
  18 Entities Affected
  147,495 Victims
+ Physical Attack:
  2 Entities Affected
  Unknown Number of Victims

Charts

Top 10 Compromises | *Q1, 2023*

	Compromises	*Victims*
1	*T-Mobile*	*37,000,000*
2	*PeopleConnect, Inc. – Instant Checkmare & Truthfinder*	*20,221,007*
3	*Weee! Inc.*	*11,000,000*
4	*Zacks Investment Research, Inc.*	*8,929,503*
5	*Independent Living Systems, LLC*	*4,226,508*
6	*Regal Medical Group, Inc. – Lakeside Medical Organization, ADOC Medical Group, Greater Covina Medical*	*3,300,638*
7	*Cerebral, Inc. – Pixel*	*3,179,835*
8	*Fortra, LLC*	*2,308,785*
9	*NCB Maganement Services, Inc.*	*1,087,842*
10	*ZOLL Medical Corporation*	*1,004,443*

Compromises by Sector | *Q1, Year-Over-Year*

	Q1, 2023		Q1, 2022		Q1, 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	31	515,099	21	106,099	24	112,684
Financial Services	70	10,554,189	68	5,732,597	49	7,848,115
Government	23	759,622	13	790,763	11	647,917
Healthcare	81	14,199,413	73	4,377,462	71	3,332,703
Hospitality	7	196,891	6	57,392	6	53,152
HR/Staffing	3	20,616	–	–	–	–
Manufacturing	49	1,160,681	52	249,706	38	384,934
Mining/Construction	15	59,292	–	–	–	–
Non-Profit/NGO	19	85,420	20	629,822	15	590,219
Professional Services	48	75,222	45	3,022,491	30	3,566,213
Retail	16	179,622	18	272,950	20	506,821
Social Services	3	154,160	–	–	–	–
Technology	35	24,399,696	16	10,832,588	23	17,377,396
Transportation	13	11,096,783	8	20,930	14	139,250
Utilities	6	37,054,637	–	–	–	–
Wholesale Trade	11	62,316	–	–	–	–
Other	12	27,698	64	675,411	53	6,695,075
Unknown	–	–	–	–	–	–
Totals	**442**	**100,601,357**	**404**	**26,768,211**	**354**	**41,254,479**

Attack Vectors | *Q1, Year-Over-Year*

	Q1, 2023	Q1, 2022	Q1, 2021
Cyberattacks	**375**	**366**	**311**
Phishing/Smishing/BEC	111	112	117
Ransomware	58	71	62
Malware	19	24	34
Non-Secured Cloud Environment	5	3	4
Credential Stuffing	8	2	2
Unpatched Software Flaw	–	–	–
Zero Data Attack	2	–	1
Other	5	7	86
Not Specified	167	147	5
System & Human Error	**59**	**33**	**31**
Failure to Configure Cloud Security	7	4	8
Correspondence (Email/Letter)	23	12	12
Misconfigured Firewall	5	5	–
Lost Device or Document	–	1	2
Other	21	5	9
Not Specified	3	6	–
Physical Attacks	**6**	**3**	**12**
Document Theft	–	1	1
Device Theft	6	1	3
Improper Disposal	–	1	–
Skimming Decive	–	–	–
Other	–	–	8
Not Specified	–	–	–
Data Leak	-	–	–
Unknown	**2**	**2**	–

Q2 Data Compromises, 2023

Number of Compromises

Total Data Compromises:
940 Compromises
64,846,283 Victims

Data Breaches:
935 Data Breaches
64,840,190 Victims

Data Exposures:
5 Data Exposures
6,093 Victims

Data Leaks:
0 Data Leaks
0 Victims

Uknown
0 Compromises
0 Victims

Attack Vectors, 2023

Cyberattacks:
660 Breaches
64,402,165 Victims

+ 133 Phishing/Smishing/BEC
+ 70 Malware
+ 64 Ransomware
+ 14 Credential Stuffing
+ 14 Zero-Day Attack
+ 3 Non-Secured Cloud Environment
+ 9 Other
+ 353 NA

System & Human Error:
255 Breaches/Exposures
421,273 Victims

+ 152 Correnspondence (Email/Letter)
+ 24 Lost Devices or Documents
+ 5 Failure to Configure Cloud Security
+ 3 Misconfigured Firewalls
+ 65 Other
+ 6 NA

Physical Attacks:
25 Breaches/Exposures
22,845 Victims

+ 7 Device Theft
+ 7 Skimming Devices
+ 4 Improper Disposal
+ 2 Document Theft
+ 5 Other

Supply Chain Attacks *(Including Above)*:

+ Cyberattack:
  331 Entities Affected
  11,574,407 Victims
+ System & Human Error:
  11 Entities Affected
  1,143 Victims
+ Physical Attack:
  0 Entities Affected
  0 Victims

Charts

Top 10 Compromises | *Q2, 2023*

	Compromises	*Victims*
1	*PBI Research Services – MOVEit Transfer*	*11,781,156*
2	*MCNA Insurance Company*	*8,923,662*
3	*Louisiana Office of Motor Vehicles – MOVEit Transfer*	*6,000,000*
4	*PharMerica Corporation*	*5,815,591*
5	*TMX Finance Corporate Services, Inc.*	*4,822,580*
6	*Oregon Department of Transportation - MOVEit Transfer*	*3,500,000*
7	*Brightly Software, Inc.*	*2,964,292*
8	*Harvard Pilgrim Health Center*	*2,550,922*
9	*Enzo Biochem, Inc.*	*2,470,000*
10	*Apria Healthcare LLC*	*1,869,598*

Compromises by Sector | *Q2, Year-Over-Year*

	Q2, 2023		Q2, 2022		Q2, 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	49	1,072,408	20	299,394	33	178,083
Financial Services	173	14,340,181	59	16,752,160	84	1,986,604
Government	27	10,319,523	20	19,766	23	616,779
Healthcare	296	10,383,044	88	8,752,680	91	7,232,146
Hospitality	16	231,469	5	20,369	12	29,619
HR/Staffing	2	4,528	–	–	–	–
Manufacturing	63	190,491	63	240,829	61	558,658
Mining/Construction	16	49,397	–	–	–	–
Non-Profit/NGO	28	2,039,965	16	42,306	20	475,898
Professional Services	89	12,881,698	49	323,557	45	16,888,654
Retail	41	5,962,966	12	52,580	33	1,579,340
Social Services	5	16,212	–	–	–	–
Technology	52	6,529,868	15	4,974,681	24	23,946,126
Transportation	23	61,141	11	824,893	8	46,913
Utilities	16	322,799	–	–	–	–
Wholesale Trade	18	167,842	–	–	–	–
Other	26	272,751	55	2,948,226	60	1,549,744
Unknown	–	–	–	-	3	232,664
Totals	**940**	**64,846,283**	**413**	**35,251,441**	**497**	**55,321,228**

Attack Vectors | *Q2, Year-Over-Year*

	Q22, 2023	Q2, 2022	Q2, 2021
Cyberattacks	**660**	**364**	**412**
Phishing/Smishing/BEC	133	109	132
Ransomware	64	60	92
Malware	70	23	39
Non-Secured Cloud Environment	3	2	10
Credential Stuffing	14	4	6
Unpatched Software Flaw	–	–	–
Zero Data Attack	14	2	–
Other	9	4	124
Not Specified	353	160	9
System & Human Error	**255**	**34**	**60**
Failure to Configure Cloud Security	5	6	20
Correspondence (Email/Letter)	152	9	18
Misconfigured Firewall	3	10	5
Lost Device or Document	24	–	3
Other	65	7	14
Not Specified	6	2	–
Physical Attacks	**25**	**13**	**16**
Document Theft	2	2	–
Device Theft	7	8	8
Improper Disposal	4	2	3
Skimming Decive	7	1	–
Other	5	–	5
Not Specified	–	–	–
Data Leak	-	–	**5**
Unknown	–	**2**	**4**

Q3 Data Compromises, 2023

Number of Compromises

Total Data Compromises:
734 Compromises
80,376,716 Victims

Data Breaches:
717 Data Breaches
77,615,076 Victims

Data Exposures:
6 Data Exposures
52,458 Victims

Data Leaks:
2 Data Leaks
2,696,728 Victims

Uknown
9 Compromises
12,454 Victims

Attack Vectors, 2023

Cyberattacks:
614 Breaches
77,492,293 Victims

+ 81 Phishing/Smishing/BEC
+ 63 Ransomware
+ 18 Malware
+ 4 Credential Stuffing
+ 69 Zero-Day Attack
+ 5 Non-Secured Cloud Environment
+ 7 Other
+ 367 NA

System & Human Error:
95 Breaches/Exposures
169,854 Victims

+ 40 Correnspondence (Email/Letter)
+ 7 Misconfigured Firewalls
+ 9 Lost Devices or Documents
+ 6 Failure to Configure Cloud Security
+ 27 Other
+ 6 NA

Physical Attacks:
14 Breaches/Exposures
5,387 Victims

+ 7 Device Theft
+ 2 Skimming Devices
+ 1 Improper Disposal
+ 1 Document Theft
+ 3 NA

Supply Chain Attacks *(Including Above)*:

+ Cyberattack:
  1,316 Entities Affected
  19,972,949 Victims
+ System & Human Error:
  4 Entities Affected
  131 Victims
+ Physical Attack:
  0 Entities Affected
  0 Victims

Charts

Top 10 Compromises | *Q3, 2023*

	Compromises	Victims
1	HCA Healthcare, Inc.	11,270,000
2	Maximus, Inc. – MOVEit Transfer	11,000,000
3	The Freecycle Network	7,000,000
4	Delta Dental of California – MOVEit Transfer	6,928,932
5	IBM Consulting – MOVEit Transfer	4,091,794
6	Caeesrs Entertainment, Inc.	3,381,410
7	CareSource - MOVEit Transfer	3,180,537
8	Duolingo	2,676,696
9	Tampa General Hospital	2,430,920
10	PH TECH – MOVEit Transfer	1,750,000

Compromises by Sector | *Q3, Year-Over-Year*

	Q3, 2023		Q3, 2022		Q3, 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	42	1,908,134	23	1,097,584	25	1,259,723
Financial Services	205	17,664,167	66	3,153,208	69	1,732,946
Government	26	2,869,273	19	220,738	21	1,927,008
Healthcare	113	17,589,621	93	5,060,271	78	11,150,980
Hospitality	10	3,513,594	10	69,027,431	5	31,069
HR/Staffing	2	134,469	–	–	–	–
Manufacturing	65	3,589,714	64	23,095,176	48	48,306,467
Mining/Construction	20	38,048	–	–	–	–
Non-Profit/NGO	22	7,178,851	16	65,161	21	143,457
Professional Services	81	16,956,381	69	1,705,652	48	1,534,208
Retail	30	1,287,107	20	363,880	21	520,028
Social Services	3	17,349	–	–	–	–
Technology	40	5,957,954	21	2,969,682	13	406,007
Transportation	25	18,471	6	2,517,830	8	329,171
Utilities	10	12,859	–	–	–	–
Wholesale Trade	13	23,694	–	–	–	–
Other	27	1,617,030	64	691,134	87	63,908,379
Unknown	–	–	–	-	1	35,000,000
Totals	**734**	**80,376,716**	**471**	**109,967,747**	**445**	**166,249,443**

Attack Vectors | *Q3, Year-Over-Year*

	Q3, 2023	Q3, 2022	Q3, 2021
Cyberattacks	**614**	**414**	**534**
Phishing/Smishing/BEC	81	131	192
Ransomware	63	78	109
Malware	18	15	43
Non-Secured Cloud Environment	5	1	6
Credential Stuffing	4	8	4
Unpatched Software Flaw	–	–	2
Zero Data Attack	69	2	2
Other	7	2	133
Not Specified	367	177	43
System & Human Error	**95**	**42**	**61**
Failure to Configure Cloud Security	6	3	22
Correspondence (Email/Letter)	40	15	20
Misconfigured Firewall	7	7	6
Lost Device or Document	9	3	4
Other	27	10	9
Not Specified	6	4	–
Physical Attacks	**14**	**12**	**13**
Document Theft	1	2	4
Device Theft	7	4	4
Improper Disposal	1	1	–
Skimming Decive	2	2	–
Other	–	2	5
Not Specified	3	1	–
Data Leak	**2**	–	**1**
Unknown	**9**	**3**	**9**

Q4 Data Compromises, 2023

Number of Compromises

Total Data Compromises:
1,089 Compromises
107,203,536 Victims

Data Breaches:
1,037 Data Breaches
106,243,785 Victims

Data Exposures:
7 Data Exposures
823,222 Victims

Data Leaks:
0 Data Leaks
0 Victims

Uknown
45 Compromises
136,529 Victims

Attack Vectors, 2023

Cyberattacks:
716 Breaches
104,966,686 Victims

+ 113 Phishing/Smishing/BEC
+ 61 Ransomware
+ 11 Malware
+ 3 Credential Stuffing
+ 25 Zero-Day Attack
+ 1 Non-Secured Cloud Environment
+ 9 Other
+ 493 NA

System & Human Error:
320 Breaches/Exposures
2,090,691 Victims

+ 165 Correnspondence (Email/Letter)
+ 20 Lost Devices or Document
+ 7 Failure to Configure Cloud Security
+ 4 Misconfigured Firewalls
+ 107 Other
+ 17 NA

Physical Attacks:
8 Breaches/Exposures
9,630 Victims

+ 3 Device Theft
+ 3 Document Theft
+ 2 NA

Supply Chain Attacks *(Including Above)*:

+ Cyberattack:
  1,026 Entities Affected
  11,452,591 Victims
+ System & Human Error:
  5 Entities Affected
  Unknown Number of Victims
+ Physical Attack:
  2 Entities Affected
  1,357 Victims

Charts

Top 10 Compromises | *Q4, 2023*

	Compromises	Victims
1	Xfinity	35,879,455
2	Nationstar Mortgage LLC bda Mr. Cooper	14,690,284
3	Perry Johnson & Associates, Inc.	8,952,212
4	Welltok, Inc. – MOVEit Transfer	8,493,379
5	HealthEC, LLC	4,452,782
6	ESO Solutions, Inc.	2,700,000
7	Norton Healthcare, Inc.	2,500,000
8	Postmeds, Inc.	2,364,359
9	McLaren Health Care	2,192,515
10	INTEGRIS Health, Inc.	2,000,000

Compromises | *Quarter-to-Quarter*

	Compromises	Victims
Q4, 2023	1,089	107,203,536
Q3, 2023	734	80,376,716
Q2, 2023	940	64,846,283
Q4, 2023	442	100,601,357
Q4, 2022	513	253,224,691
Q3, 2022	471	109,967,747
Q2, 2022	413	35,251,441
Q1, 2022	404	26,768,211
Q4, 2021	564	37,782,013
Q3, 2021	445	166,249,443
Q2, 2021	497	55,321,228
Q1, 2021	354	41,254,479

Compromises by Sector | *Q4, Year-Over-Year*

	Q4, 2023		Q4, 2022		Q4, 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	51	773,943	35	789,112	43	136,702
Financial Services	296	18,382,872	76	1,781,716	77	8,410,443
Government	24	1,457,836	22	720,412	11	52,751
Healthcare	319	13,803,944	89	9,522,121	89	11,531,595
Hospitality	12	1,584,155	13	412,933	10	124,605
HR/Staffing	3	79,753	–	–	–	–
Manufacturing	82	195,270	70	420,616	75	532,524
Mining/Construction	20	75,245	–	–	–	–
Non-Profit/NGO	36	227,258	20	271,389	30	1,130,072
Professional Services	90	240,668	60	1,353,998	60	740,316
Retail	32	2,754,538	15	108,555	28	4,606,723
Social Services	4	5,377	–	–	–	–
Technology	40	28,349,888	35	229,869,351	19	2,954,651
Transportation	40	1,047,329	11	630,817	14	54,350
Utilities	12	36,028,227	–	–	–	–
Wholesale Trade	11	43,114	–	–	–	–
Other	16	2,154,119	67	7,343,671	108	7,507,281
Unknown	1	0	–	-	–	–
Totals	**1,089**	**107,203,536**	**513**	**253,224,691**	**564**	**37,782,013**

Attack Vectors | *Q4, Year-Over-Year*

	Q4, 2023	Q4, 2022	Q4, 2021
Cyberattacks	**716**	**440**	**500**
Phishing/Smishing/BEC	113	115	164
Ransomware	61	84	106
Malware	11	11	35
Non-Secured Cloud Environment	1	4	4
Credential Stuffing	3	4	2
Unpatched Software Flaw	–	–	2
Zero Data Attack	25	4	2
Other	9	4	91
Not Specified	493	214	94
System & Human Error	**320**	**54**	**45**
Failure to Configure Cloud Security	7	5	6
Correspondence (Email/Letter)	165	19	26
Misconfigured Firewall	4	8	4
Lost Device or Document	20	3	5
Other	107	14	4
Not Specified	17	5	–
Physical Attacks	**8**	**18**	**17**
Document Theft	3	2	5
Device Theft	3	8	5
Improper Disposal	–	1	2
Skimming Decive	–	3	1
Other	–	4	3
Not Specified	2	–	–
Data Leak	–	–	**1**
Unknown	**45**	**1**	**1**

Trends, 2018 – 2023

Total Compromises | *2018 – 2023*

	Compromises	Victims
2023	3,205	353,027,892
2022	1,801	425,212,090
2021	1,860	300,607,163
2020	1,108	310,235,204
2019	1,279	883,558,186
2018	1,175	2,227,849,622

Attack Vectors | *2018 – 2023*

	2023	2022	2021	2020	2019	2018
Cyberattacks	**2,365**	**1,584**	**1,611**	**877**	**928**	**754**
Phishing/Smishing/BEC	438	467	537	383	490	379
Ransomware	246	293	353	159	83	53
Malware	118	73	141	103	112	102
Non-Secured Cloud Environment	14	10	24	51	15	15
Credential Stuffing	29	18	14	17	3	10
Unpatched Software Flaw	–	–	4	3	3	–
Zero Data Attack	110	8	4	1	–	–
Other	30	17	424	159	223	195
Not Specified	1,380	698	110	1	–	–
System & Human Error	**729**	**163**	**179**	**153**	**231**	**261**
Failure to Configure Cloud Security	25	18	54	58	56	49
Correspondence (Email/Letter)	380	55	66	55	89	121
Misconfigured Firewall	19	30	13	4	4	29
Lost Device or Document	53	7	12	5	19	17
Other	220	36	34	31	63	45
Not Specified	32	17	–	–	–	–
Physical Attacks	**53**	**46**	**51**	**78**	**118**	**152**
Document Theft	6	7	9	15	19	25
Device Theft	23	21	17	30	57	57
Improper Disposal	5	5	5	11	14	21
Skimming Decive	9	6	1	5	4	12
Other	5	6	19	17	24	37
Not Specified	5	1	–	–	–	–
Data Leak	**2**	–	**7**	–	–	–
Unknown	**56**	**8**	**12**	–	**2**	**8**

Compromises by Sector | *2018 – 2023*

	2023		2022		2021		2020		2019		2018	
	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	173	~4M	99	~2M	125	~2M	42	~974K	71	~5M	85	~42M
Financial Services	744	~61M	269	~27M	279	~20M	138	~3M	171	~104M	203	~17M
Government	100	~15M	74	~2M	66	~3M	47	~1M	64	~1M	74	~63M
Healthcare	809	~56M	343	~28M	329	~33M	306	~10M	398	~9M	255	~7M
Hospitality	45	~6M	34	~70M	33	~238K	17	~22M	40	~1M	37	~424M
HR/Staffing	10	~239K	–	–	–	–	–	–	–	–	–	–
Manufacturing	259	~5M	249	~24M	222	~50M	70	~3M	103	~70M	96	~26M
Military	–	–	–	–	–	–	–	–	1	~1K	2	~185K
Mining/Construction	71	~222K	–	–	–	–	–	–	–	–	–	–
Non-Profit/NGO	105	~10M	72	~1M	86	~2M	31	~38K	36	~249K	22	~367K
Professional Services	308	~30M	223	~6M	183	~23M	144	~73M	84	~2M	112	~497K
Retail	119	~10M	65	~798K	102	~7M	53	~11M	86	~370M	91	~47M
Social Services	15	~193K	–	–	–	–	–	–	–	–	–	–
Technology	167	~65M	87	~249M	79	~45M	67	~142M	63	~108M	61	~920M
Transportation	101	~12M	36	~4M	44	~570K	21	~1M	15	~211K	19	~12M
Utilities	44	~73M	–	–	–	–	–	–	–	–	–	–
Wholesale Trade	53	~297K	–	–	–	–	–	–	–	–	–	–
Other	81	~4M	250	~12M	308	~80M	172	~43M	147	~212M	118	~670M
Unknown	1	0	–	–	4	~35K	–	–	–	–	–	–
Totals	**3,205**	**~353M**	**1,801**	**~425M**	**1,860**	**~300M**	**1,108**	**~310M**	**1,279**	**~884M**	**1,175**	**~2B**

Top 5 Industries | *2018 – 2023*

	2023		2022		2021		2020		2019		2018	
	Industry	Compromises	Industry	Compromises	Industry	Compromises	Industry	Compromises	Industry	Compromises	Industry	Compromises
1.	Healthcare	809	Healthcare	343	Healthcare	329	Healthcare	306	Healthcare	398	Healthcare	255
2.	Financial	744	Financial	269	Other	308	Other	172	Financial	171	Financial	203
3.	Professional Services	308	Other	250	Financial	279	Professional Services	144	Other	147	Other	118
4.	Manufacturing	259	Manufacturing	249	Manufacturing	222	Financial	138	Manufacturing	103	Professional Services	112
5.	Education	173	Professional Services	223	Professional Services	183	Manufacturing	70	Retail	86	Manufacturing	96

Public Company vs Other Entity[4] Trends

Compromises and Victims | *Public vs Other, 2023*

	Compromises	Victims
Publicly Traded	358	143,027,616
Other Entity	2,847	210,000,276
Total	**3,205**	**353,027,892**

Actionable vs Non-Actionable Notices | *Public vs Other, 2023*

	Notices Without Attack Vector	Percentage	Notices With Attack Vector	Percentage
Publicly Traded	170	47%	188	53%
Other Entity	1,303	46%	1,544	54%

Attack Vectors | *Public vs Other, 2023*

	Publicly Traded	Other Entity
Cyberattacks	**249**	**2,166**
Phishing/Smishing/BEC	23	415
Ransomware	17	229
Malware	4	114
Non-Secured Cloud Environment	3	11
Credential Stuffing	11	18
Unpatched Software Flaw	–	–
Zero Data Attack	28	82
Other	3	27
Not Specified	160	1,220
System & Human Error	**95**	**634**
Failure to Configure Cloud Security	–	25
Correspondence (Email/Letter)	42	338
Misconfigured Firewall	1	18
Lost Device or Document	5	48
Other	43	177
Not Specified	4	28
Physical Attacks	**10**	**43**
Document Theft	1	5
Device Theft	2	21
Improper Disposal	–	5
Skimming Decive	2	7
Other	1	4
Not Specified	4	1
Data Leak	**2**	–
Unknown	**2**	**54**

[4]*Other entities include private businesses, government agencies, non-profit organizations, schools, colleges and universities, and other non-publicly traded institutions.*

Data Map

The ITRC database of publicly reported data breaches includes a comprehensive set of data points described in the following data map. This information feeds our data breach tracking and alert tools that are available for free to consumers and for a fee to businesses under the *notified* brand name.

Data Breach – Data removed by malicious action or error from the database or system where it was created, collected, processed, or maintained. NIST definition: The unauthorized transfer of information from an information system.

Data Exposure – Data that was available for viewing or download where data was NOT removed (exfiltrated) from the database or system where it was created, collected, processed, or maintained. Example: a Cloud database where data was open to the internet but where there is no evidence the data was removed.

Data Compromise/Data Event – Generic terms for a data breach or data exposures.

Breach Number – Salesforce unique assigned value.

Date Breach orExposure Reported – Date a data event was reported by a compromised organization, government agency, or media.

Entity Name – Name of a compromised organization.

State – State where a compromised organization is headquartered or where a compromise occurred.

Individuals Impacted – Number of individuals impacted by the breach/exposure.

Sector– Standard categories used to filter data compromises by organization type/sector and industry (based on SIC code).

Publicly Traded – Indicates if a company is publicly traded.

Total Records Breached or Exposed – Total records compromised linked to a single individual.

Sensitive Records Exposed – Y/N - Records compromised contain sensitive personal identifiable information (SPII) as defined by statute, such as passport numbers, SSN, health information, etc.

Nonensitive Records Exposed – Y/N - Records compromised only contain non-sensitive personal information (PII) as defined by statute, such as telephone numbers, email addresses, login & passwords, etc.

Unknown Records Exposed – Y/N - Type of records compromised are unknown.

Threat Actor – A threat actor is the person or group whose actions or failure to act results in a data compromise. The act or failure to act may be malicious or it may be an error. Internal actors are employees of a compromised organization. An external actor may be an independent person or group as well as an affiliated 3rd party such as a vendor. A Nation/State actor is acting on behalf of a government.

Attack Vector – The category of method used by a threat actor to compromise an organization's data. Cyberattacks involve compromising an electronic information system using software or computer technology. Physical attacks involve compromising data through a physical act. System or Human Errors are failures of a system or human being to perform as expected or required without malicious intent that results in a data compromise.

Last Modified Date – Last date information about a compromise was updated in the ITRC database.

Breach Info Source – Source of information about a compromise.

Sensitive Records Count – Number of records that contain sensitive personal identifiable information (SPII) as defined by statute, such as passport numbers, SSN, health information, etc.

Nonsensitive Records Count – Number of records compromised that only contain non-sensitive personal information (PII) as defined by statute, such as telephone numbers, email addresses, login & passwords, etc.

Industry – Standard categories used to filter data compromises by organization type/sector and industry (based on SIC code).

Data Exposed/Breached – The common types of personal data exposed in data compromises.

Attack Vector Details – The category of method used by a threat actor to compromise an organization's data. Cyberattacks involve compromising an electronic information system using software or computer technology. Physical attacks involve compromising data through a physical act. System or Human Errors are failures of a system or human being to perform as expected or required without malicious intent that results in a data compromise.

Identity Theft Protection Offered – Individuals whose data was compromised are or are not offered ID Theft protection by the compromised organization.

Identity Theft Protection Company – Name of ID Theft Protection provider assisting consumers whose information was compromised.

Data Attributes – Specific data points compromised in a data event.

Date Breach Discovered – Date an organization first discovered it had been compromised.

Date of Breach – Date a threat actor first compromised an organization or system.

Methodology

For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure, or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's *notified* data compromise tracking database.

The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's notified breach tracking solution.

The ITRC reports Third-Party/Supply Chain Attacks as a single attack against the company that lost control of the information. The total number of individuals impacted by third-party incidents is based on notices sent by the multiple organizations impacted by the single data compromise.