ITRC | IDENTITY THEFT RESOURCE CENTER

JANUARY 2025

CONTENTS

INTRODUCTION
from the President

Twenty years ago next month, I was sitting at my desk in suburban Atlanta when my phone rang. On the other end of the line was a reporter for NBC News – Bob Sullivan – who had some questions about letters the company where I worked had sent to around 20,000 residents of California about a data breach.

That phone call started a media and public policy avalanche that, in some ways, continues to this day. After two decades, we still have not sufficiently addressed the root causes of most data breaches. Nor have the technical and policy cures adopted in the intervening years been particularly effective in slowing, let alone stopping, the steady increase in events that compromise information.

In the pages that follow, you'll find the data that shows we are not making much progress in data protection. In fact, stolen and compromised data is so ubiquitous that the number of people and businesses who have not been impacted by a data breach is now dwarfed by the number of victims who have been – by a factor of five[1].

In 2024, we did not exceed the record number of data breaches set in 2023, but we did come "this" close to doing so. Within that near-record number of compromise notices, there are a number of trends that require discussion:

+ A significant number of data compromises could have been avoided with basic cybersecurity.
+ Federal and State disclosure regulations are not having the intended prevention effects, but state privacy laws may be.
+ The actual impact of data breaches on people is often masked by the scale of mega-breaches.
+ It's difficult to quantify the impact of Artificial Intelligence on data compromises, but there are red flags.

In 2024, the ITRC tracked 3,158 data compromises that resulted in more than 1.3 billion notices going to individuals. The number of compromises is essentially flat with the previous record-breaking year, but the number of victim notices is up 211 percent (211%) – also known as "off the chart."

It's impossible to know how many individuals are actually represented in that billion-plus notice count – but back-of-the-envelop-math tells us that's an average of six (6) alerts for every adult[2] in the country. If mandatory data breach notices are supposed to reduce the number of breaches, they are not having the intended effect.

Despite the disconcerting overall trend lines, there is some good news. Forty percent (40%) of states have adopted comprehensive privacy laws, all but one of which includes mandatory cybersecurity standards. As we head into the 2025 state legislative season, expect to see more state privacy laws introduced and passed[3] in the absence of a uniform federal privacy law.

There is also an advancement in technology that is rapidly being deployed by companies and adopted by consumers that has the potential to all but eliminate an entire class of cyberattacks. The technology involves the use of "passkeys" that make stealing or using stolen passwords obsolete.

Today's password practices require users to remember a credential and organizations to store them in databases that can be compromised. Passkeys, though, can't be stolen, and users cannot self-compromise because they never know the access key. Read more about how to set up and use passkeys.

Best of all, if passkeys had been deployed at the time of most, if not all, of the organizations reporting breaches related to stolen credentials in 2024, there would not have been a breach. A whopping 94 percent (94%) of all devices are now ready to use passkeys, with major providers like Amazon and Microsoft offering access to passkeys to 100 percent (100%) of users, according to the FIDO Alliance[4].

Consumer support for passkeys is rapidly growing, too. ITRC research shows that 30 percent (30%) of U.S. consumers already use passkeys on at least one account after one year of availability. Here's to a near future where breaches linked to credential attacks are a thing of the past.

James E. Lee
President, Identity Theft Resource Center

[1]*The ITRC's 2024 Consumer & Business Impact Report (CIBIR) includes research findings that indicate that approximately eight in ten consumers and a similar number of businesses were directly impacted by at least one data breach, cyberattack or both in the previous 12 months.*

[2]*The U.S. adult population in 2022 was 260M, according to the U.S. Census Bureau.*

[3]*Unfortunately, none of the new state privacy laws address the deficiencies in state data breach notification laws.*

[4]*Biometric Update: Passkeys build momentum, enabling access to 15 billion online accounts*

GLOSSARY

Since 2020, the ITRC has published the definitions we use in compiling and publishing this report. We have updated our terms for the 2024 report to include a new definition of Victim Notices to reflect the complex dynamics of reporting the number of individuals impacted by a compromise.

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.

Data Compromise/Event – 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).

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

Sensitive Records – Sensitive personal identifiable information (SPII) as defined by statute, such as passport numbers, SSN, driver's license, health information, etc.

Non-Sensitive Records – Non-sensitive personal information (PII) as defined by statute, such as telephone numbers, email addresses, login and passwords, etc.

Unknown Records – Type of records compromised are is unknown.

Threat Actor – A threat actor is the person or group whose malicious actions results in a data compromise. Internal actors are employees of a compromised organization. An external actor may be an independent person or group. A Nation/State actor is acting on behalf of a government.

Victim Notices – The ITRC reports the number of Victim Notices for both individual events and as a total for all reported compromises as a measure of the scale of events and impacts on individuals. However, Victim Notices should not be considered a 1-to-1 count of actual victims since not all notices include a victim count, and those that do may not reflect the number of individuals impacted, but rather the number of accounts compromised including instances where a person has multiple accounts. Aggregated totals also inflate the number of individuals affected because of single individuals receiving breach notices from multiple events.

DBR

IDENTITY THEFT RESOURCE CENTER

2024 Data Breach Report

The ITRC's *Annual Data Breach Report* explores near-record levels of data compromises and victim notices in 2024, as well as the underlying trends behind them. It also looks at the types of data compromised, solutions and more.

ITRC | IDENTITY THEFT RESOURCE CENTER

TOTAL COMPROMISES

3,158

44 Events Short of 2023 All-Time-High

1,350,835,988
VICTIM NOTICES

2,850 DATA BREACHES
1,246,573,396 VICTIM NOTICES

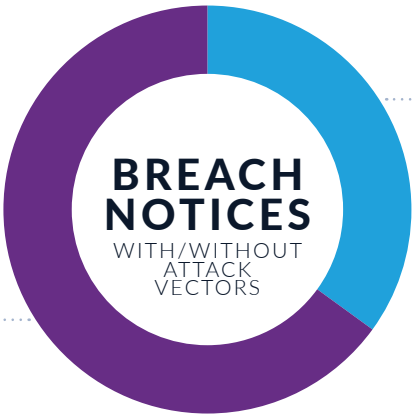
18 DATA EXPOSURES
100,153,761 VICTIM NOTICES

2 DATA LEAKS
2,795,947 VICTIM NOTICES

288 UNKNOWN COMPROMISES
1,312,884 VICTIM NOTICES

*Prior to 2020, **approximately 100% of breach notices** included attack vector information.*

Number of Victim Notices
211% INCREASE
YEAR-OVER-YEAR
*This is primarily due to **five "mega-breaches"** that resulted in at least 100M breach notices being issued in each event.*



35%
OF ALL NOTICES
Did Contain Attack Vector Details
1,093
NOTICES

65%
OF ALL NOTICES
Did Not Contain Attack Vector Details
2,065
NOTICES

TOP COMPROMISES IN 2024

BY INDUSTRY

1. ***Financial Services***
   737 COMPROMISES
2. ***Healthcare***
   536 COMPROMISES
3. ***Professional Services***
   345 COMPROMISES
4. ***Manufacturing***
   317 COMPROMISES
5. ***Education***
   162 COMPROMISES

Healthcare Was Previously the Most Attacked Industry
SINCE 2018

TOTAL ATTACK VECTORS

BREACHES/EXPOSURES & VICTIM NOTICES

Cyberattacks
2,525 BREACHES
1,229,866,035 VICTIM NOTICES

System & Human Errors
310 BREACHES OR EXPOSURES
116,671,768 VICTIM NOTICES

Physical Attacks
33 BREACHES OR EXPOSURES
189,354 VICTIM NOTICES

Supply Chain Attacks
134 BREACHES OR EXPOSURES
657 ENTITIES AFFECTED
203,144,092 VICTIM NOTICES

TOP COMPROMISES IN 2024

BY VICTIM NOTICE COUNT

1. ***Ticketmaster Entertainment, LLC***
   560,000,000 VICTIM NOTICES
2. ***Change Healthcare***
   190,000,000 VICTIM NOTICES
3. ***DemandScience by Pure Incubation***
   121,796,165 VICTIM NOTICES
4. ***AT&T***
   110,000,000 VICTIM NOTICES
5. ***MC2 Data***
   100,000,000 VICTIM NOTICES

EXECUTIVE SUMMARY

+ The number of data compromises reported in 2024 totaled 3,158, essentially flat with the previous year.
+ The number of victim notices increased 211 percent (211%) year-over-year, primarily due to five (5) "mega-breaches" that resulted in at least 100M breach notices being issued in each event. Mega-breach victim notices totaled more than 1B of the more than 1.3B victim notices issued in 2024.
+ Excluding the five (5) mega-breaches, the ~224M other victim notices issued in 2024 represent a 47 percent (47%) decrease in victim notices compared to the previous year.
+ Financial Services, led by Commercial Banks and Insurance, was the most breached industry, followed by Healthcare (the most attacked industry each year since 2018 until this year), Professional Services, Manufacturing and Technology.
+ Cyberattacks remained the primary root cause that resulted in data breaches in 2024. Yet, the number of notices that did not list a specific attack vector increased significantly for the fifth consecutive year.
  + Approximately 70 percent (70%) of cyberattack-related breach notices did not include attack information compared to 58 percent (58%) in 2023. In 2019 and previous years, ~100 percent (~100%) of breach notices included attack vector information.
+ Compromises linked to System and Human Errors dropped by 58 percent (58%) year-over-year; Physical Attack-related compromises such as skimmers and stolen devices dropped to a six-year low – 33 events out of a total of 3,158 compromises reported in 2024.
+ Publicly traded companies represented only seven percent (7%) of all compromised organizations (221 companies) but issued 72 percent (72%) of victim notices (939M) in 2024.
+ Of the 133 cyberattacks against publicly traded companies resulting in a data breach notice, a stolen credential(s) was the leading attack vector. However, 99 of the 133 breached organizations (74 percent) did not list an attack vector in a breach notice.

ANALYSIS

YEAR-OVER-YEAR

Compromises & Victim Notices

Sensitive vs Non-Sensitive Records

Actionable vs Non-Actionable Notices

Attack Vector

PUBLIC VS PRIVATE

Compromises & Victim Notices

Attack Vector

COMPROMISES BY INDUSTRY

FINANCIAL SERVICES BREAKOUT

ANALYSIS

The number of data compromises reported in the United States in 2024 reached the second-highest level since the ITRC began tracking data events in 2005. Compromises totaled 3,158, 44 events short of 2023's record high of 3,202 or an approximately one percent (1%) reduction from the previous 12 months.

However, the number of data breach notices issued by organizations in the past year (1.3B) far exceeded the previous number, largely due to five (5) mega-breaches. Each of those events resulted in victim notices ranging from 100M to 560M, representing 83 percent (83%) of the total number of victim notices issued for all events in 2024.

Adjusting for the small number of mega-breaches, the number of regular victim notices issued in the year – 224M victim notices related to 3,153 compromises – would have been a significant drop from previous years.

COMPROMISES & VICTIM NOTICES

Year-Over-Year

Figure 1 | *Total Compromises & Victim Notices, 2019 – 2024*

	Compromises	*Victim Notices*
2024	3,158	1,350,835,988
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

SENSITIVE VS NON-SENSITIVE RECORDS

Year-Over-Year

The types of information exposed in data compromises, including data breaches, skewed toward sensitive information with a renewed focus on financial information along with a continued increase in driver's license and health information.

Figure 2 | *Sensitive vs Non-Sensitive Records, 2019 – 2024*

	Compromises Involving Sensitive Records	*Percentage*	*Compromises Involving Non-Sensitive Records*	*Percentage*	*Compromises Involving Unknown Records*	*Percentage*
2024	2,655	84%	80	3%	422	13%
2023	2,497	78%	123	4%	582	18%
2022	1,553	86%	76	4%	169	9%
2021	1,554	84%	115	6%	190	10%
2020	883	80%	118	11%	106	10%
2019	1,088	85%	123	10%	67	5%

ACTIONABLE VS NON-ACTIONABLE NOTICES

Year-Over-Year

Information about the root cause of data breaches continued to be elusive in 2024. Almost two-thirds of all notices did not include actionable information about what led to a compromise. Notices without attack vector information increased by 20 percentage points in 2024 over the previous year.

Figure 3 | *Actionable vs Non-Actionable Notices, 2019 – 2024*

	Notices Without Attack Vectors	Percentage	Notices With Attack Vectors	Percentage
2024	2,065	65%	1,093	35%
2023	1,450	45%	1,752	55%
2022	720	40%	1,078	60%
2021	122	7%	1,737	93%
2020	2	0%	1,105	100% (99.9%)
2019	2	0%	1,276	100% (99.9%)

ATTACK VECTOR

Year-Over-Year

The lack of specific information was especially acute when the general attack vector was a cyberattack. Cyberattacks continued to be the primary root cause of most data breaches, but only 30 percent (30%) of notices included any information about the attack vector in 2024. That was a 29 percent (29%) increase over 2023 in a year when the overall number of compromises dropped one percent (1%).

Figure 4 | *Attack Vector, 2019 – 2024*

	2024	2023	2022	2021	2020	2019
Cyberattacks	**2,525**	**2,364**	**1,581**	**1,610**	**876**	**927**
Phishing/Smishing/BEC	455	442	468	537	383	488
Ransomware	188	259	293	352	159	83
Malware	48	119	73	141	103	112
Non-Secured Cloud Environment	3	14	10	24	51	16
Credential Stuffing	29	30	18	14	17	3
Unpatched Software Flaw	2	1	–	4	3	3
Zero Day Attack	17	109	8	4	1	–
Other	27	29	17	424	157	222
Not Specified	1,756	1,361	694	110	2	–
System & Human Error	**310**	**730**	**163**	**179**	**153**	**231**
Failure to Configure Cloud Security	18	24	18	54	58	56
Correspondence (Email/Letter)	114	382	55	66	55	89
Misconfigured Firewall	13	19	30	13	4	4
Lost Device/Documents	14	53	7	12	5	19
Other	130	221	36	34	31	63
Not Specified	21	31	17	–	–	–
Physical Attacks	**33**	**53**	**46**	**51**	**78**	**117**
Document Theft	9	6	7	9	15	19
Device Theft	14	23	21	17	30	57
Improper Disposal	4	5	5	5	11	13
Skimming Device	4	9	6	1	5	4
Other	2	5	6	19	17	24
Not Specified	–	5	1	–	–	–
Data Leak	**2**	**2**	**–**	**7**	**–**	**1**
Unknown	**288**	**53**	**8**	**12**	**–**	**2**

PUBLIC VS PRIVATE COMPROMISES & VICTIM NOTICES

2024

Data breach notices from publicly traded companies represented less than ten percent (10%) of all breach notices but 72 percent (72%) of victims in 2024.

Figure 5 | *Public vs Private Compromises & Victim Notices, 2024*

	Compromises	Victim Notices
Public	221	939,302,369
Private	2,937	411,533,619
Total	**3,158**	**1,350,835,988**

PUBLIC VS PRIVATE ATTACK VECTORS

2024

Publicly traded and privately owned businesses issued breach notices in 2024 that lacked information about the root cause of the breach. Publicly traded companies failed to report specific information 75 percent (75%) of the time. Private companies issued most data breach notices, 69 percent (69%) of which did not include attack vector details.

Figure 6 | *Public vs Private Attack Vector, 2024*

	Public	Private
Cyberattacks	**133**	**2,392**
Phishing/Smishing/BEC	4	451
Ransomware	11	117
Malware	3	45
Non-Secured Cloud Environment	–	3
Credential Stuffing	15	14
Unpatched Software Flaw	–	2
Zero Day Attack	–	17
Other	1	26
Not Specified	99	1,657
System & Human Error	**66**	**244**
Failure to Configure Cloud Security	–	18
Correspondence (Email/Letter)	25	89
Misconfigured Firewall	1	12
Lost Device/Documents	3	11
Other	35	95
Not Specified	2	19

	Public	Private
Physical Attacks	**2**	**31**
Document Theft	–	9
Device Theft	1	13
Improper Disposal	–	4
Skimming Device	–	4
Other	1	1
Not Specified	–	–
Data Leak	–	**2**
Unknown	**20**	**268**

COMPROMISES BY INDUSTRY

Year-Over-Year

The Financial Services industry knocked Healthcare companies out of the top slot as the most compromised industry for the first time since 2018, despite a slight drop in the number of reported compromises among financial institutions compared to 2023. However, nine (9) other industries exceeded the number of victim notices associated with financial institutions and healthcare organizations.

Figure 7 | *Compromises by Industry, 2019 – 2024*

	2024	2023	2022
Education	162 Compromises ~3M Victim Notices	173 Compromises ~5M Victim Notices	99 Compromises ~2M Victim Notices
Financial Services	737 Compromises ~48M Victim Notices	742 Compromises ~81M Victim Notices	270 Compromises ~27M Victim Notices
Government	128 Compromises ~12M Victim Notices	99 Compromises ~15M Victim Notices	74 Compromises ~2M Victim Notices
Healthcare	536 Compromises ~47M Victim Notices	811 Compromises ~60M Victim Notices	341 Compromises ~28M Victim Notices
Hospitality	69 Compromises ~565M Victim Notices	45 Compromises ~6M Victim Notices	34 Compromises ~70M Victim Notices
HR/Staffing	23 Compromises ~345K Victim Notices	11 Compromises ~239K Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	317 Compromises ~51M Victim Notices	258 Compromises ~41M Victim Notices	247 Compromises ~24M Victim Notices
Military	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Mining/Construction	104 Compromises ~226M Victim Notices	71 Compromises ~222K Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	146 Compromises ~2M Victim Notices	102 Compromises ~10M Victim Notices	72 Compromises ~1M Victim Notices
Professional Services	345 Compromises ~3M Victim Notices	310 Compromises ~30M Victim Notices	223 Compromises ~6M Victim Notices
Retail	96 Compromises ~71M Victim Notices	118 Compromises ~10M Victim Notices	65 Compromises ~798K Victim Notices
Social Services	18 Compromises ~359K Victim Notices	16 Compromises ~212K Victim Notices	0 Compromises 0 Victim Notices
Technology	142 Compromises ~326M Victim Notices	167 Compromises ~70M Victim Notices	87 Compromises ~249M Victim Notices
Transportation	88 Compromises ~5M Victim Notices	101 Compromises ~12K Victim Notices	36 Compromises ~4M Victim Notices
Utilities	66 Compromises ~112M Victim Notices	44 Compromises ~73M Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	54 Compromises ~148K Victim Notices	53 Compromises ~434K Victim Notices	0 Compromises 0 Victim Notices
Other	112 Compromises ~105M Victim Notices	80 Compromises ~4M Victim Notices	250 Compromises ~12M Victim Notices
Unknown	15 Compromises ~3K Victim Notices	1 Compromise 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**3,158 Compromises ~1.3B Victim Notices**	**3,202 Compromises ~419M Victim Notices**	**1,798 Compromises ~425M Victim Notices**

	2021	2020	2019
Education	125 Compromises ~2M Victim Notices	43 Compromises ~991K Victim Notices	70 Compromises ~5M Victim Notices
Financial Services	279 Compromises ~20M Victim Notices	136 Compromises ~3M Victim Notices	171 Compromises ~104M Victim Notices
Government	66 Compromises ~3M Victim Notices	47 Compromises ~1M Victim Notices	64 Compromises ~1M Victim Notices
Healthcare	330 Compromises ~33M Victim Notices	306 Compromises ~10M Victim Notices	397 Compromises ~9M Victim Notices
Hospitality	33 Compromises ~238K Victim Notices	17 Compromises ~22M Victim Notices	40 Compromises ~1M Victim Notices
HR/Staffing	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	221 Compromises ~50M Victim Notices	70 Compromises ~3M Victim Notices	103 Compromises ~70M Victim Notices
Military	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	1 Compromise ~1K Victim Notices
Mining/Construction	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	86 Compromises ~2M Victim Notices	31 Compromises ~38K Victim Notices	36 Compromises ~249K Victim Notices
Professional Services	182 Compromises ~23M Victim Notices	144 Compromises ~73M Victim Notices	84 Compromises ~2M Victim Notices
Retail	102 Compromises ~7M Victim Notices	52 Compromises ~11M Victim Notices	86 Compromises ~370M Victim Notices
Social Services	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Technology	79 Compromises ~45M Victim Notices	69 Compromises ~142M Victim Notices	64 Compromises ~108M Victim Notices
Transportation	44 Compromises ~570K Victim Notices	21 Compromises ~1M Victim Notices	15 Compromises ~221K Victim Notices
Utilities	1 Compromises ~51M Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	1 Compromise 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Other	307 Compromises ~80M Victim Notices	171 Compromises ~36M Victim Notices	146 Compromises ~212M Victim Notices
Unknown	4 Compromises ~35K Victim Notices	0 Compromises 0 Victim Notices	1 Compromises 0 Victim Notices
Totals	**1,859 Compromises ~352M Victim Notices**	**1,107 Compromises ~303M Victim Notices**	**1,278 Compromises ~884M Victim Notices**

2024 FINANCIAL SERVICES BREAKOUT

The growth in compromises in the Financial Services category was primarily attributable to a significant rise in attacks against Commercial Banking and Insurance entities during the past two years. A smaller number of increased attacks in other industry segments also contributed to the overall rise in ranking.

Figure 8 | *Compromises by Financial Services, 2019 – 2024*

	2024	2023	2022
Commercial Bank	336 Compromises ~8M Victim Notices	309 Compromises ~3M Victim Notices	30 Compromises ~2M Victim Notices
Insurance	148 Compromises ~12M Victim Notices	175 Compromises ~29M Victim Notices	97 Compromises ~11M Victim Notices
Investment Advice	62 Compromises ~254K Victim Notices	59 Compromises ~1M Victim Notices	2 Compromises 412 Victim Notices
Credit Union	59 Compromises ~2M Victim Notices	47 Compromises ~587K Victim Notices	4 Compromises ~11K Victim Notices
Other Financial	51 Compromises ~6M Victim Notices	44 Compromises ~760K Victim Notices	66 Compromises ~4M Victim Notices
Investment Bank	43 Compromises ~236K Victim Notices	34 Compromises ~9M Victim Notices	41 Compromises ~8M Victim Notices
Retail Bank	20 Compromises 305 Victim Notices	39 Compromises ~5M Victim Notices	4 Compromises ~3K Victim Notices
Mortgage Lender	14 Compromises ~18M Victim Notices	24 Compromises ~33M Victim Notices	21 Compromises ~3M Victim Notices
Payment Processor	2 Compromises ~2M Victim Notices	5 Compromises ~69K Victim Notices	5 Compromises ~172K Victim Notices
Credit Card Issuer	2 Compromises ~100K Victim Notices	2 Compromises ~91K Victim Notices	0 Compromises 0 Victim Notices
Private Bank	0 Compromises 0 Victim Notices	4 Compromises ~1K Victim Notices	0 Compromises 0 Victim Notices
Totals	**737 Compromises ~48M Victim Notices**	**742 Compromises ~81M Victim Notices**	**270 Compromises ~27M Victim Notices**

	2021	2020	2019
Commercial Bank	42 Compromises ~438K Victim Notices	22 Compromises ~63K Victim Notices	23 Compromises ~100M Victim Notices
Insurance	133 Compromises ~11M Victim Notices	55 Compromises ~2M Victim Notices	81 Compromises ~3M Victim Notices
Investment Advice	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Credit Union	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Other Financial	54 Compromises ~574K Victim Notices	34 Compromises ~414K Victim Notices	37 Compromises ~203K Victim Notices
Investment Bank	26 Compromises ~7M Victim Notices	16 Compromises ~624K Victim Notices	21 Compromises ~158K Victim Notices
Retail Bank	4 Compromises ~80K Victim Notices	0 Compromises 0 Victim Notices	2 Compromises ~10K Victim Notices
Mortgage Lender	17 Compromises ~559K Victim Notices	5 Compromises ~19K Victim Notices	2 Compromises ~2K Victim Notices
Payment Processor	1 Compromises ~2K Victim Notices	4 Compromises ~9K Victim Notices	1 Compromises 0 Victim Notices
Credit Card Issuer	2 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	3 Compromises 229 Victim Notices
Private Bank	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	1 Compromises ~3K Victim Notices
Totals	**279 Compromises ~20M Victim Notices**	**136 Compromises ~3M Victim Notices**	**171 Compromises ~104M Victim Notices**

2024 INSIGHTS

BETTER CYBER PRACTICES & REQUIREMENTS COULD PREVENT COMPROMISES

DISCLOSURE REQUIREMENTS HAVE NO SIGNIFICANT IMPACT

MEGA-BREACHES SHOW SCALE BUT OFTEN MASK IMPACT

AI IS LIKELY IMPACTING COMPROMISES BUT CAN BE USED FOR PREVENTION

ZERO DAY & SUPPLY CHAIN ATTACKS

2024 INSIGHTS

BETTER CYBER PRACTICES & REQUIREMENTS COULD PREVENT MANY DATA COMPROMISES; STATES MAY LEAD THE WAY

At least 196[5] of the compromises reported in 2024 could have been prevented, including three (3) of the five (5) mega-breaches that resulted in 860M victim notices being issued. Attacks using stolen credentials against Ticketmaster, AT&T and Change Healthcare could have been blocked with the addition of Multi-factor Authentication (MFA). In testimony before Congress, Change executives admitted that attackers broke into Change Healthcare's systems using a single password on a user account not protected with MFA.

At least 21 compromises were linked to misconfigured or non-secured cloud environments, and at least 114 compromises were linked to files being attached to emails or in physical correspondence – events that could have been avoided with improved employee training and process monitoring tools.

Attacks against known and unknown software flaws resulted in at least 83 attacks that could have been blocked with the adoption of cybersecurity best practices, including Zero Trust cybersecurity practices, improved software development processes like those recommended by the U.S. Cybersecurity & Infrastructure Security Agency (CISA), practices recommended by the National Institute of Standards and Technology (NIST) and improved testing, monitoring and patching.

At least 29 cyberattacks reported last year involved "credential stuffing" attacks using compromised logins and passwords that could have been prevented with MFA or passkeys. As mentioned in the introduction to this report, passkeys, when fully implemented for internal and external use, offer the opportunity to all but eliminate[6] credential stuffing and other credential-related attacks.

While it's too early to tell the degree to which state privacy laws will help prevent future data compromises[7], states continue to step into the data protection void created by Congress's failure to adopt a national privacy law in 2024. Twenty (20) states have passed comprehensive privacy laws[8], eight (8) of which go into effect in 2025:

+ ***Iowa*** – Data Privacy Law
  Effective January 1, 2025
+ ***Delaware*** – Personal Data Privacy Act
  Effective January 1, 2025
+ ***Nebraska*** – Data Privacy Act
  Effective January 1, 2025
+ ***New Hampshire*** – Privacy Act
  Effective January 1, 2025
+ ***New Jersey*** – Data Privacy Law
  Effective January 15, 2025
+ ***Tennessee*** – Information Protection Act
  Effective July 1, 2025
+ ***Minnesota*** – Consumer Data Privacy Act
  Effective July 15, 2025
+ ***Maryland*** – Online Data Privacy Act
  Effective October 1, 2025

Four states – Michigan, Oklahoma, Pennsylvania and Ohio – have had privacy legislation carried over from 2024 or have already been introduced for the 2025 legislative session.

Small business leaders who responded to the ITRC's annual Small Business Cyber questionnaire were very aware of their state's new cybersecurity requirements (77 percent). However, an almost equal number were concerned about how they would comply (76 percent).

STATE & FEDERAL DISCLOSURE REQUIREMENTS ARE HAVING NO SIGNIFICANT IMPACT ON DATA BREACHES

The number of data breach notices that did not include actionable information, such as the root cause of the compromise, increased in the past year. In 2024, 70 percent (70%) of data breach notices associated with cyberattacks did not contain information about the root cause of the attack, an increase of 20 percentage points in one year. The overall number of compromises with no root cause information grew 21 percentage points year-over-year. Before 2020, the number of deficient breach notices was at or near zero.

Each state and some federal agencies define a breach differently, as well as what information must be disclosed and when. Importantly, each state allows the organization that has been compromised to determine if disclosure is required. If the organization believes there is no risk to a person from the information being exposed or stolen, then no notice is required.

This patchwork quilt of state laws and federal regulations with wildly varying disclosure requirements leads to a significant amount of underreporting. How significant is akin to proving a negative, but there is plenty of anecdotal evidence[9] to support the conclusion. In the U.S., there are an average of nine (9) data compromises reported each day compared to 335 per day in the European Union, which also requires data breach notifications[10].

The ITRC is not the only organization that has concluded that data breach notices suffer from a lack of helpful information. The U.S. Securities and Exchange Commission breach disclosure rules adopted in 2023 required publicly traded companies to disclose cyber incidents within four business days after determining an incident is material. That resulted in a 60 percent (60%) increase in disclosures in 2024, but less than ten percent (10%) of the notices included details of the cyber event's impact, including breaches, according to an analysis by the global law firm Paul Hastings[11].

States occasionally update their state data breach notice laws in reaction to trends. Most recently, New York added health and health insurance information[12] to the list of items that can trigger a data breach, effective January 2025. Empire State lawmakers also updated the amount of time breached organizations have to inform victims from the previous "most expedient time possible and without reasonable delay" to 30 days from discovering a breach. The latest change in the New York breach law also requires the state Department of Financial Services to be notified of all breaches – not just by organizations regulated by the agency – along with the Attorney General and two other state agencies.

MEGA-BREACHES SHOW THE SCALE OF COMPROMISES BUT OFTEN MASK THE IMPACT ON PEOPLE

Headline-grabbing mega-breaches forced the distribution of more than 1B victim notices in 2024. Additionally, initial reports related to a breach at data broker National Public Data claimed that 2.9B people were impacted by the compromise. That was later revealed to be 2.9B records, which impacted an estimated 1.3M people.

Figure 9 | *Top 10 Compromises, 2024*

	Entity	Victim Notices
1	Ticketmaster Entertainment, LLC	560,000,000
2	Change Healthcare	190,000,000
3	DemandScience by Pure Incubation	121,796,165
4	AT&T	110,000,000
5	MC2 Data	100,000,000
6	Hot Topic, Inc.	56,904,909
7	Dell Technologies, Inc.	49,000,000
8	LoanDepot, Inc.	16,924,071
9	Kaiser Foundation Health Plan, Inc.	13,400,000
10	U.S. Environmental Protection Agency	8,460,182

Five (5) mega-breaches[13] account for only .001 percent (.001%) of compromises in the past year but ~83 percent (~83%) of data breach notices. Adjusting for the mega-breaches, data breach notices in 2024 were the lowest number of alerts issued since the final set of states adopted data breach laws in 2018.

There are risks that come with overly focusing on mega-breaches. They give consumers a skewed sense of risks and contribute to a sense of "breach fatigue" and despair. Focusing on mega-breaches may also result in businesses – especially small businesses – mis-allocating limited cybersecurity and data protection resources.

While consumers can have little impact on preventing data compromises, they can take actions to make their personal information less useful to bad actors. Adopting and updating basic cyber hygiene practices involve simple and easy-to-take steps. However, they can seem overwhelming in the face of compromises linked to numbers that can exceed the total population of the U.S.

The ITRC offers free information for people who want to learn about protecting their personal information and support for people who have questions about what steps to take after they receive a data breach notice.

If you receive a data breach notice, take the following immediate actions:

+ Freeze your credit. Find out how at FrozenPII.com powered by the ITRC.
+ Change the password of any impacted account and any account where you use the same password.
+ If you use the same password on more than one account, set up unique passwords on each account you own to prevent all of your accounts from being compromised.
+ Set up passkeys where available.
+ Set up Multi-factor Authentication if you can't create a passkey.
+ Sign up for any credit monitoring or identity restoration services offered in a breach notice letter.
+ Contact the ITRC for additional help free of charge.

ARTIFICIAL INTELLIGENCE IS LIKELY CAUSING DATA COMPROMISES, BUT IT CAN ALSO BE USED TO PREVENT THEM

No data breach notice directly linked the use of Artificial Intelligence (AI) to a compromise in 2024. However, it's clear that AI is enabling identity-related phishing attacks and identity scams that do lead to data compromises. The quality of phishing lures – emails, spoofed websites, texts, pitch scripts, etc. – has dramatically improved since the introduction of generative AI into the mainstream in 2022. At least 455 cyberattacks in 2024 were linked to some form of phishing[14].

Threat actors are gearing up to launch a new wave of attacks fueled by AI to find known and unknown software flaws in enterprise applications as well as bypass system protections[15]. These kinds of technical innovations have typically been the precursor to exponential increases in data breaches, most recently seen in 2023 after low-cost data breach toolkits flooded identity crime marketplaces.

However, AI also offers defenders the same opportunities to improve detection, defenses and remediation. AI can improve the monitoring of systems and inbound traffic to look for indications of attacks. AI-driven tools in the hands of software developers can help find and fix flaws before an application is put into production. In other words, the defenders can use AI for the same purposes as attackers to prevent the mistakes that threat actors want (and need) to exploit.

A SPECIAL NOTE ABOUT ZERO DAY & SUPPLY CHAIN ATTACKS

There were fewer data breaches directly linked to Zero Day and Supply Chain[16] attacks in 2024 compared to the previous year.

However, since more data breach notices linked to cyberattacks did not include the attack vector that led to the breach, it is not possible to know the actual number of Zero Day and Supply Chain-based breaches.

Figure 10 | *Zero Day & Supply Chain Attacks, 2020 – 2024*

	Zero Day Breaches	Zero Day Victim Notices	Third-Party/Supply Chain Attacks	Entities Impacted By Third-Party/Supply Chain Attacks	Third-Party/Supply Chain Victim Notices
2024	17	1,857,149	134	657	203,144,092
2023	109	76,206,344	242	2,768	58,420,366
2022	8	233,201,188	115	1,748	10,396,314
2021	4	7,959,343	84	558	25,680,516
2020	1	–	69	687	42,401,304

Zero Day attacks (exploits against previously unknown software vulnerabilities) continued to be a significant focus of attackers, with at least 17 attacks resulting in 1,857,149 victim notices.

Supply Chain attacks (attacks against third-party vendors who hold the information of multiple larger organizations) directly impacted 134 organizations and indirectly impacted an additional 657 entities, resulting in 203,144,092 victim notices, 190M of which were related to the Change Healthcare breach.

Change Healthcare is a major part of the healthcare supply chain that processes approximately one-third of all medical claims in the U.S., according to company executives. On January 24, 2025 after the end of the trading day on the NYSE, Change Healthcare's parent company, United Healthcare (NYSE:UNH) updated the number of victim notices issued related to a February 2024 cyberattack. UNH reported 190M victims impacted, but has yet to disclose how many companies in their supply chain have been impacted by the ransomware attack. UNH has indicated it will file additional updates in the future with the U.S. Department of Health & Human Services.

[5]Because 2,065 of the 3,158 public data compromise reports did not include information in 2024 about the root cause of the data compromise, it is not possible to determine precisely how many events could have been blocked or prevented.

[6]Identity Access Management (IAM) and security experts agree that password use is unlikely to be completely eliminated, but the risk of credential attacks will be dramatically reduced, especially when combined with app-based MFA.

[7]Small business leaders who responded to the ITRC's annual Small Business Cyber questionnaire were very aware of their state's new cybersecurity requirements (77 percent). However, an almost equal number were concerned about how they would comply (76 percent).

[8]Nineteen (19) of the 20 states that have passed comprehensive privacy laws include cybersecurity provisions to varying degrees. Learn more about current and proposed state privacy laws here.

[9]"As a result, notification to the consumers whose personal information was exposed was significantly delayed or never occurred at all, as Blackbaud downplayed the incident and led its customers to believe that no notification was required." (Emphasis added) Attorney General James and Multistate Coalition Secure $49.5 Million from Cloud Company for Data Breach

[10]"Continuing the trend of the last couple of years, on average, there were 335 breach notifications per day from 28 January 2023 to 27 January 2024 compared to 328 during the same period last year." - DLA Piper GDPR Fines and Data Breach Survey: January 2024

[11]See analysis from Paul Hastings: SEC Cybersecurity Incident Disclosure Report

[12]Healthcare was the most breached industry from 2019 through 2023, prompting regulators to propose changes to state and federal breach notice and cybersecurity requirements. HIPAA Security Rule Notice of Proposed Rulemaking to Strengthen Cybersecurity for Electronic Protected Health Information

[13]Advanced Auto Parts was among customers of a popular cloud data storage platform where more than 100 companies were breached that did not require multi-factor authentication for account access, a basic cybersecurity tool that could have prevented the attack from succeeding. Initial reports from security researchers and claims from the threat actors who attacked Advanced Auto Parts indicated ~380M customer and company accounts were compromised that included personal information. While security researchers claim customer information was included in the stolen information, Advanced Auto Parts filed a breach notice with the State of Maine stating the personal information of only ~2.3M current and former employees as well as job applicants was compromised. The ITRC initially reported the higher number of victims, but has updated the information regarding the Advanced Auto Parts breach to reflect the lower number of victim notices in keeping with our revised victim count methodology.

[14]Because 2,065 of the 3,158 public data compromise reports in 2024 did not include information about the root cause of the data compromise, it is not possible to determine precisely how many events were linked to phishing attacks.

[15]Ransomware Gangs Seek Pen Testers to Boost Quality

[16]Supply Chain attacks are classified within cyberattacks since they are not classified by the ITRC as attack vectors. Only the organization breached, not the number of organizations whose data was compromised, are included in the event count.

SOLUTIONS

ALLIANCE FOR IDENTITY RESILIENCE (AIR) ADVISORY BOARD

CONTACT CENTER SUPPORT FOR BUSINESS

CERTIFIED IDENTITY RECOVERY SPECIALIST TRAINING

DATA SERVICES

ANNUAL IDENTIVATION CONFERENCE

SOLUTIONS

The ITRC is a 501(c)3 nonprofit that provides identity remediation, free of charge, to victims of identity crime and education assistance to people seeking to protect their identity. The Center also provides, for a fee, data services as well as contact center support and training services for businesses, government agencies and academic institutions.

The ITRC does not engage in lobbying but does provide objective research and victim-based information to policymakers and business leaders on topics related to identity verification, identity crimes, data protection and privacy.

We gather information from online surveys, anonymized victim case notes and input from subject matter experts to identify possible solutions. The ITRC is currently focusing on the use of biometrics to improve identity verification and reduce identity crimes. The ITRC will expand to focus on data protection and privacy solutions in 2025.

The ITRC offers a range of subject matter activities and services.

ALLIANCE FOR IDENTITY RESILIENCE (AIR) ADVISORY BOARD

Currently, the ITRC hosts an AIR advisory board, which is the primary advisory board for the ITRC, and a Biometric Cohort focused on the use of biometrics in identity verification. A new advisory board on comprehensive data protection (privacy and cybersecurity) will convene in 2025.

CONTACT CENTER SUPPORT FOR BUSINESS

Designed as either a first-stop or an escalation service, organizations can provide direct access to trained ITRC expert advisors where victims will receive personalized, concierge-level support based on their unique needs.

The ITRC offers businesses a variety of trauma-informed and culturally aware support services to help organizations address the wide range of unique issues experienced by their customers who are identity crime victims.

CERTIFIED IDENTITY RECOVERY SPECIALIST TRAINING

The ITRC offers a certificate training program for customer support center representatives. The ITRC's new Certified Identity Recovery Specialist training program provides front-line staff with the tools and skills needed to effectively partner with customers or prospects who are identity crime victims in a supportive and effective way.

DATA SERVICES

Consumers may access the latest information about data breaches and enroll in *Breach Alert for Consumers* to receive an email when an organization where they have an account issues a data breach notice. These services are free to individuals.

Businesses, government agencies and academic institutions may access the ITRC's comprehensive data breach database that dates back to 2005 on a paid batch or subscription basis.

Breach Alert for Business allows businesses to conduct due diligence and monitor partner organizations and prospective vendors. This paid service includes unlimited breach searches and future breach monitoring alerts.

ANNUAL IDENTIVATION CONFERENCE

Each year, the ITRC hosts a meeting with senior leaders from all levels of government and the private sector to discuss the latest trends and innovations in identity, privacy and data protection. The 2025 Identivation (Identity + Innovation) Conference is invitation only and is scheduled for October 2025 in Washington, D.C.

ADDITIONAL RESOURCES

SIGNATURE REPORTS

The ITRC publishes comprehensive signature reports and analysis throughout the year.

CONSUMER IMPACT – BUSINESS IMPACT REPORT (CIBIR)

Published October 2024

The CIBIR is a research and analysis report of the impacts identity crimes have on victims who contact the ITRC compared to a representative sample of general consumers. The report also includes analysis of the impact of cyberattacks and data breaches on small businesses based on an online survey of business owners and executives.

TRENDS IN IDENTITY REPORT (TIR)

Published June 2024

Based on the information provided by the identity crime victims and consumers who contact the ITRC for assistance, the TIR offers insight into current and emerging identity issues that victims have faced in the previous year.

DATA BREACH REPORT (DBR)

Published January 2024

The DBR looks at the number of data compromises, the types of data compromised, the root causes of data compromises and much more.

PODCASTS

Posted Weekly

The ITRC offers two podcasts that cover a wide range of issues that impact people and businesses when it comes to identity crimes and cybersecurity.

The *Weekly Breach Breakdown* is posted three times a month and focuses on the latest data breaches and cybersecurity issues.

The *Fraudian Slip* is a monthly discussion podcast where ITRC experts and guests talk about the latest trends in identity.

Join us wherever you listen to your favorite podcasts.

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.

CONTRIBUTORS

Thanks to the team responsible for the *2024 ITRC Data Breach Report*:

Data Team – Colleen Huppert, Maria Almanza
Analysis & Editorial – James E. Lee
Layout & Design – Meagan Lechleiter

ITRC | IDENTITY THEFT RESOURCE CENTER

JANUARY 2025

APPENDIX

END OF YEAR

2024 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

3,158 Compromises
1,350,835,988 Victim Notices

Data Breaches

2,850 Breaches
1,246,573,396 Victim Notices

Data Exposures

18 Exposures
100,153,761 Victim Notices

Data Leaks

2 Leaks
2,795,947 Victim Notices

Unknown

288 Unknown Compromises
1,312,884 Victim Notices

ATTACK VECTORS

CYBERATTACKS

2,525 Breaches
1,229,866,035 Victim Notices

+ 455 Phishing/Smishing/BEC
+ 188 Ransomware
+ 48 Malware
+ 29 Credential Stuffing
+ 17 Zero-Day Attack
+ 3 Non-Secured Cloud Environment
+ 2 Unpatched Software Flaw (CVE)
+ 27 Other
+ 1,756 Not Specified

SYSTEM & HUMAN ERROR

310 Breaches/Exposures
116,671,768 Victim Notices

+ 114 Correspondence (Email/Letter)
+ 18 Failure to Configure Cloud Security
+ 14 Lost devices or documents
+ 13 Misconfigured Firewalls
+ 130 Other
+ 21 Not Specified

PHYSICAL ATTACKS

33 Breaches/Exposures
189,354 Victim Notices

+ 14 Device Theft
+ 9 Document Theft
+ 4 Improper Disposal
+ 4 Skimming devices
+ 2 Other

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

637 Entities Affected
201,803,150 Victim Notices

System & Human Errors

19 Entities Affected
1,340,942 Victim Notices

Physical Attack

1 Entity Affected
Unknown Number of Victim Notices

YEAR-OVER-YEAR

Compromise Year-Over-Year Totals, 2019 – 2024

	Compromises	*Victim Notices*
2024	3,158	1,350,835,988
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Top 10 Compromises, 2024

	Entity	*Victim Notices*
1	Ticketmaster Entertainment, LLC	560,000,000
2	Change Healthcare	190,000,000
3	DemandScience by Pure Incubation	121,796,165
4	AT&T	110,000,000
5	MC2 Data	100,000,000
6	Hot Topic, Inc.	56,904,909
7	Dell Technologies, Inc.	49,000,000
8	LoanDepot, Inc.	16,924,071
9	Kaiser Foundation Health Plan, Inc.	13,400,000
10	U.S. Environmental Protection Agency	8,460,182

Sensitive vs Nonsensitive Records, 2019 – 2024

	Compromises Involving Sensitive Records	*Percentage*	*Compromises Involving Non-Sensitive Records*	*Percentage*	*Compromises Involving Unknown Records*	*Percentage*
2024	2,655	84%	80	3%	422	13%
2023	2,497	78%	123	4%	582	18%
2022	1,553	86%	76	4%	169	9%
2021	1,554	84%	115	6%	190	10%
2020	883	80%	118	11%	106	10%
2019	1,088	85%	123	10%	67	5%

Compromises by Industry, 2019 – 2024

	2024	*2023*	*2022*
Education	162 Compromises ~3M Victim Notices	173 Compromises ~5M Victim Notices	99 Compromises ~2M Victim Notices
Financial Services	737 Compromises ~48M Victim Notices	742 Compromises ~81M Victim Notices	270 Compromises ~27M Victim Notices
Government	128 Compromises ~12M Victim Notices	99 Compromises ~15M Victim Notices	74 Compromises ~2M Victim Notices
Healthcare	536 Compromises ~47M Victim Notices	811 Compromises ~60M Victim Notices	341 Compromises ~28M Victim Notices
Hospitality	69 Compromises ~565M Victim Notices	45 Compromises ~6M Victim Notices	34 Compromises ~70M Victim Notices
HR/Staffing	23 Compromises ~345K Victim Notices	11 Compromises ~239K Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	317 Compromises ~51M Victim Notices	258 Compromises ~41M Victim Notices	247 Compromises ~24M Victim Notices
Military	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Mining/Construction	104 Compromises ~226M Victim Notices	71 Compromises ~222K Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	146 Compromises ~2M Victim Notices	102 Compromises ~10M Victim Notices	72 Compromises ~1M Victim Notices
Professional Services	345 Compromises ~3M Victim Notices	310 Compromises ~30M Victim Notices	223 Compromises ~6M Victim Notices
Retail	96 Compromises ~71M Victim Notices	118 Compromises ~10M Victim Notices	65 Compromises ~798K Victim Notices
Social Services	18 Compromises ~359K Victim Notices	16 Compromises ~212K Victim Notices	0 Compromises 0 Victim Notices
Technology	142 Compromises ~326M Victim Notices	167 Compromises ~70M Victim Notices	87 Compromises ~249M Victim Notices
Transportation	88 Compromises ~5M Victim Notices	101 Compromises ~12K Victim Notices	36 Compromises ~4M Victim Notices
Utilities	66 Compromises ~112M Victim Notices	44 Compromises ~73M Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	54 Compromises ~148K Victim Notices	53 Compromises ~434K Victim Notices	0 Compromises 0 Victim Notices
Other	112 Compromises ~105M Victim Notices	80 Compromises ~4M Victim Notices	250 Compromises ~12M Victim Notices
Unknown	15 Compromises ~3K Victim Notices	1 Compromise 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**3,158 Compromises ~1.3B Victim Notices**	**3,202 Compromises ~419M Victim Notices**	**1,798 Compromises ~425M Victim Notices**

	2021	*2020*	*2019*
Education	125 Compromises ~2M Victim Notices	43 Compromises ~991K Victim Notices	70 Compromises ~5M Victim Notices
Financial Services	279 Compromises ~20M Victim Notices	136 Compromises ~3M Victim Notices	171 Compromises ~104M Victim Notices
Government	66 Compromises ~3M Victim Notices	47 Compromises ~1M Victim Notices	64 Compromises ~1M Victim Notices
Healthcare	330 Compromises ~33M Victim Notices	306 Compromises ~10M Victim Notices	397 Compromises ~9M Victim Notices
Hospitality	33 Compromises ~238K Victim Notices	17 Compromises ~22M Victim Notices	40 Compromises ~1M Victim Notices
HR/Staffing	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	221 Compromises ~50M Victim Notices	70 Compromises ~3M Victim Notices	103 Compromises ~70M Victim Notices
Military	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	1 Compromise ~1K Victim Notices
Mining/Construction	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	86 Compromises ~2M Victim Notices	31 Compromises ~38K Victim Notices	36 Compromises ~249K Victim Notices
Professional Services	182 Compromises ~23M Victim Notices	144 Compromises ~73M Victim Notices	84 Compromises ~2M Victim Notices
Retail	102 Compromises ~7M Victim Notices	52 Compromises ~11M Victim Notices	86 Compromises ~370M Victim Notices
Social Services	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Technology	79 Compromises ~45M Victim Notices	69 Compromises ~142M Victim Notices	64 Compromises ~108M Victim Notices
Transportation	44 Compromises ~570K Victim Notices	21 Compromises ~1M Victim Notices	15 Compromises ~221K Victim Notices
Utilities	1 Compromises ~51M Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	1 Compromise 0 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Other	307 Compromises ~80M Victim Notices	171 Compromises ~36M Victim Notices	146 Compromises ~212M Victim Notices
Unknown	4 Compromises ~3K Victim Notices	0 Compromises 0 Victim Notices	1 Compromises 0 Victim Notices
Totals	**1,859 Compromises ~352M Victim Notices**	**1,107 Compromises ~303M Victim Notices**	**1,278 Compromises ~884M Victim Notices**

TOP 5 INDUSTRIES

2024

1. ***Financial*** – 737 Compromises
2. ***Healthcare*** – 536 Compromises
3. ***Professional Services*** – 345 Compromises
4. ***Manufacturing*** – 317 Compromises
5. ***Education*** – 162 Compromises

2023

1. ***Healthcare*** – 811 Compromises
2. ***Financial*** – 742 Compromises
3. ***Professional Services*** – 310 Compromises
4. ***Manufacturing*** – 258 Compromises
5. ***Education*** – 173 Compromises

2022

1. ***Healthcare*** – 343 Compromises
2. ***Financial*** – 269 Compromises
3. ***Other*** – 250 Compromises
4. ***Manufacturing*** – 249 Compromises
5. ***Professional Services*** – 223 Compromises

2021

1. ***Healthcare*** – 330 Compromises
2. ***Other*** – 307 Compromises
3. ***Financial*** – 279 Compromises
4. ***Manufacturing*** – 221 Compromises
5. ***Professional Services*** – 182 Compromises

2020

1. ***Healthcare*** – 306 Compromises
2. ***Other*** – 171 Compromises
3. ***Professional Services*** – 144 Compromises
4. ***Financial*** – 136 Compromises
5. ***Manufacturing*** – 70 Compromises

2019

1. ***Healthcare*** – 397 Compromises
2. ***Financial*** – 171 Compromises
3. ***Other*** – 146 Compromises
4. ***Manufacturing*** – 103 Compromises
5. ***Retail*** – 86 Compromises

***Attack Vector**, 2019 – 2024*

	2024	2023	2022	2021	2020	2019
Cyberattacks	**2,525**	**2,364**	**1,581**	**1,610**	**876**	**927**
Phishing/Smishing/BEC	455	442	468	537	383	488
Ransomware	188	259	293	352	159	83
Malware	48	119	73	141	103	112
Non-Secured Cloud Environment	3	14	10	24	51	16
Credential Stuffing	29	30	18	14	17	3
Unpatched Software Flaw	2	1	–	4	3	3
Zero Day Attack	17	109	8	4	1	–
Other	27	29	17	424	157	222
Not Specified	1,756	1,361	694	110	2	–
System & Human Error	**310**	**730**	**163**	**179**	**153**	**231**
Failure to Configure Cloud Security	18	24	18	54	58	56
Correspondence (Email/Letter)	114	382	55	66	55	89
Misconfigured Firewall	13	19	30	13	4	4
Lost Device/Documents	14	53	7	12	5	19
Other	130	221	36	34	31	63
Not Specified	21	31	17	–	–	–
Physical Attacks	**33**	**53**	**46**	**51**	**78**	**117**
Document Theft	9	6	7	9	15	19
Device Theft	14	23	21	17	30	57
Improper Disposal	4	5	5	5	11	13
Skimming Device	4	9	6	1	5	4
Other	2	5	6	19	17	24
Not Specified	–	5	1	–	–	–
Data Leak	**2**	**2**	**–**	**7**	**–**	**1**
Unknown	**288**	**53**	**8**	**12**	**–**	**2**

***Compromises Containing PII Types**, 2019 – 2024*

	2024	2023	2022	2021	2020	2019
Social Security Number (SSN)	1,825	1,713	1,215	1,151	562	638
Protected Health Information (PHI)	884	790	604	563	409	483
Driver's License (DI)	851	714	558	456	219	227
Bank Account	901	826	506	417	218	220
Email/Password	205	251	188	254	232	194
Credit/Debit Card	672	599	211	215	181	236
Other	407	370	245	255	200	221

Compromises Containing PII Piece, 2019 – 2024

	2024	2023	2022	2021	2020	2019
Name	2,718	2,599	1,613	1,620	953	1,173
Full Social Security Number	1,817	1,706	1,215	1,146	560	640
Date of Birth	911	847	660	688	428	513
Bank Account Number	890	811	501	410	212	204
Current House Address	806	806	588	688	430	521
Undisclosed Records	423	583	169	190	107	68
Driver's License/State ID Number	857	717	557	456	218	225
Medical History/Condition/ Treatment/Diagnosis	812	701	507	469	360	430
Full Payment Card Number	671	600	211	212	179	236
Medical Insurance Account Number	531	413	390	365	258	339
Phone Number	250	293	169	220	158	192
Payment Cardholder Name	326	242	181	178	153	197
Payment Card Expiration Date	319	233	155	175	152	193
Personal Email Address	193	244	160	211	199	189
Payment Card Security Code	301	212	153	171	142	189
Medical Provider Account Number/ Medical Record Number	258	211	193	198	194	234
Passport Number/Visitor Status/ Green Card	229	201	145	118	77	63
Bank Account Routing Number	74	97	82	91	67	136
Other Account Credentials	41	57	46	42	66	46
Tax ID Number	51	57	11	9	27	41
Income/Wages/Earnings/ Compensation	8	35	36	40	41	40
Employee ID Number/ Credentials/Position	16	24	13	25	18	9
Work Email Address	13	22	10	32	21	30
Student ID Number/Student Login/ Student Details	17	17	21	21	8	17
IP Address/Device ID	11	13	12	12	10	22
Biometric/Authentication Data	12	12	17	12	5	3
Partial Social Security Number	6	14	9	13	2	10
Loan Account Details/Credentials	11	12	13	6	4	11
Employer Name	15	11	7	17	32	34
Bank Account Login Credentials	7	10	7	4	3	8
Other Biographical	1	8	5	14	12	1
Employer Contact Information	11	10	3	16	11	2
Partial Payment Card Number	12	8	9	13	8	6
Investment Account Details/Credentials	9	6	7	7	–	19
Merchant Login	–	6	2	5	–	10
Education	5	6	3	3	3	1
Insurance Account Details/Credentials	10	4	6	5	9	12
Medical Provider Login Credentials	11	4	11	15	6	–
Medical Insurance Account Credentials	3	3	4	14	3	–
W2 Other Information	12	3	4	3	3	–
Location	3	4	1	4	3	–
Personal Email Account Credentials	2	3	2	–	1	2
Employer Site/System Access Credentials	5	2	1	6	2	4
Friends/Family	3	2	–	7	4	1
Financial Account PIN	1	2	–	6	6	18
Work Email Account Credentials	–	2	–	–	–	2
Prior Home Address	4	1	3	3	8	4
Phone Account Credentials	–	1	–	4	–	1
Social Media Login Credentials	1	1	–	1	4	5
Affiliations	–	1	–	–	1	–
Utility Account Number	1	–	–	2	–	–
Utility Account Credentials	–	–	–	–	1	–
Security Clearance/Access	–	–	–	–	–	2
Hometown	–	–	–	–	1	–
Voter Registration Information/ Preferences	1	–	–	–	1	–
Web History/Preferences	–	–	–	–	1	–
Credit Dispute Information	–	–	–	–	–	–
Non-Debit Payment Account Credentials	–	–	–	–	–	–

Actionable vs Non-Actionable Notices, 2019 – 2024

	Notices Without Attack Vectors	Percentage	Notices With Attack Vectors	Percentage
2024	2,065	65%	1,093	35%
2023	1,450	45%	1,752	55%
2022	720	40%	1,078	60%
2021	122	7%	1,737	93%
2020	2	0%	1,105	100% (99.9%)
2019	2	0%	1,276	100% (99.9%)

Total Compromises & Victim Notices, 2005 – 2024

	Compromises	Victim Notices
2024	3,158	1,350,835,988
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154
2018	1,175	2,224,601,976
2017	1,505	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

PUBLIC VS PRIVATE

***Compromises & Victim Notices**, 2024*

	Compromises	*Victim Notices*
Public	221	939,302,369
Private	2,937	411,533,619
Total	**3,158**	**1,350,835,988**

***Attack Vectors**, 2024*

	Public	*Private*
Cyberattacks	**133**	**2,392**
Phishing/Smishing/BED	4	451
Ransomware	11	177
Malware	3	45
Non-Secured Cloud Environment	–	3
Credential Stuffing	15	14
Unpatched Software Flaw	–	2
Zero Day Attack	–	17
Other	1	26
Not Specified	99	1,657
System & Human Error	**66**	**244**
Failure to Configure Cloud Security	–	18
Correspondence (Email/Letter)	25	89
Misconfiguration	1	12
Lost Device or Document	3	11
Other	35	95
Not Specified	2	19
Physical Attacks	**2**	**31**
Document Theft	–	9
Device Theft	1	13
Improper Disposal	–	4
Skimming Device	–	4
Other	1	1
Non Specified	–	–
Data Leak	**–**	**2**
Unknown	**20**	**268**

2024 BREAKDOWN

Q1 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

835 Compromises
38,360,202 Victim Notices

Data Breaches

735 Breaches
38,240,538 Victim Notices

Data Exposures

4 Exposures
20,600 Victim Notices

Data Leaks

0 Leaks
0 Victim Notices

Unknown

96 Unknown
99,064 Victim Notices

ATTACK VECTORS

CYBERATTACKS

644 Breaches
37,812,047 Victim Notices

+ 108 Phishing/Smishing/BEC
+ 60 Ransomware
+ 12 Malware
+ 10 Credential Stuffing
+ 5 Zero-Day Attack
+ 2 Unpatched Software Flaw (CVE)
+ 1 Non-Secured Cloud Environment
+ 8 Other
+ 438 Not Specified

SYSTEM & HUMAN ERROR

84 Breaches/Exposures
396,720 Victim Notices

+ 29 Correspondence (Email/Letter)
+ 4 Failure to Configure Cloud Security
+ 4 Misconfigured Firewalls
+ 4 Lost Device or Document
+ 36 Other
+ 7 Not Specified

PHYSICAL ATTACKS

11 Breaches/Exposures
52,371 Victim Notices

+ 6 Device Theft
+ 2 Document Theft
+ 1 Skimming Device
+ 1 Improper Disposal
+ 1 Other

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

241 Entities Affected
7,458,724 Victim Notices

System & Human Errors

4 Entities Affected
52,061 Victim Notices

Physical Attack

0 Entities Affected
Unknown Number of Victim Notices

CHARTS

Top 10 Compromises, Q1 2024

	Entity	Victim Notices
1	LoanDepot, Inc.	16,924,071
2	Infosys McCamish Systems LLC	6,078,263
3	Medical Management Resource Group, LLC	2,350,236
4	Eastern Radiologists, Inc.	886,746
5	Cencora, Inc.	852,725
6	City of Hope	827,149
7	UNITE HERE	791,273
8	Plaza Radiology dba Chattanooga Imaging	569,022
9	Association of Texas Professional Educators	426,280
10	Houser LLP	370,001

Compromise Year-Over-Year Totals, 2019 – Q1 2024

	Compromises	Victim Notices
Q1 2024	835	38,360,202
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Compromise Quarter-by-Quarter Totals, Q1 2022 – Q1 2024

	Compromises	Victim Notices
Q1 2024	835	38,360,202
Q4 2023	1,087	154,832,918
Q3 2023	733	81,752,518
Q2 2023	940	82,065,475
Q1 2023	442	100,686,535
Q4 2022	511	253,285,922
Q3 2022	471	109,967,747
Q2 2022	412	35,197,623
Q1 2022	404	26,768,211

Compromises by Sector, Q1, 2022 – 2024

	Q1 2024	Q1 2023	Q1 2022
Education	36 Compromises 511,672 Victim Notices	31 Compromises 569,618 Victim Notices	21 Compromises 106,099 Victim Notices
Financial Services	222 Compromises 18,582,863 Victim Notices	70 Compromises 10,555,103 Victim Notices	68 Compromises 5,732,597 Victim Notices
Government	43 Compromises 147,902 Victim Notices	23 Compromises 759,622 Victim Notices	13 Compromises 790,763 Victim Notices
Healthcare	124 Compromises 7,379,647 Victim Notices	81 Compromises 14,199,413 Victim Notices	73 Compromises 4,377,462 Victim Notices
Hospitality	16 Compromises 687,334 Victim Notices	7 Compromises 196,891 Victim Notices	6 Compromises 57,392 Victim Notices
HR/Staffing	4 Compromises 130,853 Victim Notices	3 Compromises 20,616 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	77 Compromises 996,147 Victim Notices	49 Compromises 1,190,146 Victim Notices	52 Compromises 249,706 Victim Notices
Mining/Construction	19 Compromises 12,174 Victim Notices	15 Compromises 59,292 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	37 Compromises 1,286,092 Victim Notices	19 Compromises 85,420 Victim Notices	20 Compromises 629,822 Victim Notices
Professional Services	99 Compromises 1,169,450 Victim Notices	48 Compromises 75,502 Victim Notices	45 Compromises 3,022,491 Victim Notices
Retail	22 Compromises 185,193 Victim Notices	16 Compromises 179,622 Victim Notices	18 Compromises 272,950 Victim Notices
Social Services	2 Compromises 15,116 Victim Notices	3 Compromises 154,160 Victim Notices	0 Compromises 0 Victim Notices
Technology	41 Compromises 6,829,438 Victim Notices	35 Compromises 24,399,696 Victim Notices	16 Compromises 10,832,588 Victim Notices
Transportation	37 Compromises 141,917 Victim Notices	13 Compromises 11,096,783 Victim Notices	8 Compromises 20,930 Victim Notices
Utilities	17 Compromises 204,354 Victim Notices	6 Compromises 37,054,637 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	11 Compromise 10,703 Victim Notices	11 Compromises 62,316 Victim Notices	0 Compromises 0 Victim Notices
Other	26 Compromises 69,345 Victim Notices	12 Compromises 27,698 Victim Notices	64 Compromises 675,411 Victim Notices
Unknown	2 Compromises 2 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**835 Compromises 38,360,202 Victim Notices**	**442 Compromises 100,686,535 Victim Notices**	**404 Compromises 26,768,211 Victim Notices**

Attack Vector, Q1, 2022 – 2024

	Q1 2024	Q1 2023	Q1 2022
Cyberattacks	**644**	**375**	**366**
Phishing/Smishing/BED	108	111	112
Ransomware	60	60	71
Malware	12	20	24
Non-Secured Cloud Environment	1	5	3
Credential Stuffing	10	8	2
Unpatched Software Flaw	2	–	–
Zero Attack Day	5	2	–
Other	8	5	7
Not Specified	438	164	147
System & Human Error	**84**	**59**	**33**
Failure to Configure Cloud Security	4	7	4
Correspondence (Email/Letter)	29	23	12
Misconfigured Firewall	4	5	5
Lost Device or Document	4	–	1
Other	36	21	5
Not Specified	7	3	6
Physical Attacks	**11**	**6**	**3**
Document Theft	2	–	1
Device Theft	6	6	1
Improper Disposal	1	–	1
Skimming Device	1	–	–
Other	1	–	–
Not Specified	–	–	–
Data Leak	**–**	**–**	**–**
Unknown	**96**	**2**	**2**

2024 BREAKDOWN

Q2 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

729 Compromises
857,526,105 Victim Notices

Data Breaches

652 Breaches
857,322,978 Victim Notices

Data Exposures

4 Exposures
118,000 Victim Notices

Data Leaks

0 Leaks
0 Victim Notices

Unknown

73 Unknown
85,127 Victim Notices

ATTACK VECTORS

CYBERATTACKS

579 Breaches
842,035,841 Victim Notices

+ 104 Phishing/Smishing/BEC
+ 12 Malware
+ 53 Ransomware
+ 5 Credential Stuffing
+ 5 Zero-Day Attack
+ 1 Non-Secured Cloud Environment
+ 6 Other
+ 393 Not Specified

SYSTEM & HUMAN ERROR

70 Breaches/Exposures
15,399,693 Victim Notices

+ 26 Correspondence (Email/Letter)
+ 3 Lost Device or Document
+ 4 Failure to Configure Cloud Security
+ 5 Misconfigured Firewalls
+ 25 Other
+ 7 Not Specified

PHYSICAL ATTACKS

7 Breaches/Exposures
5,444 Victim Notices

+ 2 Device theft
+ 3 Improper Disposal
+ 1 Document Theft
+ 1 Other

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

211 Entities Affected
192,663,708 Victim Notices

System & Human Errors

10 Entities Affected
1,288,785 Victim Notices

Physical Attack

0 Entities Affected
0 Victim Notices

CHARTS

Top 10 Compromises, Q2 2024

	Entity	Victim Notices
1	Ticketmaster Entertainment, LLC	560,000,000
2	Change Healthcare	190,000,000
3	Dell Technologies Inc.	49,000,000
4	Kaiser Foundation Health Plan, Inc.	13,400,000
5	U.S. Environmental Protection Agency	8,460,182
6	Financial Business and Consumer Solutions, Inc.	4,253,394
7	Omni Hotels and Resorts	3,500,000
8	A&A Services dba Sav-Rx	2,812,336
9	The Prudential Insurance Company of America	2,556,210
10	WebTPA Employer Services, LLC	2,429,175

Compromise Year-Over-Year Totals, 2019 – Q2 2024

	Compromises	Victim Notices
Q2 2024 YTD	1,565	895,886,319
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Compromise Quarter-by-Quarter Totals, Q1 2022 – Q2 2024

	Compromises	Victim Notices
Q2 2024	729	857,526,105
Q1 2024	835	38,360,202
Q4 2023	1,087	154,832,918
Q3 2023	733	81,752,518
Q2 2023	940	82,065,475
Q1 2023	442	100,686,535
Q4 2022	511	253,285,922
Q3 2022	471	109,967,747
Q2 2022	412	35,197,623
Q1 2022	404	26,768,211

Compromises by Sector, Q2, 2022 – 2024

	Q2 2024	Q2 2023	Q2 2022
Education	40 Compromises 211,705 Victim Notices	49 Compromises 1,087,195 Victim Notices	20 Compromises 299,394 Victim Notices
Financial Services	180 Compromises 10,867,189 Victim Notices	173 Compromises 30,938,950 Victim Notices	60 Compromises 16,754,396 Victim Notices
Government	30 Compromises 9,298,847 Victim Notices	27 Compromises 10,319,523 Victim Notices	20 Compromises 19,766 Victim Notices
Healthcare	112 Compromises 19,972,941 Victim Notices	296 Compromises 10,932,417 Victim Notices	86 Compromises 8,696,626 Victim Notices
Hospitality	17 Compromises 563,559,291 Victim Notices	16 Compromises 231,469 Victim Notices	5 Compromises 20,369 Victim Notices
HR/Staffing	9 Compromises 162,524 Victim Notices	2 Compromises 4,528 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	74 Compromises 49,456,447 Victim Notices	63 Compromises 190,491 Victim Notices	63 Compromises 240,829 Victim Notices
Mining/Construction	30 Compromises 42,920 Victim Notices	16 Compromises 49,397 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	33 Compromises 329,111 Victim Notices	28 Compromises 2,040,994 Victim Notices	16 Compromises 42,306 Victim Notices
Professional Services	78 Compromises 285,936 Victim Notices	89 Compromises 12,881,863 Victim Notices	49 Compromises 323,557 Victim Notices
Retail	24 Compromises 6,420,002 Victim Notices	41 Compromises 5,962,966 Victim Notices	12 Compromises 52,580 Victim Notices
Social Services	4 Compromises 66,437 Victim Notices	5 Compromises 34,901 Victim Notices	0 Compromises 0 Victim Notices
Technology	25 Compromises 192,721,375 Victim Notices	52 Compromises 6,566,234 Victim Notices	15 Compromises 4,974,681 Victim Notices
Transportation	17 Compromises 1,538,096 Victim Notices	23 Compromises 61,141 Victim Notices	11 Compromises 824,893 Victim Notices
Utilities	17 Compromises 1,362,192 Victim Notices	16 Compromises 322,812 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	17 Compromise 93,060 Victim Notices	18 Compromises 167,842 Victim Notices	0 Compromises 0 Victim Notices
Other	19 Compromises 1,138,000 Victim Notices	26 Compromises 272,752 Victim Notices	55 Compromises 2,948,226 Victim Notices
Unknown	3 Compromises 32 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**729 Compromises 857,526,105 Victim Notices**	**940 Compromises 82,065,475 Victim Notices**	**412 Compromises 35,197,623 Victim Notices**

Attack Vector, Q2, 2022 – 2024

	Q2 2024	Q2 2023	Q2 2022
Cyberattacks	**579**	**660**	**363**
Phishing/Smishing/BED	104	134	110
Ransomware	53	67	60
Malware	12	70	23
Non-Secured Cloud Environment	1	3	2
Credential Stuffing	5	14	4
Unpatched Software Flaw	–	–	–
Zero Attack Day	5	14	2
Other	6	9	4
Not Specified	393	349	158
System & Human Error	**70**	**255**	**34**
Failure to Configure Cloud Security	4	5	6
Correspondence (Email/Letter)	26	152	9
Misconfigured Firewall	5	3	10
Lost Device or Document	3	24	–
Other	25	65	7
Not Specified	7	6	2
Physical Attacks	**7**	**25**	**13**
Document Theft	1	2	2
Device Theft	2	7	8
Improper Disposal	3	4	2
Skimming Device	–	7	1
Other	1	5	–
Not Specified	–	–	–
Data Leak	**–**	**–**	**–**
Unknown	**73**	**–**	**2**

2024 BREAKDOWN

H1 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

1,565 Compromises
895,886,319 Victim Notices

Data Breaches

1,388 Breaches
895,563,528 Victim Notices

Data Exposures

8 Exposures
138,600 Victim Notices

Data Leaks

0 Leaks
0 Victim Notices

Unknown

169 Unknown
184,191 Victim Notices

ATTACK VECTORS

CYBERATTACKS

1,224 Breaches
879,847,900 Victim Notices

+ 212 Phishing/Smishing/BEC
+ 113 Ransomware
+ 24 Malware
+ 15 Credential Stuffing
+ 10 Zero-Day Attack
+ 2 Non-Secured Cloud Environment
+ 14 Other
+ 832 Not Specified

SYSTEM & HUMAN ERROR

154 Breaches/Exposures
15,796,413 Victim Notices

+ 55 Correspondence (Email/Letter)
+ 7 Lost Device or Document
+ 8 Failure to Configure Cloud Security
+ 9 Misconfigured Firewalls
+ 61 Other
+ 14 Not Specified

PHYSICAL ATTACKS

18 Breaches/Exposures
57,815 Victim Notices

+ 8 Device Theft
+ 1 Skimming Device
+ 4 Improper Disposal
+ 3 Document Theft
+ 2 Other

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

452 Entities Affected
200,122,432 Victim Notices

System & Human Errors

14 Entities Affected
1,340,846 Victim Notices

Physical Attack

0 Entities Affected
Unknown Victim Notices

CHARTS

Top 10 Compromises, *H1 2024*

	Entity	*Victim Notices*
1	Ticketmaster Entertainment, LLC	560,000,000
2	Change Healthcare	190,000,000
3	Dell Technologies Inc.	49,000,000
4	LoanDepot, Inc.	16,924,071
5	Kaiser Foundation Health Plan, Inc.	13,400,000
6	U.S. Environmental Protection Agency	8,460,182
7	Infosys McCamish Systems LLC	6,078,263
8	Financial Business and Consumer Solutions, Inc.	4,253,394
9	Omni Hotels and Resorts	3,500,000
10	A&A Services dba Sav-Rx	2,812,336

Compromise Year-Over-Year Totals, *2019 – H1 2024*

	Compromises	*Victim Notices*
H1 2024 YTD	1,565	895,886,319
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Compromise Quarter-by-Quarter Totals, *Q1 2022 – Q2 2024*

	Compromises	*Victim Notices*
Q2 2024	729	857,526,105
Q1 2024	835	38,360,202
Q4 2023	1,087	154,832,918
Q3 2023	733	81,752,518
Q2 2023	940	82,065,475
Q1 2023	442	100,686,535
Q4 2022	511	253,285,922
Q3 2022	471	109,967,747
Q2 2022	412	35,197,623
Q1 2022	404	26,768,211

Compromises by Sector, *H1, 2022 – 2024*

	H1 2024	*H1 2023*	*H1 2022*
Education	76 Compromises 723,377 Victim Notices	80 Compromises 1,656,813 Victim Notices	41 Compromises 405,493 Victim Notices
Financial Services	403 Compromises 29,450,064 Victim Notices	243 Compromises 41,494,053 Victim Notices	128 Compromises 22,486,993 Victim Notices
Government	73 Compromises 9,446,749 Victim Notices	50 Compromises 11,079,145 Victim Notices	33 Compromises 810,529 Victim Notices
Healthcare	236 Compromises 27,352,588 Victim Notices	377 Compromises 25,131,830 Victim Notices	159 Compromises 13,074,088 Victim Notices
Hospitality	33 Compromises 564,246,625 Victim Notices	23 Compromises 428,360 Victim Notices	11 Compromises 77,761 Victim Notices
HR/Staffing	13 Compromises 293,377 Victim Notices	5 Compromises 25,144 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	151 Compromises 50,452,594 Victim Notices	112 Compromises 1,380,637 Victim Notices	115 Compromises 490,535 Victim Notices
Mining/Construction	49 Compromises 55,094 Victim Notices	31 Compromises 108,689 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	70 Compromises 1,615,203 Victim Notices	47 Compromises 2,126,414 Victim Notices	36 Compromises 672,128 Victim Notices
Professional Services	177 Compromises 1,455,386 Victim Notices	137 Compromises 12,957,365 Victim Notices	94 Compromises 3,346,048 Victim Notices
Retail	46 Compromises 6,605,195 Victim Notices	57 Compromises 6,142,588 Victim Notices	30 Compromises 325,530 Victim Notices
Social Services	6 Compromises 81,553 Victim Notices	8 Compromises 189,061 Victim Notices	0 Compromises 0 Victim Notices
Technology	66 Compromises 199,550,813 Victim Notices	87 Compromises 30,965,930 Victim Notices	31 Compromises 15,807,269 Victim Notices
Transportation	54 Compromises 1,680,013 Victim Notices	36 Compromises 11,157,924 Victim Notices	19 Compromises 845,823 Victim Notices
Utilities	34 Compromises 1,566,546 Victim Notices	22 Compromises 37,377,449 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	28 Compromise 103,763 Victim Notices	29 Compromises 230,158 Victim Notices	0 Compromises 0 Victim Notices
Other	45 Compromises 1,207,345 Victim Notices	38 Compromises 300,450 Victim Notices	119 Compromises 3,623,637 Victim Notices
Unknown	5 Compromises 34 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**1,565 Compromises 895,886,319 Victim Notices**	**1,382 Compromises 182,752,010 Victim Notices**	**816 Compromises 61,965,834 Victim Notices**

Attack Vector, *H1, 2022 – 2024*

	H1 2024	*H1 2023*	*H1 2022*
Cyberattacks	**1,224**	**1,035**	**729**
Phishing/Smishing/BED	212	245	222
Ransomware	113	127	131
Malware	24	90	47
Non-Secured Cloud Environment	2	8	5
Credential Stuffing	15	22	6
Unpatched Software Flaw	2	–	–
Zero Attack Day	10	16	2
Other	14	14	11
Not Specified	832	513	305
System & Human Error	**154**	**314**	**67**
Failure to Configure Cloud Security	8	12	10
Correspondence (Email/Letter)	55	175	21
Misconfigured Firewall	9	8	15
Lost Device or Document	7	24	1
Other	61	86	12
Not Specified	14	9	8
Physical Attacks	**18**	**31**	**16**
Document Theft	3	2	3
Device Theft	8	13	9
Improper Disposal	4	4	3
Skimming Device	1	7	1
Other	2	5	–
Not Specified	–	–	–
Data Leak	**–**	**–**	**–**
Unknown	**169**	**2**	**4**

2024 BREAKDOWN

Q3 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

670 Compromises
248,539,238 Victim Notices

Data Breaches

616 Breaches
147,674,113 Victim Notices

Data Exposures

6 Exposures
100,014,000 Victim Notices

Data Leaks

1 Leak
Unknown Number of Victim Notices

Unknown

47 Unknown
851,125 Victim Notices

ATTACK VECTORS

CYBERATTACKS

550 Breaches
147,480,020 Victim Notices

+ 105 Phishing/Smishing/BEC
+ 42 Ransomware
+ 10 Malware
+ 6 Credential Stuffing
+ 4 Zero-Day Attack
+ 7 Other
+ 376 Not Specified

SYSTEM & HUMAN ERROR

67 Breaches/Exposures
100,194,221 Victim Notices

+ 28 Correspondence (Email/Letter)
+ 6 Failure to Configure Cloud Security
+ 3 Misconfigured Firewalls
+ 2 Lost Device or Document
+ 27 Other
+ 1 Not Specified

PHYSICAL ATTACKS

5 Breaches/Exposures
13,872 Victim Notices

+ 4 Device Theft
+ 1 Skimming Device

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

91 Entities Affected
1,041,789 Victim Notices

System & Human Errors

5 Entities Affected
96 Victim Notices

Physical Attack

1 Entity Affected
0 Victim Notices

CHARTS

Top 10 Compromises, Q3 2024

	Entity	Victim Notices
1	AT&T	110,000,000
2	MC2 Data	100,000,000
3	Evolve Bank & Trust	7,640,112
4	Ascension Health	5,599,699
5	HealthEquity Inc.	4,300,000
6	Acadian Ambulance Service, Inc.	2,896,985
7	Rite Aid Corporation	2,200,000
8	Slim CD, Inc.	1,693,000
9	National Public Data	1,300,000
10	Patelco Credit Union	1,009,472

Compromise Year-Over-Year Totals, 2019 – Q3 2024

	Compromises	Victim Notices
Q3 2024 YTD	2,237	1,144,425,559
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Compromise Quarter-by-Quarter Totals, Q1 2022 – Q3 2024

	Compromises	Victim Notices
Q3 2024	670	248,539,238
Q2 2024	729	857,526,105
Q1 2024	835	38,360,202
Q4 2023	1,087	154,832,918
Q3 2023	733	81,752,518
Q2 2023	940	82,065,475
Q1 2023	442	100,686,535
Q4 2022	511	253,285,922
Q3 2022	471	109,967,747
Q2 2022	412	35,197,623
Q1 2022	404	26,768,211

Compromises by Sector, Q3, 2022 – 2024

	Q3 2024	Q3 2023	Q3 2022
Education	33 Compromises 447,576 Victim Notices	42 Compromises 2,708,234 Victim Notices	23 Compromises 1,097,584 Victim Notices
Financial Services	140 Compromises 16,555,633 Victim Notices	205 Compromises 17,891,371 Victim Notices	66 Compromises 3,153,208 Victim Notices
Government	19 Compromises 1,593,214 Victim Notices	26 Compromises 2,869,285 Victim Notices	19 Compromises 220,738 Victim Notices
Healthcare	122 Compromises 9,815,379 Victim Notices	113 Compromises 17,758,006 Victim Notices	93 Compromises 5,060,271 Victim Notices
Hospitality	17 Compromises 348,171 Victim Notices	10 Compromises 3,525,136 Victim Notices	10 Compromises 69,027,431 Victim Notices
HR/Staffing	9 Compromises 37,933 Victim Notices	2 Compromises 134,469 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	66 Compromises 148,109 Victim Notices	64 Compromises 3,589,747 Victim Notices	64 Compromises 23,095,176 Victim Notices
Mining/Construction	17 Compromises 108,249 Victim Notices	20 Compromises 38,049 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	32 Compromises 94,528 Victim Notices	22 Compromises 7,178,856 Victim Notices	16 Compromises 65,161 Victim Notices
Professional Services	91 Compromises 374,978 Victim Notices	81 Compromises 16,961,393 Victim Notices	69 Compromises 1,705,652 Victim Notices
Retail	30 Compromises 2,385,437 Victim Notices	30 Compromises 1,289,333 Victim Notices	20 Compromises 363,880 Victim Notices
Social Services	7 Compromises 74,035 Victim Notices	3 Compromises 17,349 Victim Notices	0 Compromises 0 Victim Notices
Technology	31 Compromises 3,243,439 Victim Notices	40 Compromises 5,958,195 Victim Notices	21 Compromises 2,969,682 Victim Notices
Transportation	11 Compromises 2,933,933 Victim Notices	25 Compromises 175,859 Victim Notices	6 Compromises 2,517,830 Victim Notices
Utilities	18 Compromises 110,034,597 Victim Notices	10 Compromises 16,502 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	5 Compromise 2,335 Victim Notices	13 Compromises 23,694 Victim Notices	0 Compromises 0 Victim Notices
Other	18 Compromises 100,339,045 Victim Notices	27 Compromises 1,617,040 Victim Notices	64 Compromises 691,134 Victim Notices
Unknown	4 Compromises 2,647 Victim Notices	0 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**670 Compromises 248,539,238 Victim Notices**	**733 Compromises 81,752,518 Victim Notices**	**471 Compromises 109,967,747 Victim Notices**

Attack Vector, Q3, 2022 – 2024

	Q3 2024	Q3 2023	Q3 2022
Cyberattacks	**550**	**612**	**414**
Phishing/Smishing/BED	105	83	131
Ransomware	42	63	78
Malware	10	18	15
Non-Secured Cloud Environment	–	5	1
Credential Stuffing	6	5	8
Unpatched Software Flaw	–	–	–
Zero Attack Day	4	69	2
Other	7	7	2
Not Specified	376	362	177
System & Human Error	**67**	**96**	**42**
Failure to Configure Cloud Security	6	6	3
Correspondence (Email/Letter)	28	42	15
Misconfigured Firewall	3	7	7
Lost Device or Document	2	9	3
Other	27	27	10
Not Specified	1	5	4
Physical Attacks	**5**	**14**	**12**
Document Theft	–	1	2
Device Theft	4	7	4
Improper Disposal	–	1	1
Skimming Device	1	2	2
Other	–	–	2
Not Specified	–	3	1
Data Leak	**1**	**2**	–
Unknown	**47**	**9**	**3**

2024 BREAKDOWN

Q4 Data Compromise Details

NUMBER OF COMPROMISES

TOTAL DATA COMPROMISES

917 Compromises
206,384,116 Victim Notices

Data Breaches

840 Breaches
203,309,440 Victim Notices

Data Exposures

4 Exposures
1,161 Victim Notices

Data Leaks

1 Leaks
2,795,947 Victim Notices

Unknown

72 Unknown
277,568 Victim Notices

ATTACK VECTORS

CYBERATTACKS

746 Breaches
202,511,801 Victim Notices

+ 138 Phishing/Smishing/BEC
+ 33 Ransomware
+ 14 Malware
+ 7 Credential Stuffing
+ 3 Zero-Day Attack
+ 1 Non-Secured Cloud Environment
+ 6 Other
+ 544 Not Specified

SYSTEM & HUMAN ERROR

88 Breaches/Exposures
681,133 Victim Notices

+ 31 Correspondence (Email/Letter)
+ 5 Lost Devices or Documents
+ 4 Failure to Configure Cloud Security
+ 1 Misconfigured Firewalls
+ 41 Other
+ 5 Not Specified

PHYSICAL ATTACKS

10 Breaches/Exposures
117,667 Victim Notices

+ 6 Document Theft
+ 2 Device Theft
+ 2 Skimming Device

SUPPLY CHAIN ATTACKS

(Included in Attack Vectors Above)

Cyberattack

94 Entities Affected
638,929 Victim Notices

System & Human Errors

0 Entities Affected
0 Victim Notices

Physical Attack

0 Entity Affected
0 Victim Notices

CHARTS

Top 10 Compromises, Q4 2024

	Entity	Victim Notices
1	DemandScience by Pure Incubation	121,796,165
2	Hot Topic, Inc.	56,904,909
3	Blooms Today	3,184,010
4	HuntStand	2,795,947
5	Summit Pathology and Summit Pathology Laboratories, Inc.	1,813,538
6	OnePoint Patient Care	1,741,152
7	Texas Tech University Health Sciences Center El Paso and Texas Tech University Health Sciences Center	1,465,000
8	Lubbock County Hospital District	1,260,929
9	Set Forth, Inc.	1,224,506
10	ConnectOnCall.com, LLC	914,138

Compromise Year-Over-Year Totals, 2019 – 2024

	Compromises	Victim Notices
2024	3,158	1,350,835,988
2023	3,202	419,337,446
2022	1,798	425,219,503
2021	1,859	351,833,545
2020	1,107	302,869,661
2019	1,278	883,569,154

Compromise Quarter-by-Quarter Totals, Q1 2022 – Q4 2024

	Compromises	Victim Notices
Q4 2024	917	206,384,116
Q3 2024	670	248,539,238
Q2 2024	729	857,526,105
Q1 2024	835	38,360,202
Q4 2023	1,087	154,832,918
Q3 2023	733	81,752,518
Q2 2023	940	82,065,475
Q1 2023	442	100,686,535
Q4 2022	511	253,285,922
Q3 2022	471	109,967,747
Q2 2022	412	35,197,623
Q1 2022	404	26,768,211

Compromises by Sector, Q4, 2022 – 2024

	Q4 2024	Q4 2023	Q4 2022
Education	53 Compromises 2,285,085 Victim Notices	51 Compromises 1,204,898 Victim Notices	35 Compromises 789,112 Victim Notices
Financial Services	190 Compromises 2,388,530 Victim Notices	294 Compromises 21,177,439 Victim Notices	76 Compromises 1,781,716 Victim Notices
Government	35 Compromises 1,151,406 Victim Notices	23 Compromises 1,474,528 Victim Notices	22 Compromises 720,412 Victim Notices
Healthcare	177 Compromises 9,502,466 Victim Notices	321 Compromises 17,174,866 Victim Notices	89 Compromises 9,593,847 Victim Notices
Hospitality	19 Compromises 115,812 Victim Notices	12 Compromises 1,584,157 Victim Notices	13 Compromises 412,933 Victim Notices
HR/Staffing	1 Compromises 13,818 Victim Notices	4 Compromises 79,753 Victim Notices	0 Compromises 0 Victim Notices
Manufacturing	100 Compromises 435,688 Victim Notices	82 Compromises 36,244,130 Victim Notices	68 Compromises 410,121 Victim Notices
Mining/Construction	38 Compromises 62,963 Victim Notices	20 Compromises 75,566 Victim Notices	0 Compromises 0 Victim Notices
Non-Profit/NGO	44 Compromises 110,509 Victim Notices	33 Compromises 216,160 Victim Notices	20 Compromises 271,389 Victim Notices
Professional Services	77 Compromises 915,813 Victim Notices	92 Compromises 487,639 Victim Notices	60 Compromises 1,353,998 Victim Notices
Retail	20 Compromises 62,239,135 Victim Notices	31 Compromises 2,741,550 Victim Notices	15 Compromises 108,555 Victim Notices
Social Services	5 Compromises 203,776 Victim Notices	5 Compromises 5,377 Victim Notices	0 Compromises 0 Victim Notices
Technology	45 Compromises 123,016,634 Victim Notices	40 Compromises 33,160,566 Victim Notices	35 Compromises 229,869,351 Victim Notices
Transportation	23 Compromises 60,709 Victim Notices	40 Compromises 1,068,518 Victim Notices	11 Compromises 630,817 Victim Notices
Utilities	14 Compromises 30,709 Victim Notices	12 Compromises 36,028,265 Victim Notices	0 Compromises 0 Victim Notices
Wholesale Trade	21 Compromise 41,774 Victim Notices	11 Compromises 180,434 Victim Notices	0 Compromises 0 Victim Notices
Other	49 Compromises 3,808,955 Victim Notices	15 Compromises 2,109,072 Victim Notices	67 Compromises 7,343,671 Victim Notices
Unknown	6 Compromises 334 Victim Notices	1 Compromises 0 Victim Notices	0 Compromises 0 Victim Notices
Totals	**917 Compromises 206,384,116 Victim Notices**	**1,087 Compromises 154,832,918 Victim Notices**	**511 Compromises 253,285,922 Victim Notices**

Attack Vector, Q4, 2022 – 2024

	Q4 2024	Q4 2023	Q4 2022
Cyberattacks	**746**	**717**	**438**
Phishing/Smishing/BED	138	114	115
Ransomware	33	69	84
Malware	14	11	11
Non-Secured Cloud Environment	1	1	4
Credential Stuffing	7	3	4
Unpatched Software Flaw	–	1	–
Zero Attack Day	3	24	4
Other	6	8	4
Not Specified	544	486	212
System & Human Error	**88**	**320**	**54**
Failure to Configure Cloud Security	4	6	5
Correspondence (Email/Letter)	31	165	19
Misconfigured Firewall	1	4	8
Lost Device or Document	5	20	3
Other	41	108	14
Not Specified	6	17	5
Physical Attacks	**10**	**8**	**18**
Document Theft	6	3	2
Device Theft	2	3	8
Improper Disposal	–	–	1
Skimming Device	2	–	3
Other	–	–	4
Not Specified	–	2	–
Data Leak	**1**	–	–
Unknown	**72**	**42**	**1**

NOTES

METHODOLOGY

For purposes of 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 comprehensive data breach database.

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

DISCLAIMERS

2021 Victim Notices Count (Full Year), Chart Note: The AT&T victim count has been added to the 2021 victim count as the compromise initially occurred and was entered in 2021. The 51M is not reflected in the Q1 2024 victim count.

2021 Victim Notices Count, Q1 DBA Note: A Special Comment Regarding AT&T; In August 2021, cybercriminals offered to sell a file of information from more than 70 million wireless AT&T accounts. AT&T denied the company was the source of the data and instead claimed the information appeared to be related to a data breach from a reseller in 2019. In mid-March 2024, cybercriminals again posted a file purported to be AT&T customer data similar in size and content to the previous data file. AT&T again denied it was the source of the compromised information that included sensitive personal information like Social Security numbers and AT&T-specific data such as PINs. On Saturday, March 30, AT&T reversed its previous position and notified 7.6M current customers of the data breach but noted the company did not know if the AT&T-specific information originated from their systems or from a vendor. AT&T promised to investigate. The information of an additional 65M former customers was also included in the breached file. Pending the outcome of AT&T's investigation, the ITRC does not classify this event as a new breach or compromise but has updated the original 2021 breach entry to reflect the number of victims (~73M) impacted by the original event. In the event AT&T's investigation results in new findings as to the source, cause, and impact of the data compromise, we will update the data breach database accordingly.

Ticketmaster Victim Notices Count: The Ticketmaster breach victim count is based on unverified information provided by the threat actor claiming responsibility for the attack. Ticketmaster has filed a mandatory breach notice that states more than 1,000 individuals have been impacted, but has not provided information on the number of victims by country. The entry will be updated if, and when, an updated victim count is reported.

Change Healthcare: On January 24, 2025 after the end of the trading day on the NYSE, Change Healthcare's parent company, United Healthcare (NYSE:UNH) updated the number of victim notices issued related to the February 2024 cyberattack. UNH reported 190M victims impacted, but has yet to disclose how many companies in their supply chain have been impacted by the ransomware attack. Due to the classification code used by UNH, victim notices are accounted for under the SIC/NAICS code for computer processing, not healthcare.

Further, according to HIPAA Journal, the ransomware attack on Change Healthcare was detected on February 21, 2024, and it was later confirmed that the BlackCat ransomware group was behind the attack. A $22 million ransom was paid to prevent the release of the stolen data; however, the BlackCat ransomware group performed an exit scam, pocketed the ransom payment, and didn't pay the affiliate who conducted the attack. The affiliate then worked with another ransomware group, RansomHub, which attempted to extort Change Healthcare further, although no additional ransom payments were made and the stolen data remains in the hands of cybercriminals.