

# Targeted Cyberattacks Fuel Massive Increase in Breach Victim Counts

## *Reported compromises in H1 2024 are running ~14 percent higher than the previous year*

Publicly reported data compromises in the first six months of 2024 show several data compromise trends from 2023 continued in the new year as well as revealed a sudden, dramatic increase in the overall estimated number of victims of data breaches. As in previous years, though, a small number of data compromises with large victim counts tend to skew the number of individuals impacted and mask the fact that an increase in the number of cyberattacks is generally impacting fewer victims.

### Highlights

The number of data compromises reported in the first half (H1) of 2024 totaled 1,571 impacting an estimated 1.07 billion victims, including individuals impacted by multiple breaches. This was a ~14 percent increase in compromises compared to the same period in 2023, a year which set the record for data events reported in a single year (3,203).

Estimated victim counts also grew in H1 well above the previous year, in part, because of updates to original estimates from compromises reported earlier in 2024 as well as a small number of very large cyberattack-related data breaches. For example:

- + Prudential Financial originally notified the U.S. Securities and Exchange Commission of a breach in February 2024 that impacted an estimated 36,000 victims. Prudential later revised the victim count in June 2024 to 2.5M.
- + Infosys McCamish System revised their estimated victim count from ~84,000 in February's notice to 6M.
- + Chicago's Lurie Children's Hospital updated a March breach notice to include an initial estimated victim count of 800,000.
- + Credential stuffing attacks that targeted customers of the Snowflake cloud service accounted for more than 900M of the victims reported in H1 2024.
- + However, the 1+ billion estimated total victim count does not include victims of the Change Healthcare supply chain attack which company executives predict will impact "a substantial number" of U.S. residents. According to [company estimates](#), Change processes one-third of all U.S. patient health records.

Supply chain attacks dropped slightly in H1 2024 compared to the same period in 2023, but the number of entities compromised increased.

Attacks against Financial Services companies jumped by more than two-thirds (67 percent) year-over-year to be the most compromised industry in H1 2024, followed by Healthcare companies. Reported compromises increased in 10 of the 16 industries tracked by the ITRC, but compromises reported by Healthcare entities decreased year-over-year by 37 percent. The decrease was enough to knock Healthcare from the most targeted industry to the second most frequently compromised for the first time in six years.

"Not Specified," at 68 percent, remained the most reported cause of a cyberattack listed in breach notices issued in H1 2024. This trend puts individuals and other businesses at risk from similar attacks.

### **A Special Note About Driver's License Data**

H1 trends reflect the increased value and use of stolen Driver's License information. Driver's License data was stolen in one-quarter (25 percent) of data breaches, based on notices issued in H1 2024. This corresponds to a 23 percent increase in cases of identity misuse reported to the ITRC by victims in 2023. (See the ITRC [\*2023 Trends in Identity Report\*](#), June 2024)

This increased rate of Driver's License data theft reflects a post-pandemic trend related to the increased use of Driver's Licenses for identity verification in a wider variety of transactions. The number of data breaches where driver's license data was stolen totaled 198 instances in pre-pandemic, full-year 2019 compared to 636 in full-year 2023 and 308 through June 30, 2024.

Financial Services, Healthcare, Professional Services, Manufacturing, and Government were, respectively, the top sources of compromised Driver's License data in H1 2024.

# Q2 Data Compromise Highlights

## Number of Q2 Compromises



### 653 DATA BREACHES

1,041,107,999 VICTIMS

### 4 DATA EXPOSURES

118,000 VICTIMS

### 0 DATA LEAKS

0 VICTIMS

### 75 UNKNOWN COMPROMISES

86,602 VICTIMS

## Q2 Attack Vectors



### CYBERATTACKS

580 Breaches

1,027,185,778 Victims



### SYSTEM AND HUMAN ERRORS

70 Breaches/Exposures

14,034,777 Victims



### PHYSICAL ATTACKS

7 Breaches/Exposures

5,444 Victims



### SUPPLY CHAIN ATTACKS

36 Breaches/Exposures

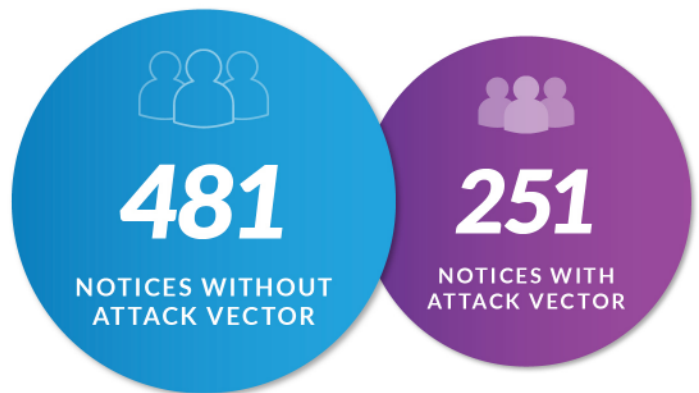
221 Entities Affected

2,629,606 Victims

## Top Compromises by Industry in Q2



## Q2 Public Data Breach Notices



## Top 5 Compromises by Victim Count in Q2



# H1 Data Compromise Highlights

## Number of H1 Compromises



**1,391 DATA BREACHES**  
1,078,664,240 VICTIMS

**8 DATA EXPOSURES**  
138,600 VICTIMS

**0 DATA LEAKS**  
0 VICTIMS

**172 UNKNOWN COMPROMISES**  
186,914 VICTIMS

## H1 Attack Vectors



**CYBERATTACKS**  
1,226 Breaches  
1,064,527,002 Victims



**SYSTEM AND HUMAN ERRORS**  
155 Breaches/Exposures  
14,218,023 Victims



**PHYSICAL ATTACKS**  
18 Breaches/Exposures  
57,815 Victims

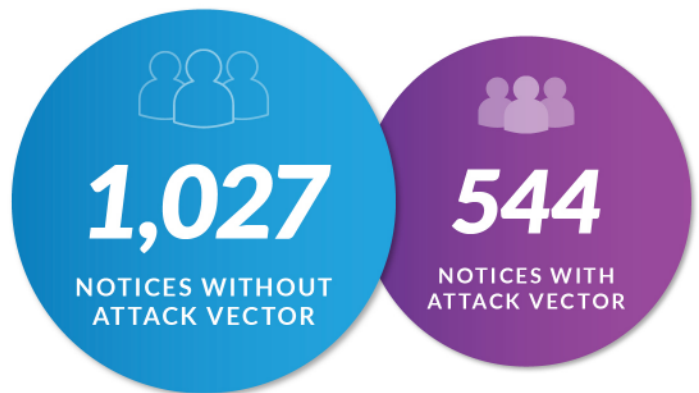


**SUPPLY CHAIN ATTACKS**  
80 Breaches/Exposures  
466 Entities Affected  
10,138,237 Victims

## Top Compromises by Industry in H1



## H1 Public Data Breach Notices



## Top 5 Compromises by Victim Count in H1



## H1 2024 Data Compromise Charts

### Top 10 Compromises of H1 2024

	Entity	Victims Impacted
1	Ticketmaster Entertainment, LLC (Live Nation Entertainment)	560,000,000*
2	Advance Auto Parts, Inc.	380,000,000
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	Omni Hotels and Resorts	3,500,000
9	Financial Business and Consumer Solutions, Inc.	3,435,640
10	A&A Services dba Sav-Rx	2,812,336

\*As of July 17, 2024 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.

### Compromise Year-over-Year Totals

Year	Compromises	Victims
H1 2024	1,571	1,078,989,754*
2023	3,203	418,738,585
2022	1,801	425,283,816
2021	1,860	351,833,545**
2020	1,107	302,869,661
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935

\*As of July 17, 2024 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.

\*\*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.

## Quarter-to-Quarter

Year	Compromises	Victims
Q2 2024	732	1,041,312,601
Q1 2024	838	37,677,141
Q4 2023	1,087	154,379,824
Q3 2023	734	81,713,625
Q2 2023	940	81,958,874
Q1 2023	442	100,686,535
Q4 2022	513	253,296,417
Q3 2022	471	109,967,747
Q2 2022	413	35,251,441
Q1 2022	404	26,768,211

## Compromises by Sector H1 2024 vs. H1 2023 & 2022

	Year					
	H1 2024		H1 2023		H1 2022	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	76	722,460	80	1,656,813	41	405,493
Financial Services	407	28,414,934	243	41,494,053	128	22,486,993
Government	74	9,376,758	50	11,079,145	33	810,529
Healthcare	236	26,885,828	377	25,025,229	160	13,127,906
Hospitality	33	564,245,892	23	428,360	11	77,761
HR/Staffing	13	291,402	5	25,144	-	-
Manufacturing	151	50,428,176	112	1,380,637	115	490,535
Mining/Construction	49	55,091	31	108,689	-	-
Non-Profit/NGO	70	1,482,176	47	2,126,414	36	672,128
Professional Services	178	1,265,261	137	12,957,365	94	3,346,048
Retail	46	384,019,001	57	6,142,588	30	325,530
Social Services	6	67,198	8	189,061	-	-
Technology	66	8,096,887	87	30,965,930	31	15,807,269
Transportation	54	1,680,013	36	11,157,924	19	845,823
Utilities	34	1,566,546	22	37,377,449	-	-
Wholesale Trade	28	102,614	29	230,158	-	-
Other	45	289,483	38	300,450	119	3,623,637
Unknown	5	34	-	-	-	-
Totals:	1,571	1,078,989,754	1,382	182,645,409	817	62,019,652

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through June 30, 2024.

## Attack Vector H1 2024 vs. H1 2023 & 2022

	H1 2024	H1 2023	H1 2022
Cyberattacks	1,226	1,035	730
Phishing/Smishing/BEC	212	245	221
Ransomware	108	125	131
Malware	23	90	47
Non-Secured Cloud Environment	2	8	5
Credential Stuffing	16	22	6
Unpatched Software Flaw	2	-	-
Zero Data Attack	10	16	2
Other	14	14	11
NA – Not Specified	839	515	307
System & Human Error	155	314	67
Failure to Configure Cloud Security	8	12	10
Correspondence (Email/Letter)	52	175	21
Misconfigured Firewall	9	8	15
Lost Device or Document	7	24	1
Other	63	86	12
NA – Not Specified	16	9	8
Physical Attacks	18	31	16
Document Theft	3	2	3
Device Theft	8	13	9
Improper Disposal	4	5	3
Skimming Device	1	7	1
Other	2	5	-
NA – Not Specified	-	-	-
Data Leak	-	-	-
Unknown	172	2	4

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

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

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

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through June 30, 2024.