Q3 2023 Data Breach Analysis: Record Smashed! How Many Data Breaches Will Be Reported In 2023?

Summary

+ As predicted at the end of the second Quarter (Q2), the number of U.S. data compromises reported so far in 2023 now exceeds the previous annual record of data events by 14 percent (14%) with three months left in the reporting period. For the nine months ending September 30, 2023, there have been 2,116 data compromises reported, including 733 in the third quarter (Q3). The number of year-to-date (YTD) data compromises surpasses the previous annual record of 1,862 reported events set in 2021.

+ In Q3:

  » Cyberattacks continued to be the most frequently reported root cause of a data breach in Q3, with 614 notices issued. More than half of breached entities (386) entities did not report an attack vector. However, among those that did, phishing attacks were the most frequently reported cause. Zero-Day Attacks (69) exceeded ransomware (64) and malware attacks (17). However, with more entities not reporting an attack vector than those that did, it is difficult to be precise about the rate of specific attack vectors.

  » Supply chain attacks impacted a large number of entities in Q3, even though they were not directly attacked. Over 1,000 (1,321) organizations reported data compromises as the result of an attack against 87 organizations, including many third parties that used the MOVEit file transfer software.

  » So far in 2023, 344 U.S. organizations have been impacted by a single or multiple vendor(s) using a vulnerable MOVEit product. An additional 79 organizations have reported being directly impacted by attacks against MOVEit software or services. Four of the top ten compromises in Q3 were related to a MOVEit attack.

  » Financial Services displaced Healthcare in Q3 as the most attacked industry for the first time since Q2 2022. However, the number of financial institutions reporting data compromises jumped dramatically in Q3, with 204 notices issued, exceeding the total number of Financial Service compromises reported in the past two years (135). Healthcare companies reported 113 data compromises in Q3. No other Industries reported compromise rates in triple digits.

  » The estimated number of victims is still well short of the pace from 2022 – 66.7M in Q3; 233.9M through the first nine months of 2023 compared to ~110M in Q3 2022 and 425M for the full year 2022.

» Cybersecurity researchers point to the rising number of successful Zero-Day attacks – an attack against a software flaw that is previously undisclosed and for which there is no patch – as a reason for the significant rise in data compromises. That conclusion is consistent with this year's Identity Theft Resource Center compiled statistics where 86 Zero-Day Attacks have been reported to date as the cause of a data breach compared to five (5) in all of 2022.

» The rise in compromises can also be attributed to a new wave of ransomware attacks as cybercrime groups return after being sidelined in the first year of the war in Ukraine, along with new ransomware groups entering the criminal environment. That, too, is consistent with the fact the number of data breaches attributed to ransomware (186) has now exceeded the number of malware attacks so far in 2023. However, malware is also up in 2023 with 106 related compromises versus 68 in full-year 2022.

Q3 Data Compromise Highlights

ITRC | IDENTITY THEFT RESOURCE CENTER

Number of Q3 Compromises

733
TOTAL COMPROMISES

66,658,764
TOTAL VICTIMS

716 DATA BREACHES
63,897,124 VICTIMS

6 DATA EXPOSURES
52,458 VICTIMS

2 DATA LEAKS
2,696,728 VICTIMS

9 UNKNOWN COMPROMISES
12,454 VICTIMS

Q3 Attack Vectors

CYBERATTACKS
614 Breaches
63,783,847 Victims

SYSTEM AND HUMAN ERRORS
94 Breaches/Exposures
160,348 Victims

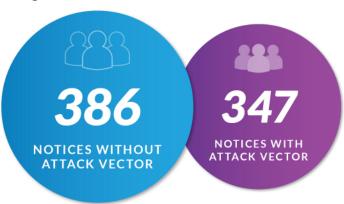**PHYSICAL ATTACKS**
14 Breaches/Exposures
5,387 Victims

SUPPLY CHAIN ATTACKS
87 Breaches/Exposures
1,321 Entities Affected
21,039,939 Victims

Top Compromises by Industry in Q3

FINANCIAL SERVICES	204 Compromises
HEALTHCARE	113 Compromises
PROFESSIONAL SERVICES	81 Compromises
MANUFACTURING	65 Compromises
EDUCATION	42 Compromises

Q3 Public Data Breach Notices

386
NOTICES WITHOUT ATTACK VECTOR

347
NOTICES WITH ATTACK VECTOR

Top 5 Compromises by Victim Count in Q3

HCA HEALTHCARE, INC.
11,270,000 VICTIMS

MAXIMUS, INC. – MOVEIT TRANSFER
11,000,000 VICTIMS

THE FREECYCLE NETWORK
7,000,000 VICTIMS

IBM CONSULTING – MOVEIT TRANSFER
4,091,794 VICTIMS

CARESOURCE – MOVEIT TRANSFER
3,180,537 VICTIMS

Q3 2023 Data Compromise Charts

Top 10 Compromises of Q3 2023

	Entity	Victims Impacted
1	HCA Healthcare, Inc.	11,270,000
2	Maximus, Inc. – MOVEit Transfer	11,000,000
3	The Freecycle Network	7,000,000
4	IBM Consulting – MOVEit Transfer	4,091,794
5	CareSource – MOVEit Transfer	3,180,537
6	Duolingo	2,676,696
7	Tampa General Hospital	2,430,920
8	PH TECH – MOVEit Transfer	1,750,000
9	Flagstar Bank	1,465,002
10	PurFoods, LLC dba Mom's Meals	1,229,333

Compromise Year-over-Year Totals

Year	Compromises	Victims
2023 YTD	2,116	233,935,731
2022	1,802	425,078,513
2021	1,862	298,213,506
2020	1,108	310,218,744
2019	1,279	883,558,186
2018	1,175	2,227,849,622
2017	1,506	1,825,413,935

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between July1, 2023, through September 30, 2023.

Compromises by Sector Q3 2023 vs. Q3 2022 & 2021

	Year					
	Q3 2023		Q3 2022		Q3 2021	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	42	1,905,778	23	1,097,582	25	1,259,723
Financial Services	204	10,455,000	66	3,152,906	69	1,732,946
Government	26	2,869,273	19	219,331	21	1,927,008
Healthcare	113	16,753,924	93	5,059,364	78	11,150,980
Hospitality	10	132,184	10	69,027,431	5	31,069
HR/Staffing	2	134,469	-	-	-	-
Manufacturing	65	2,958,947	64	23,089,103	48	48,306,467
Mining/Construction	20	37,595	-	-	-	-
Non-Profit/NGO	22	7,136,737	16	65,161	21	143,457
Professional Services	81	16,467,396	69	1,705,652	48	1,534,208
Retail	30	1,256,276	20	363,880	21	520,028
Social Services	3	17,349	-	-	-	-
Technology	40	4,883,245	21	2,969,682	12	406,007
Transportation	25	18,471	6	2,517,830	8	329,171
Utilities	10	12,857	-	-	-	-
Wholesale Trade	13	21,063	-	-	-	-
Other	27	1,598,200	64	691,134	88	63,908,379
Unknown	-	-	-	-	1	35,000,000
Totals:	733	66,658,764	471	109,959,056	445	166,249,443

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between July 1, 2023, through September 30, 2023.

Attack Vector Q3 2023 vs. Q3 2022 & 2021

	Q3 2023	Q3 2022	Q3 2021
Cyberattacks	614	414	388
Phishing/Smishing/BEC	80	131	124
Ransomware	64	78	93
Malware	17	15	33
Non-Secured Cloud Environment	5	1	6
Credential Stuffing	4	-	4
Unpatched Software Flaw	-	-	2
Zero Data Attack	69	2	1
Other	7	2	123
NA – Not Specified	368	177	2
System & Human Error	94	42	43
Failure to Configure Cloud Security	6	3	20
Correspondence *(Email/Letter)*	40	15	10
Misconfigured Firewall	7	7	4
Lost Device or Document	9	3	2
Other	26	10	7
NA – Not Specified	6	4	-
Physical Attacks	14	12	6
Document Theft	1	2	2
Device Theft	7	4	1
Improper Disposal	1	1	-
Skimming Device	2	2	-
Other	-	2	3
NA – Not Specified	3	1	-
Data Leak	2	-	1
Unknown	9	3	7

Quarter-to-Quarter

Year	Compromises	Victims
Q3 2023	733	66,658,764
Q2 2023	941	66,778,269
Q1 2023	442	100,498,698
Q4 2022	512	253,099,805
Q3 2022	473	109,959,056
Q2 2022	413	35,251,441
Q1 2022	404	26,768,211
Q4 2021	566	35,388,356
Q3 2021	445	166,249,443
Q2 2021	497	55,321,228
Q1 2021	354	41,254,479

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 July 1, 2023, through September 30, 2023.