ITRC IDENTITY THEFT RESOURCE CENTER

888.400.5530
idtheftcenter.org

Q1 2024 Data Breach Analysis: Two-Thirds of Cyberattack Notices Do Not Include the Cause; Notices Nearly Double YoY

Summary

- Building on the momentum from 2023, the number of publicly reported data compromises in the U.S. nearly doubled in Q1 2024 compared to the same period last year. The First Quarter (Q1) of each year tends to be the lowest in terms of reported data compromises.
- The number of cyberattack-related breach notices without information about the root cause increased significantly in Q1 2024 to more than two-thirds of notices. Fewer than 50 percent of cyberattack notices in Q1 2023 lacked root cause information.
- The number of victims reported by compromised organizations dropped a dramatic 72 percent (72%) compared to Q1 2023 and an 81 percent (81%) decrease from the previous Quarter. Q1 represents the fewest number of people impacted by data compromises in any quarter since Q1 2022.
- Attacks increased across 15 of 17 industries tracked by the Identity Theft Resource Center (ITRC). Financial Services (224 notices) displaced Healthcare (124 notices) as the most attacked industry in Q1. However, Healthcare remained at the top spot for industries represented in the Top Ten compromises. Attacks against Professional Services (100 notices) more than doubled, becoming the third industry to publish triple-digit notices in the Quarter. Interestingly, the Non-Profit industry entered the list of the Top Ten breaches in the Quarter for the first time.

Analysis

- In Q1:
  - Data compromises reported in Q1 2024 totaled 841, including 642 cyberattacks, 85 compromises caused by System or Human Errors, and 11 Physical Attacks, impacting an estimated 28,596,892 victims. This represents a 90 percent (90%) increase over the same Quarter in 2023 and a 108 percent (108%) increase over Q1 2022.
  - Cyberattacks remained, by a wide margin, the primary cause of data breaches where personal information was stolen. However, the number of cyberattack-related data breach notices without information about the root cause of the attack jumped from 166 in Q1 2023 to 439 in Q1 2024, or from 44 percent (44%) to 68 percent (68%) of cyberattack-related breach notices.

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through March 31, 2024.

- Publicly traded companies regulated by the U.S. Securities and Exchange Commission (SEC) or the Federal Communications Commission (FCC)[1] are under new reporting mandates that require more information sharing on a more timely basis. These new regulations appear to be prompting more information sharing. However, only 75 of the 841 entities reporting a compromise in Q1 were subject to the new regulations, a nine percent (9%) rate that is consistent with the overall number of publicly traded companies vs non-public and non-profit entities.
- Only two industries tracked by the ITRC reported fewer data breach notices on a Q1-to-Q1 basis, reflecting a broader trend of threat actors launching more attacks against an expanded set of targets that, ironically, impact fewer individuals. Notices from Financial Services tripled year-over-year (YoY) (70 notices in Q1 2023 compared to 224 in Q1 2024), displacing Healthcare (81 notices in 2023 compared to 124 in Q1 2024) as the most attacked industry. Healthcare notices still make up 50 percent (50%) of the Top Ten compromises in terms of the estimated number of victims impacted. Attacks against Professional Services firms (law firms, accounting firms, consulting firms, for example) more than doubled in Q1 2024 compared to the same period in 2023, becoming the third industry to issue 100 or more compromise notices.
- The number of organizations impacted by Supply Chain Attacks more than tripled in Q1 2024 compared to the same period in 2023. Fifty (50) new attacks in the Quarter impacted 243 organizations and ~7.5M victims compared to 73 entities and ~11.4M victims in Q1 2023.
- The consensus among cybersecurity experts and the ITRC is that the number of victims per compromise is drifting lower as identity criminals launch more targeted assaults that are vastly different from the "pray & spray" attacks of the late 20-teens. However, more breaches with fewer people impacted does not mean individuals or businesses can reduce their level of diligence. For example, legitimate login credentials remain a common attack vector that can be obtained in focused attacks and used to launch various attacks and identity scams, including Supply Chain Attacks that compromise multiple organizations in a single exploit. ***Businesses and consumers need to continue to practice good password hygiene and transition to Passkeys as soon as possible.***

[1] **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.

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through March 31, 2024.

Q1 Data Compromise Highlights

ITRC | IDENTITY THEFT RESOURCE CENTER

Number of Q1 Compromises

841 TOTAL COMPROMISES

28,596,892 TOTAL VICTIMS

734 DATA BREACHES
28,474,351 VICTIMS

4 DATA EXPOSURES
20,600 VICTIMS

0 DATA LEAKS
0 VICTIMS

103 UNKNOWN COMPROMISES
101,943 VICTIMS

Q1 Attack Vectors

CYBERATTACKS
642 Breaches
28,261,784 Victims

SYSTEM AND HUMAN ERRORS
85 Breaches/Exposures
180,796 Victims

PHYSICAL ATTACKS
11 Breaches/Exposures
52,371 Victims

SUPPLY CHAIN ATTACKS
50 Breaches/Exposures
243 Entities Affected
7,510,903 Victims

Top Compromises by Industry in Q1

FINANCIAL SERVICES	*224 Compromises*
HEALTHCARE	*124 Compromises*
PROFESSIONAL SERVICES	*100 Compromises*
MANUFACTURING	*77 Compromises*
GOVERNMENT	*43 Compromises*

Q1 Public Data Breach Notices

550 NOTICES WITHOUT ATTACK VECTOR

291 NOTICES WITH ATTACK VECTOR

Top 5 Compromises by Victim Count in Q1

LOANDEPOT, INC.
16,924,071 VICTIMS

MEDICAL MANAGEMENT RESOURCE GROUP, LLC
2,350,236 VICTIMS

EASTERN RADIOLOGISTS, INC.
886,746 VICTIMS

UNITE HERE
791,273 VICTIMS

PLAZA RADIOLOGY
569,022 VICTIMS

ITRC IDENTITY THEFT RESOURCE CENTER
888.400.5530
idtheftcenter.org

Q1 2024 Data Compromise Charts

Top 10 Compromises of Q1 2024

	Entity	Victims Impacted
1	loanDepot, Inc.	16,924,071
2	Medical Management Resource Group, LLC dba American Vision Partners	2,350,236
3	Eastern Radiologists, Inc.	886,746
4	UNITE HERE	791,273
5	Plaza Radiology dba Chattanooga Imaging	569,022
6	Azura Vascular Care	348,000
7	Deli Management, Inc. dba Jason’s Deli	344,034
8	Houser LLP	326,386
9	Des Moines Orthopaedic Surgeons, P.C.	307,864
10	V12 Software, Inc.	286,396

Compromise Year-over-Year Totals

Year	Compromises	Victims
Q1 2024	841	28,596,892
2023	3,203	416,205,332
2022	1,801	425,212,090
2021	1,860	373,607,163
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
*The AT&T victim count has been added to the 2021 victim count as the compromise initially occurred and was entered in 2021. The 73M is not reflected in the Q1 2024 victim count.		

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through March 31, 2024.

Compromises by Sector Q1 2024 vs. Q1 2023 & 2022

	Year					
	Q1 2024		Q1 2023		Q1 2022	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	36	501,925	31	569,618	21	106,099
Financial Services	224	18,262,986	70	10,555,103	68	5,732,597
Government	43	126,500	23	759,622	13	790,763
Healthcare	124	6,071,259	81	14,199,413	73	4,377,462
Hospitality	16	687,334	7	196,891	6	57,392
HR/Staffing	4	119,758	3	20,616	-	-
Manufacturing	77	143,423	49	1,190,146	52	249,706
Mining/Construction	19	10,032	15	59,292	-	-
Non-Profit/NGO	38	824,029	19	85,420	20	629,822
Professional Services	100	683,246	48	75,502	45	3,022,491
Retail	22	39,092	16	179,622	18	272,950
Social Services	1	5	3	154,160	-	-
Technology	40	634,212	35	24,399,696	16	10,832,588
Transportation	38	122,942	13	11,096,783	8	20,930
Utilities	18	204,730	6	37,054,637	-	-
Wholesale Trade	11	10,690	11	62,316	-	-
Other	28	154,727	12	27,698	64	675,411
Unknown	2	2	-	-	-	-
Totals:	841	28,596,892	442	100,686,535	404	26,768,211

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through March 31, 2024.

Attack Vector Q1 2024 vs. Q1 2023 & 2022

	Q1 2024	Q1 2023	Q1 2022
Cyberattacks	642	375	366
Phishing/Smishing/BEC	108	111	112
Ransomware	58	58	71
Malware	11	20	24
Non-Secured Cloud Environment	1	5	3
Credential Stuffing	10	8	2
Unpatched Software Flaw	2	-	-
Zero Data Attack	5	2	-
Other	8	5	7
NA – Not Specified	439	166	147
System & Human Error	85	59	33
Failure to Configure Cloud Security	4	7	4
Correspondence *(Email/Letter)*	27	23	12
Misconfigured Firewall	4	5	5
Lost Device or Document	4	-	1
Other	38	21	5
NA – Not Specified	8	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	-	-
NA – Not Specified	-	-	-
Data Leak	-	-	-
Unknown	103	2	2

Unless otherwise noted, all data reported here was entered into the ITRC *notified* database between January 7, 2024, through March 31, 2024.

Quarter-to-Quarter

Year	Compromises	Victims
Q1 2024	841	28,596,892
Q4 2023	1,087	152,679,771
Q3 2023	734	80,913,625
Q2 2023	940	81,925,401
Q1 2023	442	100,686,535
Q4 2022	513	253,224,691
Q3 2022	471	109,967,747
Q2 2022	413	35,251,441
Q1 2022	404	26,768,211

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.