JANUARY 2023

ITRC | IDENTITY THEFT RESOURCE CENTER

2022 DATA BREACH REPORT

idtheftcenter.org • 1-888-400-5530

Table of Contents

CEO Letter

Each year there is some new superlative that gets attached to a statistic about cyberattacks and data compromises. Many times, it describes a number as the "most" or "highest" or "biggest" of its kind. In 2022 it was the number 1,862, representing the largest number of publicly reported data compromises in a single year in the United States.

On the rare occasion, we also get to use words like "fewer" and terms like "downward trending" when it comes to identity compromises. In 2022 we reported fewer victims of identity crimes than the year before, for example.

In 2023, the number to remember is 34 percent (34%). It relates to the lowest number of public breach notices that include victim and attack details in five (5) years. In other words, the information individuals and businesses needed to determine the risk to their identity information after a compromise was ***not*** included in approximately two-thirds of all public breach notices.

While we did not set a record for the number of data compromises in the U.S. during 2022, we came close. The 1,802 data compromises reported last year was the second highest number of compromises reported in a single year, impacting ~422 million individuals primarily due to cyberattacks (not accounting for individuals impacted by multiple breaches).

At least 422 million individuals. I use the term "at least" to make an important point about the statistics in the previous paragraphs. In reality, these numbers are estimates because data breach notices are increasingly being issued with less information. *Figure 1* and *Figure 2* show the trend lines.

Figure 1 | *Notices with Attack Details*

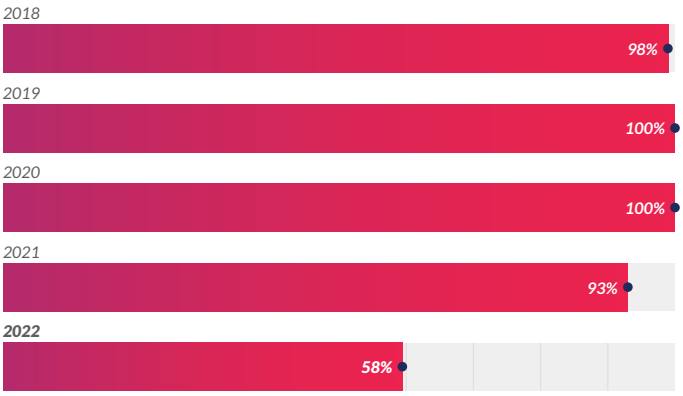
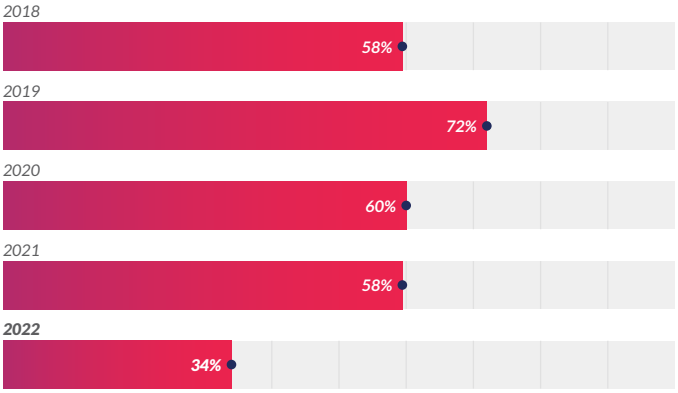


Figure 2 | *Notices with Attack & Victim Details*



The charts make it clear; the number of breach notices with detailed attack and victim information has dropped by more than 50 percent (50%) since 2019. The result of these trends is less reliable data that impairs the ability of individuals, businesses, and government officials to make informed decisions about the risk of a data compromise and the actions to take in the aftermath of one.

The trend away from transparency also points out the overall inadequacy of the current patchwork quilt of state data breach notification laws, many of which now date back to 2005 when virtually all breaches involved paper records, lost or stolen laptops, or data tapes lost in transit. In 2022, cyberattacks caused 90 percent (90%) of all data breaches.

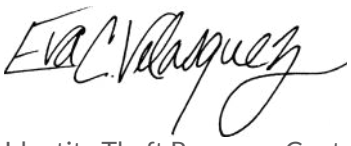
Most states put the burden of determining the risk of a data breach to individuals or business partners on the organization that was compromised. Oregon stands out as an exception because law enforcement agencies and the impacted organization jointly make the decision if individuals are at risk as a result of the breach. In all states, if the determination is there is no risk, then there is no notice.

In the U.S. there were an average of ~seven (7) breach notices issued each business day in 2022. Compare that to the 356 breach notices issued each day in the European Union during 2021, the last year for which data is available. In the E.U., as in Oregon, data protection/law enforcement officials and the compromised organization make the determination that individuals or businesses are at risk, requiring a full notice to the impacted parties.

Common sense tells us that data breaches are underreported in the United States. The 1,802 reported here are a minimum estimate. The trends related to publicly reported data breaches in 2022 reinforce the conclusion that the data breach environment is worse than we know and can prove with quantifiable data. The result is individuals are largely unable to protect themselves from the harmful effects of data compromises which are fueling an epidemic – a "scamdemic" – of identity fraud committed with stolen or compromised information.

In the pages that follow, we'll explore our interpretation of the shifts in the information related to data compromises. Increasingly, it is not so much what we know, but what we do not know that is the most troubling and compelling. The full picture of the impacts of data compromises is unclear and we hope this report will be the start of a national conversation on how to bring more clarity, transparency, and effectiveness to the breach notice process.

Eva Velasquez, *CEO*



Identity Theft Resource Center
January 2023

Key Findings of 2022 Data Compromises

+ *Summary of Key Findings*
+ *At-a-Glance*
+ *Analysis of Key Findings*

Summary of Key Findings

The Identity Theft Resource Center (ITRC) has collected, analyzed, and published information about publicly reported data compromises since 2005. While 2021 represented an all-time high for data compromises reported in the United States, 2022 represents a rare plateau for data events after years of steady increases in the number of reported compromises.

This report focuses on three key findings:

Data compromises in 2022, overall, were flat compared to 2021 while the estimated[1] number of victims jumped dramatically due to data breaches at a single organization.

A sudden lack of transparency in the content of data breach notices created risk for victims and fueled uncertainty about the true scale and impact of data compromises.

The number of data breaches resulting from supply chain attacks significantly exceeded compromises linked to malware.

[1]The ITRC describes the number of data compromise victims as "estimated" due to the fact not all states require the number of impacted individuals be disclosed in breach notices; and, there is currently no methodology to accurately determine how many individuals are impacted by multiple data compromises. In July 2022 the U.S. Census Bureau reported the number of people 18 years or older residing in the U.S. to be 259 million.

2022 DATA BREACH REPORT

idtheftcenter.org • 1-888-400-5530

The Annual Data Breach Report explores fundamental shifts in the root causes of identity-related crimes. While 2021 represented an all-time high for data compromises reported in the United States, 2022 represents a rare plateau for data events after years of steady increases in the number of reported compromises.

ITRC | IDENTITY THEFT RESOURCE CENTER

Compromises in 2022

1,802
TOTAL COMPROMISES

422,143,312
TOTAL VICTIMS

1,774 DATA BREACHES
392,180,551 VICTIMS

18 DATA EXPOSURES
7,146,425 VICTIMS

10 UNKNOWN COMPROMISES
22,816,336 VICTIMS

Public Data Breach Notices

66% of Notices
*Did **Not** Include Victim and Attack Details*

Supply Chain Attacks on the Rise

The number of supply chain attacks leapt past malware-based compromises in 2022.

+10 Million
Individuals Impacted in 2022

***+1,700 Entities** Were Targeted*

***40% More** Supply Chain Attacks than Malware Attacks*

Top 10 Compromises of 2022

01	Twitter	221,524,284 Victims
02	Neopets	69,000,000 Victims
03	AT&T Data	22,786,997 Victims
04	Cash App Investing, LLC	8,200,000 Victims
05	Beetle Eye	7,000,000 Victims
06	Twitter	5,485,636 Victims
07	Receiveables Performance Management, LLC	3,766,573 Victims
08	Flexbooker	3,756,794 Victims
09	Eye Care Leaders	3,372,880 Victims
10	Advocate Aurora Health	3,000,000 Victims

Top 10 Data Breach Attributes

Personally Identifiable Information (PII)	*Compromises*
Name	*1,560*
Full Social Security Number	*1,143*
Date of Birth	*633*
Current Home Address	*565*
Driver's License/State ID Number	*499*
Medical History/Condition/Treatment/Diagnonsis	*465*
Bank Account Number	*443*
Medical Insurance Account Number	*370*
Undisclosed Records	*226*
Medical Provider Account/Record Number	*196*

Analysis of Key Findings

The number of publicly reported data compromises in the U.S. totaled 1,802 in 2022. This represents the second highest number of data events in a single year and just 60 events short of matching 2021's all-time high number of data compromises. In reviewing the various data compromise notices, including data breaches, three major trends emerged.

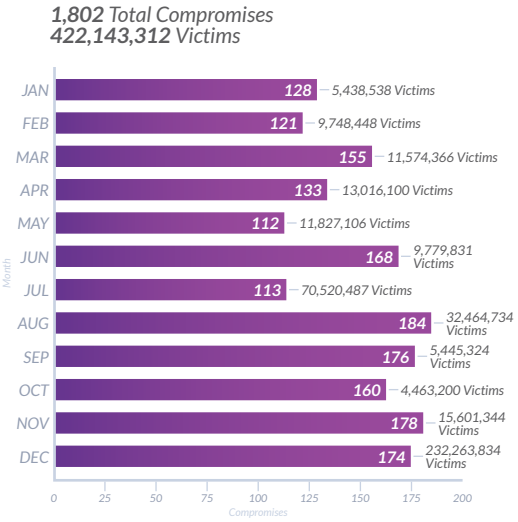
Data compromises overall were flat compared to 2021; the annual estimated victim count exceeded the previous year due to two breaches at one organization.

The first half of 2022 saw fewer data compromises reported and generally fewer victims. Cybersecurity experts pointed to Russia-based cybercriminals being distracted by the war in Ukraine for the overall drop in ransomware and cyberattacks early in the year. Extreme volatility in the cryptocurrency markets, the currency of choice for cybercriminals, was also believed to have contributed to a re-focusing of cybercriminals on other attack vectors such as phishing-based scams using stolen data and supply chain attacks.

However, the number of data compromises steadily increased in the latter half of 2022. A ~21 percent (21%) increase in compromises over the first half of 2022 turned what would have been a significant decrease in reported events into a horse race to see if the year would meet or exceed 2021's record setting pace.

See Figure 3

Figure 3 | *Compromises by Month, 2022*



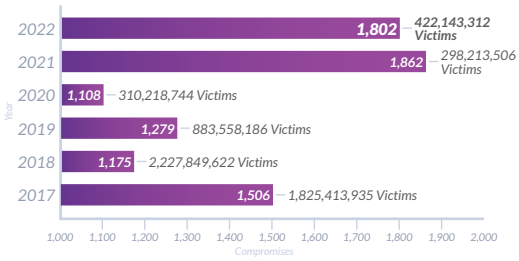
For 11 of the 12 months in 2022, the estimated number of data compromise victims was on a downward trend line for the 6th consecutive year. That trend reversed with news that personal information of 221 million Twitter users were available in illicit identity marketplaces. But for that single data compromise related to a software flaw believed to have been patched, the estimated number of data compromise victims would have dropped by ~33 percent (33%) year-over-year.

As detailed in the ITRC's *2022 Trends in Identity* and *2022 Consumer Impact* reports, there has been a dramatic increase in identity scams and fraud where cybercriminals impersonate an individual using stolen data and/or information gleaned from social media accounts to apply for government benefits and to open new financial and non-financial accounts. These impersonation attacks can also result in the takeover of existing accounts as well.

The result of this dynamic – using an individual's stolen personal information in a wide variety of identity scams to generate cash – is there are generally fewer victims of data breaches. However, the financial impact is likely higher and the time to remediate the effects of the identity misuse is longer.

See Figure 4

Figure 4 | *Total Compromises & Victims*



Data breach notices suddenly lacked detail, resulting in increased risk for individuals and businesses as well as uncertainty about the true number of data breaches and victims.

For most of the 20 years since the first data breach notice law was enacted in 2003, data breach notices generally included information that could help individuals and businesses determine the relative risk of any given breach and the steps to take to protect against similar attacks. However, beginning in Q4 2021 and accelerating throughout 2022, the trend has reversed with less information being included in required public notices.

In 2022, 747 data compromises were announced in notices that did not specify a root cause of the event. That compares to the 1,595 compromises linked to cyberattacks.

See Figure 5

The chart to the right shows the high rate of information sharing for the past five (5) years and the dramatic decrease in details in breach notices in 2022. Additional research is required to pinpoint the primary cause(s) of the sudden lack of information regarding the root cause of data breaches and the number of individual victims impacted by the compromises.

Figure 5 | *Data Breach Notices with Details*

	2022	2021	2020	2019	2018
Compromises	1,802	1,862	1,108	1,279	1,175
Notices with Attack Vectors/Details	1,045	1,732	1,107	1,277	1,163
Percentage	58%	93%	~100%	~100%	99%
Notices with Victim Count & Attack Vectors/Details	605	1,075	663	917	681
Percentage	34%	58%	60%	72%	58%

However, there is ample anecdotal evidence to suggest several causes:

- ***Recent court decisions provide an incentive to keep information sharing to a minimum.***
  Federal courts in different parts of the U.S. have recently issued rulings supporting the conclusion that actual harm, not potential harm, is required for an individual to file a damage claim linked to a data breach[2]. Absent a requirement to include details of the attack leading to a data breach and the number of victims, which most state laws do not include, businesses may no longer be inclined to include detailed information for fear of revealing facts that can be used in a lawsuit against the company.

- ***Companies are making a conscious decision to withhold information.***
  Organizations as varied as Samsung, DoorDash, and LastPass have little in common on most days, but in 2022 they all announced they had been the victim of a data breach. They, and 66 percent (66%) of other companies issuing a data breach notice, also decided to include limited or no detail about what happened and who was impacted in their state-mandated breach notice.

- ***Shifting cybersecurity priorities and an increasing volume of cyberattacks make it difficult to determine what happened and who was impacted.***
  Quickly determining the cause and effects of a data compromise is rarely easy. The 2022 IBM Cost of a Data Breach study indicates the median number of days to identify a breach is 207 days. Organizations that are preparing for a potential financial downturn or recession in 2023 are realigning their cybersecurity priorities. The result may be an increase in the amount of time required to quickly determine what happened and why due to reduced resources available for forensic activities.

- ***A lack of breach details creates risk.***
  Privacy and security experts have struggled for years to help the victims of data compromises understand the relative risk of their personal information being stolen by criminals or accidentally exposed. Large numbers of people impacted generated large headlines but did not always translate into the highest level of risk.

[2]Other federal courts have found the risk of future harm is all that is required to claim damages. This split between Circuit Courts of Appeals often triggers interest from the U.S. Supreme Court to settle the issue.

In 2020, the ITRC and a technology partner (now known as Sontiq, a TransUnion Company) launched services to help individual consumers learn more about the risks resulting from the data breaches impacting them and their personal information. The ITRC offered a robust, searchable database of data compromises and the attributes of each event based on public notices. Sontiq created a risk score based on the ITRC's data and a proprietary algorithm.

The higher the breach risk score, the higher the risk and the more urgent it is that individuals take protective actions as soon as possible. The chart below shows the risk scores of the largest data compromises in 2022.

See Figure 6

Figure 6 | *Top 10 Compromises of 2022*

	Entity	Victims Impacted	Breach IQ Score
1	Twitter	221,524,284	N/A
2	Neopets	69,000,000	3
3	AT&T Data	22,786,997	5
4	Cash App Lending, LLC	8,200,000	1
5	Bettle Eye	7,000,000	3
6	Twitter	5,485,636	N/A
7	Receivables Performance Management, LLC	3,766,573	3
8	Flexbooker	3,756,794	3
9	Eye Care Leaders	3,372,880	7
10	Advocate Aurora Health	3,000,000	1

Without robust information sharing and reliable breach notices, organizations like the ITRC that rely on data breach notices to assist data breach victims (and the victims themselves) do not have access to the information needed to develop a complete view of the environment and make fact-based recommendations to individuals and small businesses.

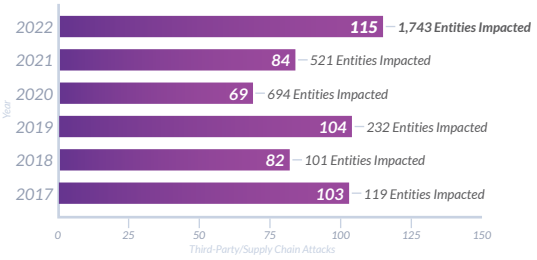
The number of data breaches resulting from supply chain attacks now exceeds compromises linked to malware.

Malware is popularly viewed as the core of most cyberattacks, but in 2022, supply chain attacks[3] surpassed the number of malware-based attacks by about 40 percent (40%). With major ransomware operators largely distracted by the conflict in Ukraine, supply chain attacks rebounded with a vengeance. More than 10 million people were impacted by supply chain attacks targeting 1,743 entities that had access to multiple organizations' data. Compare that to the 70 malware-based cyberattacks in 2022 that impacted 4.3 million people.

Phishing and related exploits remain the number one cyberattack vectors that lead to data breaches, followed by ransomware.

See Figure 7

Figure 7 | *Supply Chain Attacks Per Year*



[3]*Supply chain attacks are cyberattacks against a single entity in hopes of gaining access to information maintained by the organization on behalf of other businesses or institutions.*

Not All the News is Bad

There is some good news to be found in the trends surrounding data compromises and breach notices.

- The states of Maryland and Pennsylvania have updated their data breach laws in the past year. Maryland now requires organizations to report the details surrounding a data breach including the number of victims within ten (10) days of learning of a data breach (down from 45 days). Pennsylvania has updated their law to expand the definition of personally identifiable information to include health related information as well as usernames and email credentials.
- The number of data breaches and data exposures linked to unprotected cloud databases dropped 75 percent (75%) in 2022 compared to 2020. In 2020, 107 cloud databases with no security exposed the personal information of 155million individuals; in 2022, only 27 unsecured cloud databases caused a data breach or exposure that impacted ~7 million people.

  See Figure 8
- Physical attacks continued a multi-year downward trend, dropping to 46 out of 1,802 compromises. Nearly half were related to stolen devices. System and Human Error-based data compromises also dropped in 2022 with most events related to personal information being exposed in emails and other correspondence.

  See Figure 9
- The number of compromises increased in six (6) out of 12 industries in 2022, but the number of estimated victims dropped in seven (7) of the dozen (12) areas tracked by the ITRC. The largest growth in compromises occurred in the Healthcare, Manufacturing & Utilities, and Professional Services industries. The largest growth in terms of estimated victims was in the Financial Services, Hospitality, Technology, and Transportation industries even though the number of compromises dropped in each group except Technology.

Figure 8 | *Compromises by Attack Vector*

	2022	2021	2020
Cyberattacks	***1,595***	***1,613***	***878***
Phishing/Smishing/BEC	*461*	*537*	*383*
Ransomware	*276*	*352*	*158*
Malware	*70*	*141*	*104*
Non-Secured Cloud Environment	*9*	*24*	*50*
Credential Stuffing	*18*	*14*	*17*
Unpatched Software Flaw	*–*	*4*	*3*
Zero Attack Day	*8*	*4*	*1*
Other	*26*	*426*	*162*
Not Specified	*727*	*111*	*–*
System & Human Errors	***151***	***179***	***152***
Failure to Configure Cloud Security	*18*	*54*	*57*
Correspondence (Email/Letter)	*55*	*66*	*55*
Misconfigured Firewall	*30*	*13*	*4*
Lost Device or Document	*6*	*12*	*5*
Other	*23*	*34*	*31*
Not Specified	*19*	*–*	*–*
Physical Attacks	***46***	***51***	***78***
Document Theft	*7*	*9*	*15*
Device Theft	*21*	*17*	*30*
Improper Disposal	*5*	*5*	*11*
Skimming Device	*6*	*1*	*5*
Other	*6*	*19*	*17*
Not Specified	*1*	*–*	*–*
Data Leaks	*–*	***7***	*–*
Unknown	***10***	***12***	*–*
Totals	***1,802***	***1,862***	***1,108***

Figure 9 | *Compromises by Industry*

	2022		2021		2020	
	Comp.	Victims	Comp.	Victims	Comp.	Victims
Education	100	1,745,226	125	1,687,192	42	974,054
Financial Services	268	27,146,354	279	19,978,108	138	2,687,084
Government	74	1,739,462	66	3,244,455	47	1,100,526
Healthcare	344	26,259,933	330	30,853,767	306	9,700,238
Hospitality	34	69,235,147	33	238,445	17	22,365,384
Manufacturing & Utilities	249	23,897,836	222	49,782,583	70	2,896,627
Non-Profit/ NGO	71	980,021	86	2,339,646	31	37,528
Professional Services	224	6,248,711	184	22,729,391	144	73,012,145
Retail	65	792,195	102	7,212,912	53	10,710,681
Technology	86	248,564,988	79	44,684,180	67	142,134,883
Transportation	36	3,991,847	44	569,684	21	1,208,292
Other	251	11,541,592	308	79,660,479	172	43,391,302
Unknown	–	-	4	35,232,664	–	-
Totals	***1,802***	***422,143,312***	***1,862***	***298,213,506***	***1,108***	***310,218,744***

Case Studies

While every data breach has unique elements, there are common threads that illustrate the trends identified during 2022. The following data breaches reflect these trends.

+ *Fixed Software That Doesn't Stay Fixed*
+ *That's Our Data, But Not Our Breach*
+ *No Detail is Not Good*
+ *Breaking Supply Chains*

Fixed Software That Doesn't Stay Fixed

Twitter

Announced December 2022

In a series of breaches announced by threat actors and cybersecurity researchers – but not Twitter – more than 400 million accounts attached to an estimated 221 million users were offered for sale by cybercriminals in an illicit identity marketplace. The information was believed to have been scraped from Twitter by identity thieves who took advantage of a software flaw that was reported to have been fixed earlier in 2022, but was still vulnerable to exploitation.

221,524,284
Individuals Impacted

Source:
Hacker Claims to be Selling Twitter Data – Bleeping Computer

That's Our Data, But Not Our Breach

AT&T

Announced August 2022

Cybersecurity researchers found a file on a popular dark website containing 22.8 million unique email addresses and 23 million unique social security numbers believed to related to customers of AT&T. The telecom company did not issue a data breach notice to consumers and denied the information was stolen from their system. AT&T acknowledged the stolen data "may be tied to a previous data incident at another company," but did not elaborate.

22,786,997
Individuals Impacted

28,500,000
Records Breached/Exposed

Source:
It Might Be Our Data, But It's Not Our Breach – Krebs on Security

No Detail is Not Good

LastPass

Announced August 2022
Updated December 2022

Unknown
Individuals Impacted

Cybercriminals gained access to source code and software development information stored by LastPass, a fact the company announced in August 2022. The password management company announced at the time that the thieves had not accessed customer information. In December, the company announced that cybercriminals had indeed gained access to customer information using the information stolen in August. LastPass has not acknowledged how many accounts or individuals were compromised in the attack.

Sources:

Notice of Recent Security Incident – LastPass

Yes, It's Time to Ditch LastPass – Wired

Five Guys Enterprises, LLC

Announced December 2022

37,529
Individuals Impacted

Despite learning of a data breach of an employee application system in September 2022, fast-food chain Five Guys waited to alert government officials and impacted consumers to the compromise in a letter dated December 29, 2022. The number of individuals impacted, and the specific data exposed, was not disclosed, or information about the attack or corrective action taken to prevent a repeat occurrence has been released.

Sources:

Five Guys Consumer Notification – Montana Attorney General's Office

Five Guys Data Breach Puts HR Data Under a Heat Lamp – DarkReading

Breaking Supply Chains

Professional Finance Company, Inc. *(PFC)*

Announced May 2022
Updated July 2022

1,918,941
Individuals Impacted

618 Entities
Impacted by Breach

Accounts receivable management company PFC was the target of ransomware in February 2022 as part of a supply chain attack against a business that supports hundreds of healthcare organizations. The information of more than 600 client firms of PFC was compromised in the attack. PFC did not initially provide a victim count, but later filed a required notice with the U.S. Department of Health and Human Services disclosing that nearly 2 million individuals may have been impacted.

Sources:

PFC Breach Letter – Montana Attorney General's Office

Healthcare Providers Affected by Ransomware Attack on Professional Finance Company – HIPAA Journal

Illuminate Education

Announced March 2022

Illuminate Education provides a popular attendance and grading platforms used by school systems across the country. In January 2022, the largest breach of student information in the nation's history occurred when threat actors gained access to the data of millions of students in a single assault – a classic supply chain attack. Illuminate did not alert school officials until March 2022 of the event and did not reveal how many students may have been impacted, instead leaving the job of notifications to individual school districts. Illuminate was acquired by another education tech company in August 2022.

2,108,045*
Victim Count

611 Entities
Impacted by Breach

**Total number of victims has not been reported; victim count as of 1/5/2023.*

Sources:

Data for New York K-12 Students Compromised in Hack – UPI

List of All K-12 Schools Known to be Impacted by Illuminate Breach of Student Data as of Sept 2022 – THE Journal

Breach Alert for Business

notified **is the most comprehensive repository of publicly reported, U.S.-based data breaches.**

Details in data breach notices are decreasing while the number of data breach announcements (issued by website posts and news releases) is increasing. As a result, consumers or businesses may not receive a direct notification of a data breach with actionable information so they can take steps to protect themselves.

notified, our data compromise tracking tool, is a free service to consumers and as a batch or subscription service for businesses.

The ITRC is offering a new version of the Center's data breach alert service currently limited to consumers. Breach Alert for Consumers allows individuals to request an email alert if a data breach involving an entity where the person has a relationship is added to the ITRC's ***notified*** breach database. Breach Alert for Consumers is available free of charge.

Most state data breach laws do not require business customers to be alerted in the event of a data breach or other data compromise. That means absent a contractual obligation to inform a business customer of a data compromise, organizations may not know when a vendor suffers a data compromise.

Breach Alert for Business *is a paid service that helps organizations comply with company cybersecurity and risk management policies as well as statutory and regulatory requirements to verify vendors are meeting or exceeding a company's cybersecurity policies and performance. The service confirms vendors' previous data breaches and issues alerts in the event a vendor is the subject of future data compromises.*

Breach Alert for Business, available in late Q1 2023, provides businesses with the ability to conduct due diligence and monitor partner organizations and prospective vendors. Services include breach searches on a batch basis, or an unlimited number of breach searches and future breach monitoring alerts on a paid subscription basis. Discounts are available for annual payments as well as multi-year subscriptions.

For more information about ITRC's Breach Alert for Business, please contact ***notifiedByITRC@IDTheftCenter.org***.

2022 DATA BREACH REPORT

idtheftcenter.org • 1-888-400-5530

ITRC | IDENTITY THEFT RESOURCE CENTER

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, ***click here*** or contact the ITRC by email at ***communications@idtheftcenter.org***.

For Media

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

Appendix

+ *2022 Quarterly Breakdown: Data Breach Analyses*
+ *Glossary of Terms*
+ *About Data Collection, Data Compromises & Breach Notices*

All victim counts within this report are estimates.

Data Breach Analysis: Year End, 2022

Number of 2022 Compromises

Total Data Compromises: 1,802 Compromises; 422,143,312 Victims
- **Data Breaches:** 1,774 Data Breaches; 392,180,551 Victims
- **Data Exposures:** 18 Data Exposures; 7,146,425 Victims
- **Data Leaks:** N/A
- **Unknown:** 10 Unknown Compromises; 22,816,336 Victims Impacted

Attack Vectors, End of Year 2022

Cyberattacks: 1,595 Breaches; 374,992,920 Victims
- + 461 Phishing/Smishing/BEC
- + 276 Ransomware
- + 70 Malware
- + 26 Other
- + 18 Credential Stuffing
- + 9 Non-Secured Cloud Environment
- + 8 Zero Day Attack
- + 727 Not Specified

System & Human Errors: 151 Breaches/Exposures; 24,130,504 Victims
- + 55 Correspondence *(Email/Letter)*
- + 30 Misconfigured Firewalls
- + 23 Other
- + 18 Failure to Configure Cloud Security
- + 6 Lost Device or Document
- + 19 Not Specified

Physical Attacks: 46 Breaches; 203,552 Victims
- + 21 Device Theft
- + 7 Document Theft
- + 6 Other
- + 6 Skimming Device
- + 5 Improper Disposal
- + 1 Not Specified

Supply Chain Attacks *(Included in Attack Vectors Above)*
- **Third-Party/Supply Chain Attack *(118)*:** 1,743 Entities; 10,038,594 Victims
- **Cyberattack:** 1,726 Entities; 9,882,244 Victims
- **System & Human Errors:** 17 Entities; 156,350 Victims

Noteworthy Supply Chain Attacks *(As of 01/09/2023)*
- ***Professional Finance Company:*** 618 Entities; 1,918,941 Victims
- ***Illuminate Education:*** 611 Entities; 2,108,045 Victims*
  **Note: The ITRC is entering districts as information is reported. The total number of victims per district has not been disclosed.*
- ***Shields Health Care Group, Inc.:*** 56 Entities; 1,804,069 Victims
- ***OneTouchPoint, Inc.:*** 43 Entities; 2,651,396 Victims
- ***Eye Care Leaders:*** 37 Entities; 3,372,880 Victims
- ***Practice Resources, LLC:*** 28 Entities; 942,138 Victims
- ***MCG Health, LLC:*** 10 Entities; 793,283 Victims

Horizon Actuarial Services, LLC: 3 Entities; 2,292,080 Victims
Nelnet Servicing, LLC: 2 Entities; 2,501,324 Victims
Comstar, LLC: 2 Entities; 585,621 Victims
Adaptive Health Integrations: 1 Entities; 510,574 Victims
Connexin Software, Inc.: 1 Entities; 2,216,365 Victims

Charts

Top 10 Compromises of 2022

	Entity	Victims Impacted	Breach IQ Score
1	Twitter	221,524,284	N/A
2	Neopets	69,000,000	3
3	AT&T Data	22,786,997	5
4	Cash App Investing, LLC	8,200,000	1
5	Beetle Eye	7,000,000	3
6	Twitter	5,485,636	N/A
7	Receivables Performance Management, LLC	3,766,573	3
8	Flexbooker	3,756,794	3
9	Eye Care Leaders	3,372,880	7
10	Advocate Aurora Health	3,000,000	1

Compromises & Victims, Month-by-Month 2022

	Compromises	Victims
January	128	5,438,538
February	121	9,748,448
March	155	11,574,366
April	133	13,016,100
May	112	11,827,106
June	168	9,779,831
July	113	70,520,487
August	184	32,464,734
September	176	5,445,324
October	160	4,463,200
November	178	15,601,344
December	174	232,263,834
Total	**1,802**	**422,143,312**

Compromises & Victims, Year-over-Year

	Compromises	Victims
2022	**1,802**	**422,143,312**
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
2016	1,088	2,541,092,072

Compromises by Attack Vector: 2022, 2021, 2020

	2022 YTD	2021	2020
Cyberattacks	**1,595**	**1,613**	**878**
Phishing/Smishing/BEC	416	537	383
Ransomware	270	352	158
Malware	70	141	104
Non-Secured Cloud Environment	9	24	50
Credential Stuffing	18	14	17
Unpatched Software Flaw	–	4	3
Zero Attack Day	8	4	1
Other	26	426	162
Not Specified	727	111	–
System & Human Errors	**151**	**179**	**152**
Failure to Configure Cloud Security	18	54	57
Correspondence (Email/Letter)	55	66	55
Misconfigured Firewall	30	13	4
Lost Device or Document	6	12	5
Other	23	34	31
Not Specified	19	–	–
Physical Attacks	**46**	**51**	**78**
Document Theft	7	9	15
Device Theft	21	17	30
Improper Disposal	5	5	11
Skimming Device	6	1	5
Other	6	19	17
Not Specified	1	–	–
Data Leaks	**–**	**7**	**–**
Unknown	**10**	**12**	**–**
Totals	**1,802**	**1,862**	**1,108**

Data Exposed/Breached Per Year

	2022	2021	2020	2019	2018
SSN	1,141	1,151	562	639	617
PHI	556	563	409	484	371
Driver's License	500	456	218	192	183
Bank Account	448	416	218	221	226
Email/Password	175	252	233	192	176
Credit/Debit Card	186	215	182	236	207
Other	221	255	201	218	262

Data Attributes: Personally Identifiable Information *(PII)*

	Compromises Containing PII Piece
Name	1,560
Full Social Security Number	1,143
Date of Birth	633
Current Home Address	565
Driver's License/State ID Number	499
Medical History/Condition/Treatment/Diagnosis	465
Bank Account Number	443
Medical Insurance Account Number	370
Undisclosed Records	226
Medical Provider Account/Record Number	196
Payment Card Full Number	186
Payment Cardholder Name	172
Phone Number	166
Personal Email Address	146
Payment Card Expiration Date	145
Payment Card Security Number	142
Passport Number/Visitor Status/Green Card	125
Bank Account Routing Number	74
Other Account Credentials	41
Income/Wages/Earnings/Compensation	36
Student ID Number/Login/Details	21
Biometric/Authentication Data	17
Loan Account Details or Credentials	13
Employee ID Number/Credentials/Position/Etc.	13
IP Address	11
Medical Provider Login	10
Work Email Address	10
Partial Social Security Number	9
Payment Card Partial Number	9

	Compromises Containing PII Piece
Employer Name	7
Investment Account Details or Credentials	7
Bank Account Login Credentials	7
Tax ID Number	6
Insurance Account Details or Credentials	6
Medical Insurance Account Credentials	4
Other Biographical	4
W2 Other Information	4
Prior Home Address	3
Employer Contact Information	3
Merchant Login	2
Education	2
Personal Email Account Credentials	1
Employer Site/System Access Credentials	1
Location	1
Friends/Family	N/A
Financial Account PIN	N/A
Phone Account Credentials	N/A
Utility Account Number	N/A
Social Media Login Credentials	N/A
Utility Account Credentials	N/A
Security Clearance/Access	N/A
Affiliations	N/A
Hometown	N/A
Voter Registration Information/Preference/Etc.	N/A
Work Email Account Credentials	N/A
Web History/Preferences	N/A
Credit Dispute Information	N/A
Non-Debit Payment Account Credentials	N/A

Compromises Involving Sensitive Records

	Compromises	Records Exposed	Percentage
2022	**1,802**	**1,494**	**83%**
2021	**1,862**	**1,557**	**84%**
2020	**1,108**	**882**	**80%**
2019	**1,279**	**1,084**	**85%**
2018	**1,175**	**1,013**	**86%**
2017	**1,506**	**1,385**	**92%**

Compromises by Industry: Q4 2022/2022 YTD vs. Full Years 2021 & 2020

	Q4 2022		2022 YTD		2021		2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	35	695,961	100	1,745,226	125	1,687,192	42	974,054
Financial Services	75	1,628,050	268	27,146,354	279	19,978,108	138	2,687,084
Government	22	717,793	74	1,739,462	66	3,244,455	47	1,100,526
Healthcare	89	9,429,886	344	26,259,933	330	30,853,767	306	9,700,238
Hospitality	13	131,181	34	69,235,147	33	238,445	17	22,365,384
Manufacturing & Utilities	70	341,430	249	23,897,836	222	49,782,583	70	2,896,627
Non-Profit/NGO	20	265,389	71	980,021	86	2,339,646	31	37,528
Professional Services	60	1,304,938	224	6,248,711	184	22,729,391	144	73,012,145
Retail	15	102,870	65	792,195	102	7,212,912	53	10,710,681
Technology	34	229,840,738	86	248,564,988	79	44,684,180	67	142,134,883
Transportation	11	630,817	36	3,991,847	44	569,684	21	1,208,292
Other	68	7,239,325	251	11,541,592	308	79,660,479	172	43,391,302
Unknown	–	–	–	–	4	35,232,664	–	–
Totals	***512***	***252,328,378***	***1,802***	***422,143,312***	***1,862***	***298,213,506***	***1,108***	***310,218,744***

*Unless otherwise noted, all data reported here was entered into the ITRC **notified** database between January 1, 2022, through December 31, 2022.*

Compromises & Victims Up From Q2 – Record High Year Unlikely

Key Takeaways

- Data compromises in the Q3 of 2022 increased by 15 percent (15%) over Q2 but continued to track behind the record pace of 2021.
- The number of victims jumped dramatically in Q3 – a staggering 210 percent (210%) over Q2 2022.
- Supply Chain Attacks made a comeback in Q3 as the number of impacted entities increased 250 percent (250%) from H1 2022.
- Cyberattacks made up 88 percent (88%) of data breaches in Q3 as Phishing Attacks remained the primary attack vector for the 15th consecutive quarter.
- More than 45 percent (45%) of data breach notices related to cyberattacks did not contain information about the attack that could assist other businesses or individuals take actions to prevent or recover from a similar attack.

Summary

- The number of data compromises reported in Q3 2022 increased to 474 from 413 in Q2 and 403 in Q1 for a year-to-date (YTD) total of 1,291.
- More than 105 million victims were impacted by data compromises in Q3 compared to 61 million victims in the first half of the year, representing 55 percent (55%) of the year's total number of victims.
- Cyberattacks (419) remained the primary source of data compromises, followed by System & Human Errors (39), Physical Attacks (11) and Unknown (5).
- More than 1,280 entities were impacted by 48 Supply Chain/Third-Party attacks in Q3 compared to 367 organizations affected by 44 attacks in the first six months of 2022.
- Phishing remains the attack vector of choice, with 124 attacks in Q3, up from 107 in Q2 and 110 in Q1 2022. Ransomware attacks rebounded slightly in the Quarter – 69 attacks in Q3 compared to 55 in Q2 – while Malware-based attacks dropped to the lowest number in 3.75 years – 13 attacks.

Discussion

- With three (3) months left in 2022, the YTD number of publicly-reported data compromises – 1,291 – is only 69 percent (69%) of the year-end total in 2021. Absent a dramatic increase in data compromises in Q4 2022, it is unlikely the total number of data breaches will set a record this year. The total number of data compromises will likely surpass the penultimate record from 2017 of 1,506 compromises.

+ Despite a triple-digit increase in victims during Q3, the number of data compromise victims is likely to show a year-over-year (YoY) decline for the fourth year in a row. However, the number of victims impacted by a compromise can increase significantly with only a handful of breaches. For example, two Q3 breaches – an AT&T-related breach (23 million victims) and one at Neopets (69 million victims) – account for more than half of the year-to-date victim count.
+ The number of cyberattack-related data breach notices where there is no information available about the root cause of an attack continues to grow, along with concerns that this trend will move into 2023. From Q1 2019 through Q3 2021, the ITRC logged only 16 data breach notices where there was no information about the cause of a cyberattack. From Q4 2021 through Q3 2022, the number of notices with no specific attack vector has grown to 617, 37 percent (37%) of all cyberattack-related data breaches reported in the period. Businesses and individuals are at increased risk of a cybercrime when important information is not included in data breach notices.
+ While Physical Attacks and System & Human Errors still exist, Cyberattacks have been the root cause of the vast majority of data compromises for the past 3.75 years. Within that category, Phishing is, by far, the most common attack vector. Despite a decline in ransomware attacks earlier in the year, ransomware has rebounded slightly. Non-Russian affiliated groups have emerged, and cryptocurrency markets were less volatile in the quarter.
+ Malware attacks are increasingly rare as the number of related attacks has dropped steadily from a recent high of 39 attacks in Q2 2021 to 13 in Q3 2022. That compares to 15 data breaches associated with personal information inadvertently being exposed in correspondence in the most recent quarter.

Number of Q3 Compromises

Total Data Compromises: 474 Compromises; 105,780,986 Victims
Data Breaches: 466 Data Breaches; 82,966,797 Victims
Data Exposures: 3 Data Exposures; 2,403 Victims
Data Leaks: N/A
Unknown: 5 Unknown Compromises; 22,811,786 Victims Impacted

Attack Vectors, Q3 2022

Cyberattacks: 419 Breaches; 82,822,161 Victims

+ 124 Phishing/Smishing/BEC
+ 69 Ransomware
+ 13 Malware
+ 8 Credential Stuffing
+ 3 Other
+ 2 Zero Day Attack
+ 1 Non-Secured Cloud Environment
+ 199 Not Specified

System & Human Errors: 39 Breaches/Exposures; 131,724 Victims

+ 15 Correspondence *(Email/Letter)*
+ 7 Misconfigured Firewalls
+ 5 Other
+ 3 Failure to Configure Cloud Security
+ 3 Lost Device or Document
+ 6 Not Specified

Physical Attacks: 11 Breaches; 15,315 Victims

+ 3 Device Theft
+ 2 Document Theft
+ 2 Other
+ 2 Skimming Device
+ 1 Improper Disposal
+ 1 Not Specified

Supply Chain Attacks *(Included in Attack Vectors Above)*

Third-Party/Supply Chain Attack *(49)*: 1,286 Entities; 5,160,413 Victims
Cyberattack: 1,281 Entities; 3,744,905 Victims
System & Human Errors: 5 Entities; 1,415,508 Victims

Noteworthy Supply Chain Attacks *(As of 10/03/2023)*

Professional Finance Company: 618 Entities; 1,918,941 Victims
Illuminate Education: 611 Entities; 2,108,045 Victims*
**Note: The ITRC is entering districts as information is reported. The total number of victims per district has not been disclosed.*
Shields Health Care Group, Inc.: 56 Entities; 1,804,069 Victims
OneTouchPoint, Inc.: 42 Entities; 2,651,396 Victims
Eye Care Leaders: 36 Entities; 3,357,880 Victims
Horizon Actuarial Services, LLC: 3 Entities; 2,292,080 Victims
Nelnet Servicing, LLC: 2 Entities; 2,501,324 Victims

Charts

Compromises & Victims, Year-over-Year

	Compromises	Victims
Q3 2022	1,291	166,782,123
2021	1,862	298,197,505
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
2016	1,088	2,541,092,072

Compromises & Victims, Quarter-to-Quarter

	Compromises	Victims
2022 Q3	474	105,780,986
2022 Q2	413	34,239,785
2022 Q1	404	26,761,352
2021 Q4	566	35,388,356
2021 Q3	445	166,233,442
2021 Q2	497	55,321,228
2021 Q1	354	41,254,479
2020 Q4	326	16,683,032
2020 Q3	248	60,952,924
2020 Q2	295	100,918,230
2020 Q1	239	131,664,558

Compromises with Reported Victims Impacted Quarter-to-Quarter

	Compromises	Compromises With Reported Victims	Percentage
2022 Q3	474	264	56%
2022 Q2	413	246	60%
2022 Q1	404	264	65%
2021 Q4	566	288	51%
2021 Q3	445	292	66%
2021 Q2	497	299	60%

Attack Vector: Q3 2022/2022 YTD vs. Full Years 2021 & 2020

	Q3 2022	2022 YTD	2021	2020
Cyberattacks	***419***	***1,154***	***1,613***	***878***
Phishing/Smishing/BEC	124	343	537	383
Ransomware	69	194	351	158
Malware	13	60	141	104
Non-Secured Cloud Environment	1	6	24	50
Credential Stuffing	8	14	14	17
Unpatched Software Flaw	–	–	4	3
Zero Attack Day	2	3	4	1
Other	3	19	428	162
Not Specified	199	515	110	–
System & Human Errors	***39***	***100***	***179***	***152***
Failure to Configure Cloud Security	3	13	54	57
Correspondence (Email/Letter)	15	36	66	55
Misconfigured Firewall	7	22	13	4
Lost Device or Document	3	4	12	5
Other	5	11	34	31
Not Specified	6	14	–	–
Physical Attacks	***11***	***27***	***51***	***78***
Document Theft	2	5	9	15
Device Theft	3	12	17	30
Improper Disposal	1	4	5	11
Skimming Device	2	3	1	5
Other	2	2	19	17
Not Specified	1	1	–	–
Unknown	***5***	***10***	***12***	***N/A***

Compromises by Industry: Q3 2022/2022 YTD *(H1)* vs. Full Years 2021 & 2020

	Q3 2022		2022 YTD		2021		2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	24	483,412	65	888,905	125	1,687,192	42	974,054
Financial Services	67	3,115,672	194	25,498,818	279	19,978,108	138	2,687,084
Government	19	82,510	52	893,039	66	3,244,455	47	1,100,526
Healthcare	94	2,163,551	255	14,605,207	330	30,853,767	306	9,700,238
Hospitality	10	69,026,205	21	69,103,966	33	238,445	17	22,365,384
Manufacturing & Utilities	64	23,018,654	179	23,506,593	222	49,782,583	70	2,896,627
Non-Profit/NGO	16	40,875	51	711,574	86	2,339,646	31	37,528
Professional Services	68	1,558,274	163	4,904,796	184	22,729,391	144	73,012,145
Retail	20	288,774	50	614,219	102	7,212,912	53	10,710,681
Technology	21	2,816,199	52	18,403,626	79	44,684,180	67	142,134,883
Transportation	6	2,516,097	25	3,361,030	44	569,684	21	1,208,292
Other	65	670,763	184	4,290,350	308	79,644,478	172	43,391,302
Unknown	–	–	–	–	4	35,232,664	–	–
Totals	***474***	***105,780,986***	***1,219***	***166,782,123***	***1,862***	***298,197,505***	***1,108***	***310,218,744***

*Unless otherwise noted, all data reported here was entered into the ITRC **notified** database between July 1, 2022, through September 30, 2022.*

Victim Rates Decline as Compromises Target Businesses

Key Takeaways

- Data compromises are up slightly – two percent (2%) in the second quarter (Q2) of 2022 compared to the first quarter (Q1) of 2022. However, the overall pace of data compromises for the first half (H1) of 2022 is down four percent (4%) compared to the same period in 2021. The total number of data compromises reported in 2021 – 1,862 – was a record high.
- The number of people reportedly impacted by data compromises continued to drop in H1 2022 as the nature of data compromises shifted to attacks targeting businesses, government agencies, and institutions. However, an average of 39 percent (39%) of all data breach notices issued in H1 2022 do not list a victim count.
- Approximately 40 percent (40%) of data breach notices issued in H1 2022 do not include the root cause of the compromise, making "unknown" the top cause of data breaches so far this year for the first time since the Identity Theft Resource Center (ITRC) began tracking the causes of data compromises.
- Cyberattacks continued to be the primary attack vector leading to a data compromise in H1 2022. Ransomware attacks linked to breaches dropped 20 percent (20%) in Q2 2022 from the previous quarter – the first quarter-over-quarter (QoQ) drop since the ITRC began tracking ransomware in 2018.

Summary

- After a record-high number of publicly reported data breaches in 2021 – 1,862 – there have been fewer data compromises so far in 2022 than at the same point in 2021: 817 vs. 851.
- The number of victims in H1 2022 was down approximately 45 percent (45%) from H1 2021 as at least 53.3 million people were reported as being impacted by a data compromise.
- An estimated 87 percent (87%) of the data compromises in H1 2022 were due to a cyberattack. However, ransomware attacks declined QoQ for the first time since ransomware surpassed malware as the number two primary cause of data breaches in 2019.
- Phishing remained the number one root cause of data compromises in H1 2022.
- Supply chain attacks, a subset of cyberattacks, continue to be a favored attack vector for cyberattackers.
- For the first time in H1 2022, approximately four (4) in ten (10) data breach notices did not list a root cause of the compromise. Forty percent (40%) of entities issuing breach notices did not reveal the number of victims impacted.

Discussion

+ After a record-breaking 2021, the number of publicly reported data compromises is down in the first half of 2022 compared to the previous point in 2021. So is the number of publicly identified victims.
+ Also, down so far in 2022 are the number of data breaches linked to ransomware attacks. Security researchers speculate that the sudden decline in ransomware attacks is due to a combination of factors, including the ongoing conflict in Ukraine and the collapse of cryptocurrencies favored by cybercriminals.
+ All of these trends – fewer compromises, fewer victims, few ransomware attacks – can be reversed quickly with just a handful of large breaches or a series of smaller ones.
+ The declines could also be an illusion, masked by the 40 percent (40%) of data breach notices that do not include basic information, such as attack vector and/or a victim count. This is a new trend that requires further observation and study.

Number of Q2 Compromises

Total Data Compromises: 413 Compromises; 27,946,766 Victims
Data Breaches: 404 Data Breaches; 27,902,868 Victims
Data Exposures: 6 Data Exposures; 42,420 Victims
Data Leaks: N/A
Unknown: 3 Unknown Compromises; 1,478 Victims Impacted

Number of H1 Compromises

Total Data Compromises: 817 Compromises; 53,350,425 Victims
Data Breaches: 802 Data Breaches; 46,209,107 Victims
Data Exposures: 10 Data Exposures; 7,136,948 Victims
Data Leaks: N/A
Unknown: 5 Unknown Compromises; 4,370 Victims Impacted

Attack Vectors, Q2 2022

Cyberattacks: 367 Breaches; 17,735,760 Victims

+ 107 Phishing/Smishing/BEC
+ 55 Ransomware
+ 22 Malware
+ 8 Other
+ 4 Credential Stuffing
+ 2 Non-Secured Cloud Environment
+ 169 Not Specified

System & Human Errors: 30 Breaches/Exposures; 10,094,133 Victims

+ 10 Misconfigured Firewalls
+ 9 Correspondence *(Email/Letter)*
+ 6 Failure to Configure Cloud Security
+ 3 Other
+ 2 Not Specified

Physical Attacks: 13 Breaches; 115,395 Victims

+ 8 Device Theft
+ 2 Improper Disposal
+ 2 Document Theft
+ 1 Skimming Device

Supply Chain Attacks *(Included in Attack Vectors Above)*

Third-Party/Supply Chain Attack *(23)*: 293 Entities; 2,975,387 Victims
Cyberattack: 292 Entities; 2,975,387 Victims
System & Human Errors: 1 Entities; Unknown Victims

Attack Vectors, H1 2022

Cyberattacks: 734 Breaches; 35,891,170 Victims

+ 219 Phishing/Smishing/BEC
+ 124 Ransomware
+ 46 Malware
+ 17 Other
+ 6 Credential Stuffing
+ 5 Non-Secured Cloud Environment
+ 317 Not Specified

System & Human Errors: 62 Breaches/Exposures; 17,317,889 Victims

+ 21 Correspondence *(Email/Letter)*
+ 15 Misconfigured Firewalls
+ 10 Failure to Configure Cloud Security
+ 6 Other
+ 1 Lost Device or Document
+ 2 Not Specified

Physical Attacks: 16 Breaches; 136,996 Victims

+ 9 Device Theft
+ 3 Improper Disposal
+ 3 Document Theft
+ 1 Skimming Device

Supply Chain Attacks *(Included in Attack Vectors Above)*

Third-Party/Supply Chain Attack *(44)*: 367 Entities; 4,138,125 Victims
Cyberattack: 364 Entities; 4,136,825 Victims
System & Human Errors: 3 Entities; 1,300 Victims

Noteworthy Supply Chain Attacks *(As of 07/03/2023)*

Illuminate Education: 234 Entities; 201,586 Victims*
**Note: Roughly 600+ school districts are known to have been impacted. The ITRC is continuing to monitor and enter districts as information is being reported. The total number of victims per district has not been reported.*

Coix Health: 34 Entities; 12,493 Victims

Eye Care Leaders: 39 Entities; 2,237,515 Victims

MCG Health, LLC: 6 Entities, 793,283 Victims

Horizontal Actuarial Services, LLC: 3 Entities; 2,292,080 Victims**
***Note: Exposure number updated per total number of victims impacted as reported to the Maine AG by Horizon Actuarial.*

Charts

Compromises & Victims, Year-over-Year

	Compromises	Victims
H1 2022	817	53,350,425
2021	1,862	298,078,081
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
2016	1,088	2,541,092,072

Compromises & Victims, Quarter-to-Quarter

	Compromises	Victims
2022 Q2	413	27,946,766
2022 Q1	404	25,403,659
2021 Q4	566	35,376,838
2021 Q3	445	166,125,536
2021 Q2	497	55,321,228
2021 Q1	354	41,254,479
2020 Q4	326	16,683,032
2020 Q3	248	60,952,924
2020 Q2	295	100,918,230
2020 Q1	239	131,664,558

Compromises with Reported Victims Impacted Quarter-to-Quarter

	Compromises	Compromises With Reported Victims	Percentage
2022 Q2	413	235	58%
2022 Q1	404	263	65%
2021 Q4	566	288	51%
2021 Q3	445	292	66%
2021 Q2	497	299	60%

Attack Vector: 2022 YTD *(H1)* vs. Full Years 2021 & 2020

	2022 YTD	2021	2020
Cyberattacks	**734**	**1,613**	**878**
Phishing/Smishing/BEC	219	537	383
Ransomware	124	351	158
Malware	46	141	104
Non-Secured Cloud Environment	5	24	50
Credential Stuffing	6	14	17
Unpatched Software Flaw	–	4	3
Zero Attack Day	–	4	1
Other	17	428	162
Not Specified	317	110	–
System & Human Errors	**62**	**179**	**152**
Failure to Configure Cloud Security	10	54	57
Correspondence (Email/Letter)	21	66	55
Misconfigured Firewall	15	13	4
Lost Device or Document	1	12	5
Other	6	34	31
Not Specified	9	–	–
Physical Attacks	**16**	**51**	**78**
Document Theft	3	9	15
Device Theft	9	17	30
Improper Disposal	3	5	11
Skimming Device	1	1	5
Other	–	19	17
Not Specified	–	–	–
Unknown	**5**	**12**	**N/A**
Totals	**817**	**1,855**	**1,108**

Compromises by Industry: 2022 YTD *(H1)* vs. Full Years 2021 & 2020

	2022 YTD		2021		2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	41	405,493	125	1,687,192	42	974,054
Financial Services	127	22,309,482	279	19,973,772	138	2,687,084
Government	33	810,529	66	3,244,455	47	1,100,526
Healthcare	161	11,830,303	330	30,853,767	306	9,700,238
Hospitality	11	76,820	33	238,445	17	22,365,384
Manufacturing & Utilities	115	467,664	222	49,782,583	70	2,896,627
Non-Profit/NGO	34	590,207	86	2,339,646	31	37,528
Professional Services	95	2,053,827	184	22,726,901	144	73,012,145
Retail	30	325,445	102	7,212,912	53	10,710,681
Technology	31	12,394,573	79	44,679,488	67	142,134,883
Transportation	19	328,317	44	569,684	21	1,208,292
Other	120	1,757,785	308	79,536,572	172	43,391,302
Unknown	–	–	4	35,232,664	–	–
Totals	***817***	***20,773,963***	***1,862***	***298,078,081***	***1,108***	***310,218,744***

*Unless otherwise noted, all data reported here was entered into the ITRC **notified** database between April 1, 2022, through June 30, 2022 (Q2) and January 1, 2022 through June 30, 2022 (H1).*

Data Compromises Off to Fast Start; Victim Rates Continue to Drop

Summary

- Publicly reported data compromises totaled 404 through March 31, 2022, a 14 percent (14%) increase compared to Q1 2021.
- This is the third consecutive year when the number of total data compromises increased compared to Q1 of the previous year. It also represents the highest number of Q1 data compromises since 2020.
- The number of individual victims, though, dropped in Q1 2022. The 20.7 million victims in this reporting period is approximately a 50 percent (50%) decrease compared to Q1 2021 and a 41 percent (41%) drop from Q4 2021.
- Approximately 92 percent (92%) of the data breaches in the first three months of 2022 were the result of cyberattacks.
- Phishing and Ransomware remain the number one and number two root causes of data compromises; however, a majority of data breach notices in Q1 2022 did not list a root cause of the breach.
- System & Human Errors represent roughly eight percent (8%) of the Q1 2022 data compromises.
- Data breaches resulting from physical attacks such as document or device theft and skimming devices dropped to single digits (3) in Q1 2022.

Discussion

- After a record-breaking year for data compromises in 2021 (1,862), Q1 of 2022 begins with the highest number of data compromises in the past three (3) years. Traditionally, Q1 is the lowest number of data breaches reported each year.
- Cyberattacks that lead to data compromises continue to increase, representing about 92 percent (92%) of all data compromises. Phishing and related attack vectors, ransomware, and malware remain the top three root causes of cyberattack-related data breaches.
- However, continuing a trend that emerged in 2021, 154 out of 367 data breach notices did not include the cause of the breach. That makes "unknown" the single largest attack vector in Q1. That also represents a 40 percent (40%) increase of the total number of unknown breach causes for full-year 2021.
- While subsequent breach notice updates may include more attack information, the increasing lack of transparency in breach notices represents a risk to organizations as well as individual consumers.
- The only non-cyberattack-related attack vector in double digits during Q1 was related to email or letter correspondence with 12 instances.
- Healthcare, Financial Services, Manufacturing & Utilities, and Professional Services sectors had the most compromises in Q1 2022.

Number of Q1 Compromises

Total Data Compromises: 404 Compromises; 20,773,963 Victims
- **Data Breaches:** 398 Data Breaches; 13,676,543 Victims
- **Data Exposures:** 4 Data Exposures; 7,094,528 Victims
- **Data Leaks:** N/A
- **Unknown:** 2 Unknown Compromises; 2,892 Victims Impacted

Attack Vectors, Q1 2022

Cyberattacks: 367 Breaches; 13,525,762 Victims
- + 110 Phishing/Smishing/BEC
- + 67 Ransomware
- + 22 Malware
- + 9 Other
- + 3 Non-Secured Cloud Environment
- + 2 Credential Stuffing
- + 154 Not Specified

System & Human Errors: 32 Breaches/Exposures; 7,223,708 Victims
- + 12 Correspondence *(Email/Letter)*
- + 5 Misconfigured Firewalls
- + 4 Failure to Configure Cloud Security
- + 3 Other
- + 1 Lost Device or Document
- + 7 Not Specified

Physical Attacks: 3 Breaches; 21,601 Victims
- + 1 Document Theft
- + 1 Device Theft
- + 1 Improper Disposal

Charts

Compromises & Victims, Year-over-Year

	Compromises	Victims
Q1 2022	404	20,773,963
2021	1,862	295,429,724
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
2016	1,088	2,541,092,072

Compromises & Victims, Quarter-to-Quarter

	Compromises	Victims
2022 Q1	404	20,773,963
2021 Q4	566	35,311,922
2021 Q3	445	163,542,095
2021 Q2	497	55,321,228
2021 Q1	354	41,254,479
2020 Q4	326	16,683,032
2020 Q3	248	60,952,924
2020 Q2	295	100,918,230
2020 Q1	239	131,664,558

Attack Vector: 2022 YTD *(Q1)* vs. Full Years 2021 & 2020

	2022 YTD	2021	2020
Cyberattacks	***367***	***1,613***	***878***
Phishing/Smishing/BEC	100	537	383
Ransomware	67	351	158
Malware	22	141	104
Non-Secured Cloud Environment	3	24	50
Credential Stuffing	2	14	17
Unpatched Software Flaw	–	4	3
Zero Attack Day	–	4	1
Other	9	428	162
Not Specified	154	110	–
System & Human Errors	***32***	***179***	***152***
Failure to Configure Cloud Security	4	54	57
Correspondence (Email/Letter)	12	66	55
Misconfigured Firewall	5	13	4
Lost Device or Document	1	12	5
Other	3	34	31
Not Specified	7	–	–
Physical Attacks	***3***	***51***	***78***
Document Theft	1	9	15
Device Theft	1	17	30
Improper Disposal	1	5	11
Skimming Device	–	1	5
Other	–	19	17
Not Specified	–	–	–
Unknown	***2***	***12***	***N/A***
Totals	***404***	***1,855***	***1,108***

Compromises by Industry: 2022 YTD *(Q1)* vs. Full Years 2021 & 2020

	2022 YTD		2021		2020	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	21	106,099	125	1,681,483	42	974,054
Financial Services	68	3,384,769	279	19,973,772	138	2,687,084
Government	13	294,027	66	3,244,455	47	1,100,526
Healthcare	73	2,560,465	330	28,216,273	306	9,700,238
Hospitality	6	56,451	33	238,445	17	22,365,384
Manufacturing & Utilities	52	247,852	222	49,777,158	70	2,896,627
Non-Profit/NGO	18	558,362	86	2,339,646	31	37,528
Professional Services	46	1,719,850	184	22,725,185	144	73,012,145
Retail	18	272,950	102	7,212,912	53	10,710,681
Technology	16	10,832,588	79	44,679,488	67	142,134,883
Transportation	8	20,930	44	569,574	21	1,208,292
Other	65	719,620	308	79,538,669	172	43,391,302
Unknown	–	–	4	35,232,664	–	–
Totals	***404***	***20,773,963***	***1,862***	***295,429,724***	***1,108***	***310,218,744***

*Unless otherwise noted, all data reported here was entered into the ITRC **notified** database between January 1, 2022, through March 31, 2022.*

Glossary of Terms

For purposes of this report, the ITRC uses standard industry terms as defined by the National Institute of Standards & Technology (NIST) as well as specific definitions develop by the ITRC.

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

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

Data Exposure – When personal information is available for access and/or removal from 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).

About Data Collection, Data Compromises & Breach Notices

The ITRC gathers information about publicly reported data compromises, including data breaches, from a variety of sources including company announcements, mainstream news media, government agencies, recognized security research firms and researchers, and non-profit organizations. The ITRC accepts these reports "as is" and makes no warranty as to their accuracy or completeness.

The statistics reported here should be considered within the following context:

- Victim counts are incomplete. Because there is no universal legal requirement to disclose the number of individuals who are impacted by a data compromise, the number of victims should be considered a minimum estimate. Likewise, there is no central repository of data breach victims which means it is impossible to determine the number of individuals who are victims of multiple breaches per year. Based on the U.S. adult population of 259 million individuals 18 years or older, it is reasonable to conclude any given individual is likely the victim of multiple breaches.
- The total number of compromises, including breaches, should be considered a minimum. While the ITRC endeavors to find and report publicly reported data breaches, it is reasonable to conclude that not all breaches are publicly reported, and not all publicly reported data breaches are found by the ITRC. Certain state data breach laws allow for alternate methods of notification including posting on company websites and news releases that may not generate news coverage, making it difficult to discover the data breaches that are the subject of the notices issued under alternate methods.

It is common for the number of individuals impacted by a compromise to change over time. Initial reports are often based on incomplete or inaccurate information resulting in the number of impacted individuals, the root cause of the data breach, and the cost of the data breach to the breached company among other factors to require occasional updates.

Different states have different reporting requirements. This often results in a lag between the time a government official is notified of a data breach and when the breach is officially reported. There are also variations in how data breaches are defined and what data is governed under a given state's laws, resulting in data being subject to a breach notice in some states, but not in all.

The organization impacted by a data breach generally has the responsibility to determine if a breach notice is required based on the risk to individuals from the exposure of personal information. If the business determines there is no risk as defined by applicable law or regulation, the organization may opt not to issue a breach notice.

There are a number of for-profit and non-profit organizations that publish data breach information, but each organization captures and views the information differently. There are four key differences in how the ITRC reports data breach information:

- The ITRC tracks three distinct categories of data compromise. See our ***Glossary of Terms*** to learn more.
- The ITRC only publishes data related to publicly reported U.S. compromises.

- The ITRC focuses on the number of individuals impacted, not the number of records exposed in keeping with our mission of a victim assistance organization.
- We do not report data breaches where the information is not protected under a state's data breach notice law. For example, business records or intellectual property are generally excluded from state data breach laws.

A Special Word about Data Compromises in the Military Sector

In 2022, the *Government Accountability Office* released a report indicating that the United States Department of Defense (DoD) and branches of the armed services had experiences data breaches involving the personal information of an undetermined number of service members and civilian contractors. The same report concluded the DoD did not have an adequate system to quantify the number of breaches, the number of individuals impacted, and to track the number of people who were notified of a breach and by whom.

In 2020, 2021, and 2022, the ITRC did not receive any notices of data breaches impacting military personal. Given the recent GAO report and the conclusion that there is no functional breach notification system within the DoD, the ITRC will no longer report data breaches linked to the U.S. military sector.