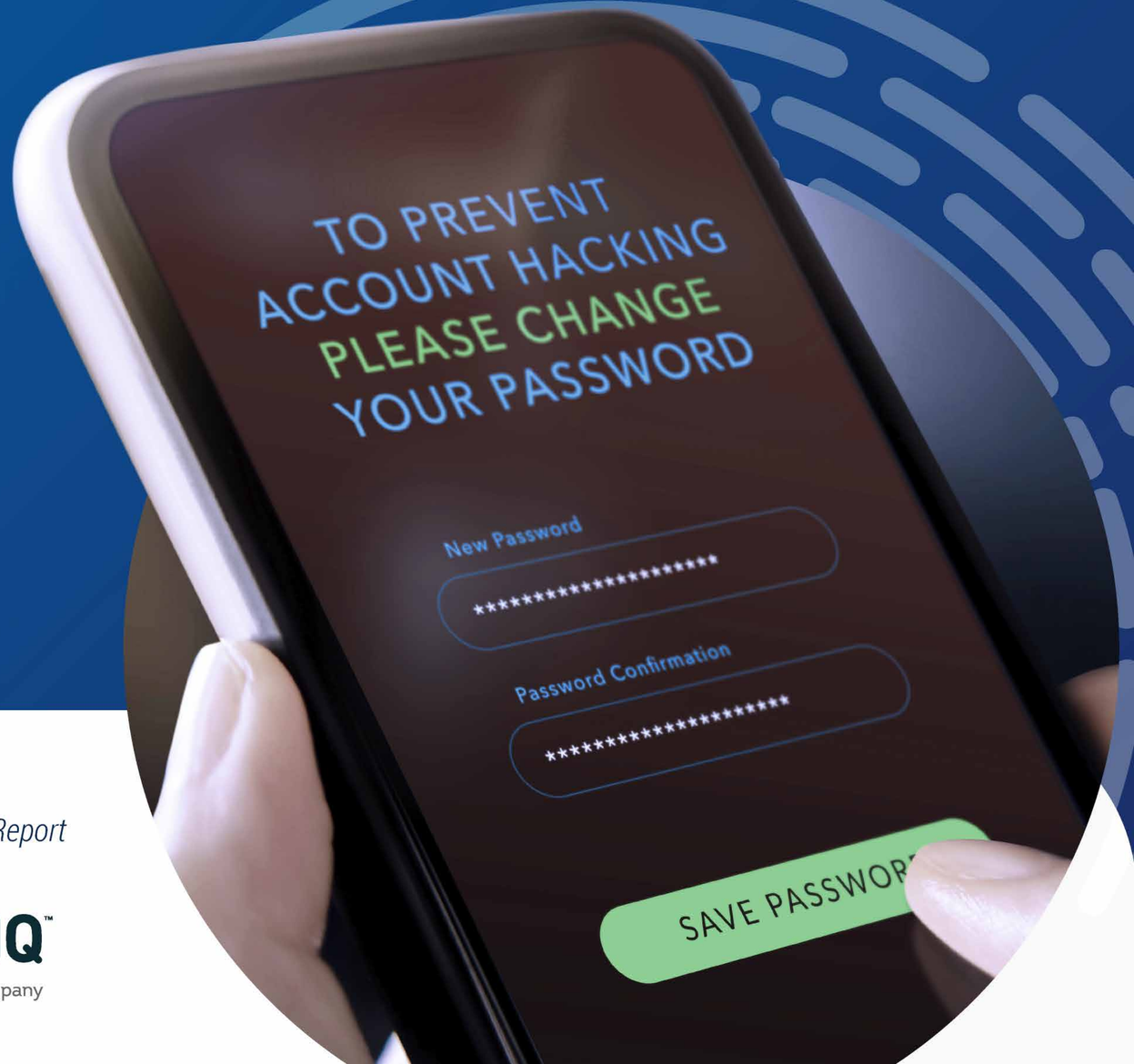
RELEASED: 01.2022

2021 in review

Data Breach

ANNUAL REPORT

Identity Compromises:
From the Era of Identity Theft to the Age of Identity Fraud



ITRC | IDENTITY THEFT RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

The 2021 Data Breach Report is supported by:

SONTIQ™
A TransUnion® Company

Table of Contents

Letter from the CEO

Eva C. Velasquez

(President & CEO, ITRC)

January 2022

In 2021, there were **more data compromises reported** in the United States of America **than in any year** since the first state data breach notice law became effective in 2003.

There are a number of watershed moments in the history of cybercrime. The first cyberattack was in 1834 when criminals intercepted bond trading information sent by a mechanical telegraph system in France. The modern era of cyberattacks began in 1957 when a blind, seven-year-old child discovered they could whistle a tone that would allow them to make long-distance telephone calls for free.

We may very well look back at 2021 as the milestone year when we officially moved from the era of identity theft to an era of identity fraud. That is to say, the time when cybercriminals shifted from mass data accumulation (identity theft) to mass data misuse (identity fraud). Fueling most identity fraud-related crimes was consumer information stolen from businesses in data breaches.

Individuals were often caught in the crossfire between professional cybergangs and organizations that hold consumer information in trust. The personal information of consumers remained valuable to cybercriminals, but individuals were not the primary target for most identity crimes committed in 2021. Instead, consumer information was often the means to the end of attacking businesses through stolen credentials – logins and pass-

words – or social engineering where savvy cybercriminals tricked people into revealing information needed to launch an attack.

To be sure, consumers are still at risk and there are still cybercriminals looking to separate trusting people from their resources. But the vast majority of data compromises that occur today represent highly sophisticated, highly complex cyberattacks that require aggressive defenses to prevent. If those defenses fail, we too often see a level of transparency that is inadequate for consumers to protect themselves from identity fraud.

To help ensure more consumers learn when their personal information is at risk due to a data compromise, we are launching a new, free data breach alert service later in Q1 2022. We hope giving consumers more timely information and more relevant advice will help reverse a trend we recently identified in new research:

> **Less than 5 percent** take the most effective protective action after receiving a data breach notice.

In our modern, digital-driven world, it is impossible to separate data, privacy, and identity protection. Yet, our current **legal, regulatory, and policy frameworks** at the state and federal levels of government do not adequately address the growing and evolving threats that data breaches represent to individuals, organizations, and society as a whole.

It is not the ITRC's purpose or place to name and shame organizations that have experienced a data compromise, but we do advocate for solutions to these issues. It is also our mission to inform public policy makers of the risks and benefits of addressing or ignoring the rise in identity crimes. It is also our job to point out that the needs of identity crime victims are at risk of being lost in the discussions of how to reduce cyber threats. And, it is our duty to share our knowledge so that individuals, organizations, and institutions can make informed decisions about how to protect themselves and those in their care from the criminals who would misuse our personal information.

This report reflects our mission and the current state of identity risks. In the pages that follow, the data will speak for itself. I hope that you will find it both informative and motivational to help us find more ways to prevent identity crimes and support identity crime victims.

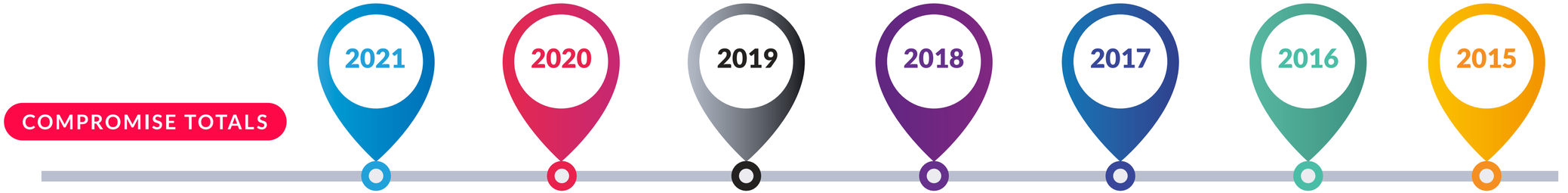
Finally, please join me in thanking ***Sontiq***, a TransUnion Company, for their support of this Report. Without the generous support of partners like Sontiq and our other **public, private, and government partners**, we would not be able to provide the research and analysis of important trends, identity education programs, or identity crime victim assistance.

Executive Summary

The overall number of data compromises (1,862) is up **68 percent** over 2020; the new record number of data compromises is **23 percent** over the previous all-time high (1,506).

+ The number of data events that involved sensitive information such as SSNs increased slightly YoY as a percent of the overall number of compromises (83 percent vs. 80 percent), but remained well below the previous all-time high of 95 percent set in 2017.
+ Ransomware-related data breaches have doubled in each of the past two years. At the current growth rate, ransomware attacks will pass Phishing as the number one root cause of data compromises in 2022.
+ The number of data breach notices that do not reveal the root cause of a compromise (607) has grown by more than 190 percent since 2020.
+ The number of supply chain attacks, where a single organization is attacked to obtain the data of multiple entities, is obscured by the root cause these compromises (e.g. phishing, ransomware, malware, etc.). In 2021, supply chain attacks would be classified as the fourth most common attack vector if a stand-alone cause.
+ There were more cyberattack–related data compromises (1,613) in 2021 than all data compromises in 2020 (1,108).
+ Compromises increased year-over-year in every primary sector but one - Military where there were no data breaches publicly disclosed. The Manufacturing & Utilities sector saw the largest percentage increase in data compromises at 217 percent over 2020.
+ As identity criminals focus more on specific data types rather than mass data acquisition, the number of victims continues to drift downward - ~5% in 2021 compared to the previous year. The number of consumers whose data is compromised multiple times per year, though, remains excessively high.

Compromise Trends 2015 to 2021



	2021	2020	2019	2018	2017	2016	2015
Number of Compromises	1,862	1,108	1,279	1,175	1,506	1,099	785
Number of Victims	293,927,708	310,116,907	883,558,186	2,227,849,622	1,825,413,935	2,541,070,438	318,276,407

ATTACK VECTOR TRENDS

	2021	2020	2019
Cyberattacks	**1,613**	**878**	**928**
Phishing/Smishing/BEC	537	383	490
Ransomware	321	158	83
Malware	139	104	112
Non-secured Cloud Environment	23	51	15
Credential Stuffing	14	17	3
Unpatched software flaw	4	3	3
Zero Day Attack	4	1	n/a
Other - not specified	436	161	222
NA	106	n/a	n/a
Human & System Errors	**179**	**152**	**231**
Failure to configure cloud security	54	57	56
Correspondence (email/letter)	66	55	89
Misconfigured firewall	13	4	4
Lost device or document	12	5	19
Other - not specified	34	31	63
Physical Attacks	**51**	**78**	**118**
Document Theft	9	15	19
Device Theft	17	30	57
Improper Disposal	5	11	14
Skimming Device	1	5	4
Other - not specified	19	17	24
Unknown	**12**	**n/a**	**2**

SECTOR TRENDS

	2021		2020		2019	
	Compromises	Victims	Compromises	Victims	Compromises	Victims
Education	125	1,680,300	42	978,254	71	5,161,005
Financial Services	279	19,745,846	138	2,687,084	172	103,939,736
Government	66	3,244,455	47	1,100,526	64	1,193,791
Healthcare	330	28,045,658	306	9,700,238	398	9,080,498
Hospitality	33	217,941	17	22,365,384	40	1,459,393
Manufacturing & Utilities	222	49,775,124	70	2,896,627	103	70,265,156
Military	--	--	--	--	1	1,243
Non-Profit/NGO	86	2,309,008	31	37,528	36	248,824
Professional Services	184	22,697,765	144	73,012,132	84	1,694,188
Retail	102	7,186,143	53	10,710,681	86	370,128,202
Technology	79	44,035,156	67	142,028,859	62	107,923,851
Transportation	44	534,280	21	1,208,292	15	211,335
Other	308	79,223,368	172	43,391,302	147	212,250,964
Unknown	4	35,232,664	--	--	--	--

Number of Compromises in 2021

1,862 compromises

293,927,708 victims

1,789
Data Breaches

189,532,878 victims

54
Data Exposures

104,392,275 victims

6,993,145,763
total records exposed

7
Data Leaks

1,823,449,287 victims*

11,659,060,239
total records exposed

*Includes non-U.S victims

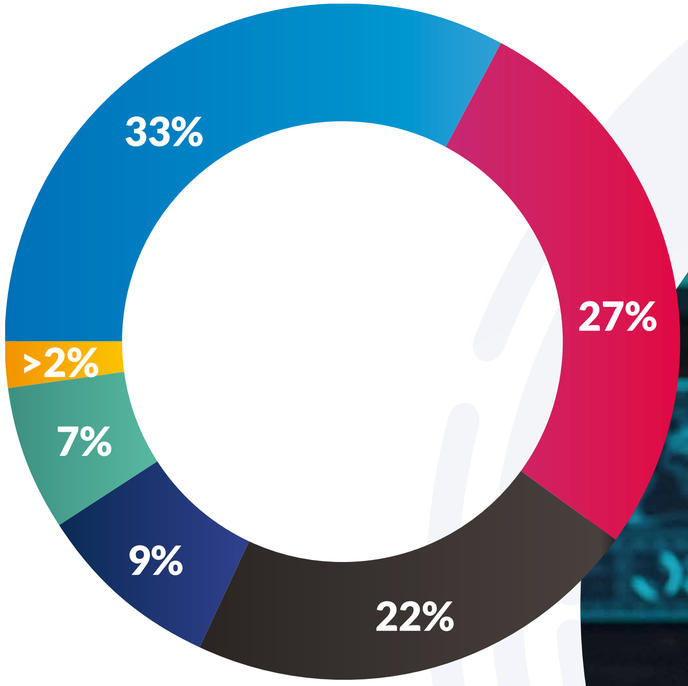
12
Unknown Compromises

2,555 individuals impacted

Root Cause of Compromises

Cyberattacks

Cause	Qty	%
Phishing/Smishing/BEC	**537**	33%
Ransomware	**350**	22%
Malware	**139**	9%
Non-secured Cloud Environment	**23**	1%
Credential Stuffing	**14**	1%
Unpatched software flaw (CVE)	**4**	0.2%
Zero Day Attack	**4**	0.2%
Other – not specified	**436**	27%
NA	**106**	7%

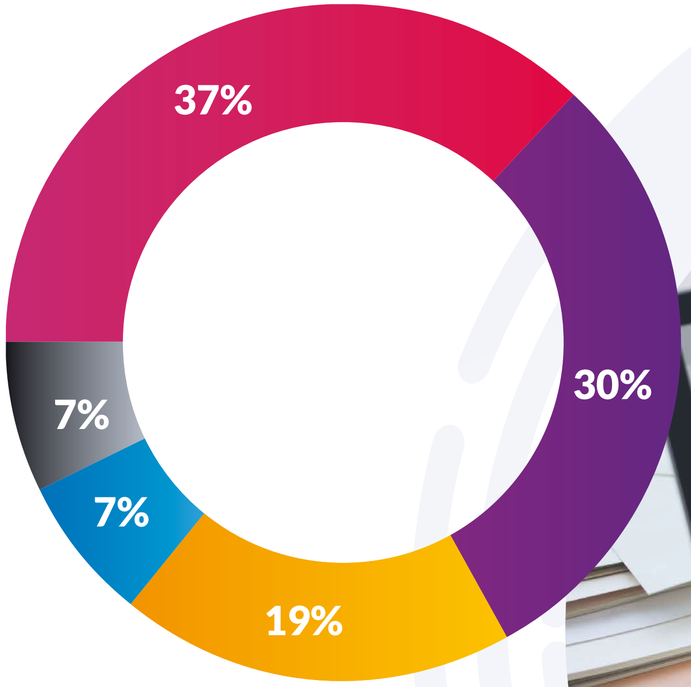


1,613 breaches/exposures

188,900,415 victims

Human & System Errors

Cause	Qty	%
Correspondence (email/letter)	**66**	37%
Failure to configure cloud security	**54**	30%
Misconfigured firewall	**13**	7%
Lost device or document	**12**	7%
Other - not specified	**34**	19%

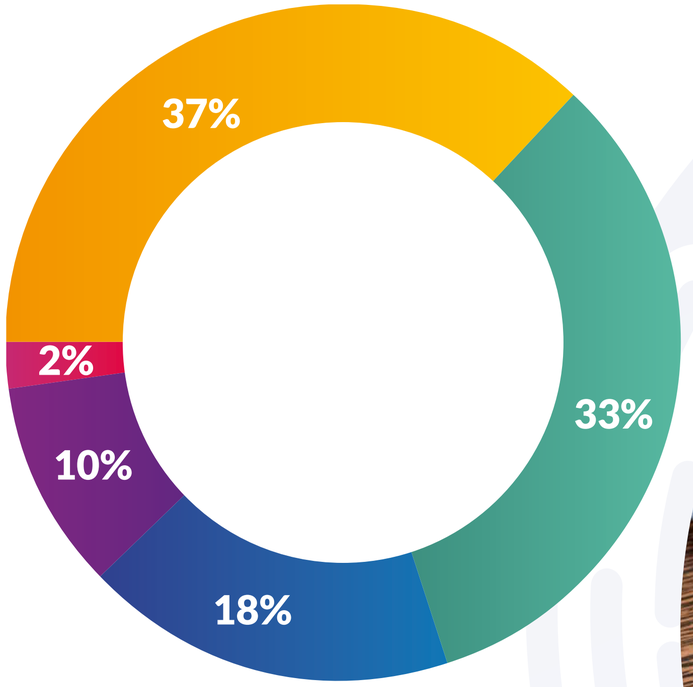


179 breaches/exposures

104,891,759 victims

Physical Attacks

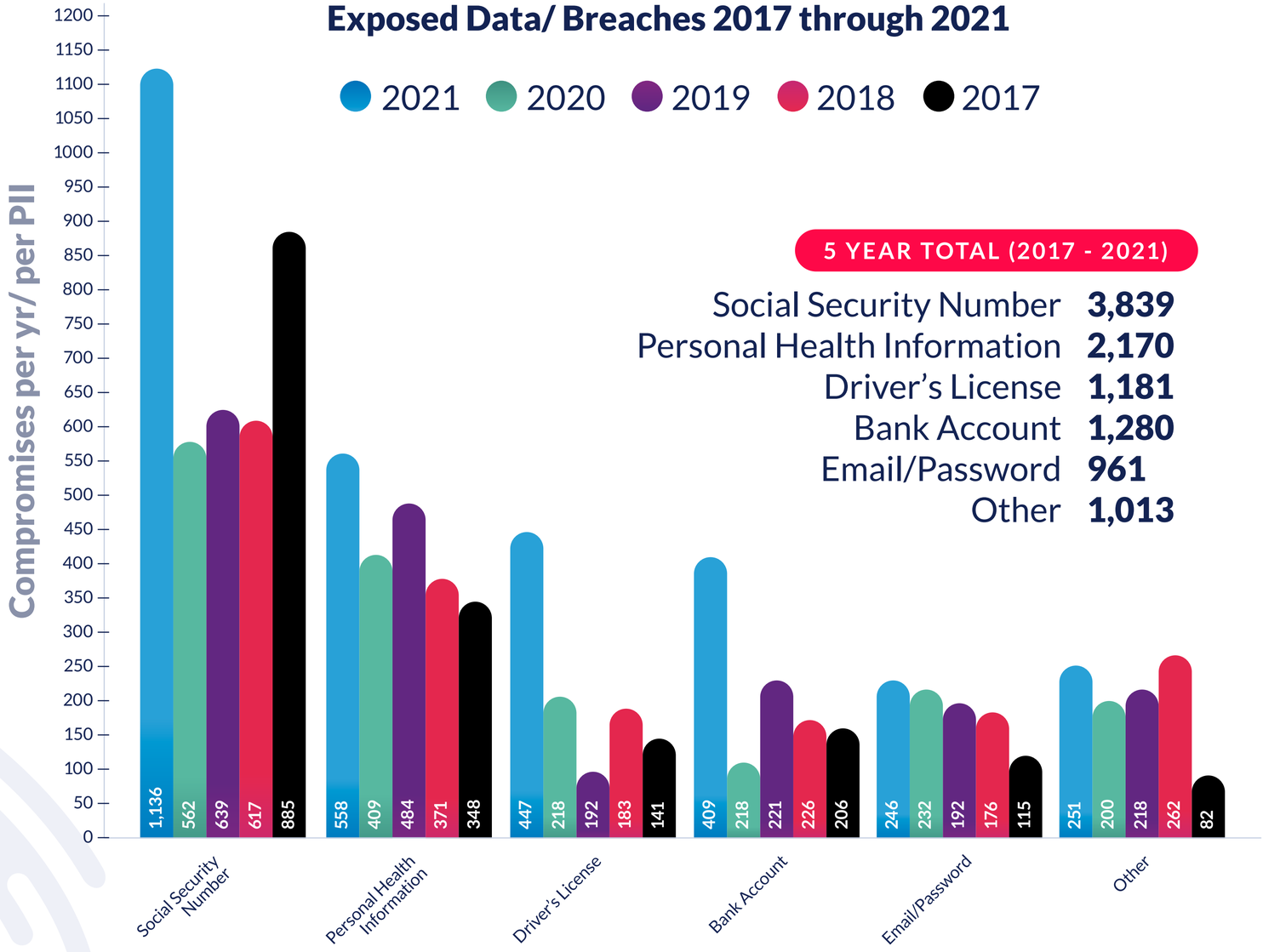
Cause	Qty	%
Device Theft	**17**	33%
Document Theft	**9**	18%
Improper Disposal	**5**	10%
Skimming Device	**1**	2%
Other - not specified	**19**	37%



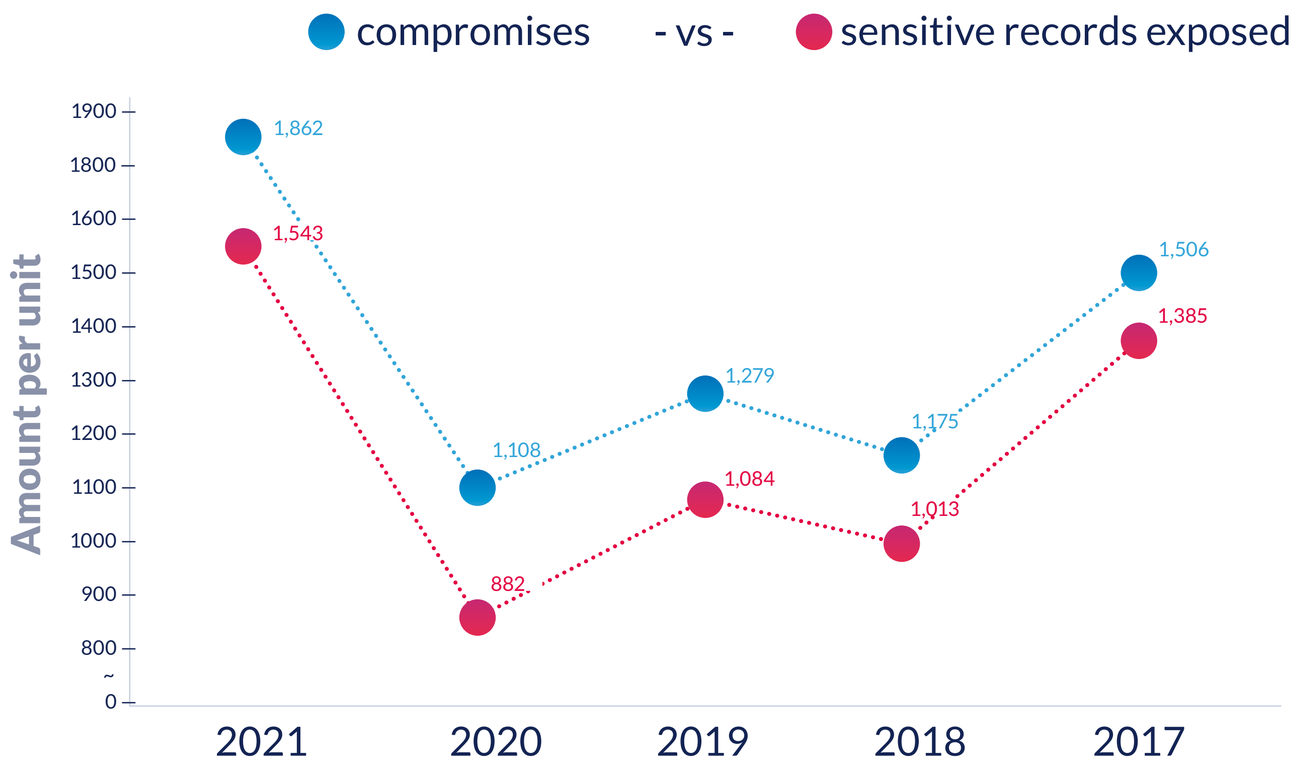
51 breaches/exposures

132,979 victims

Types of Data Compromised



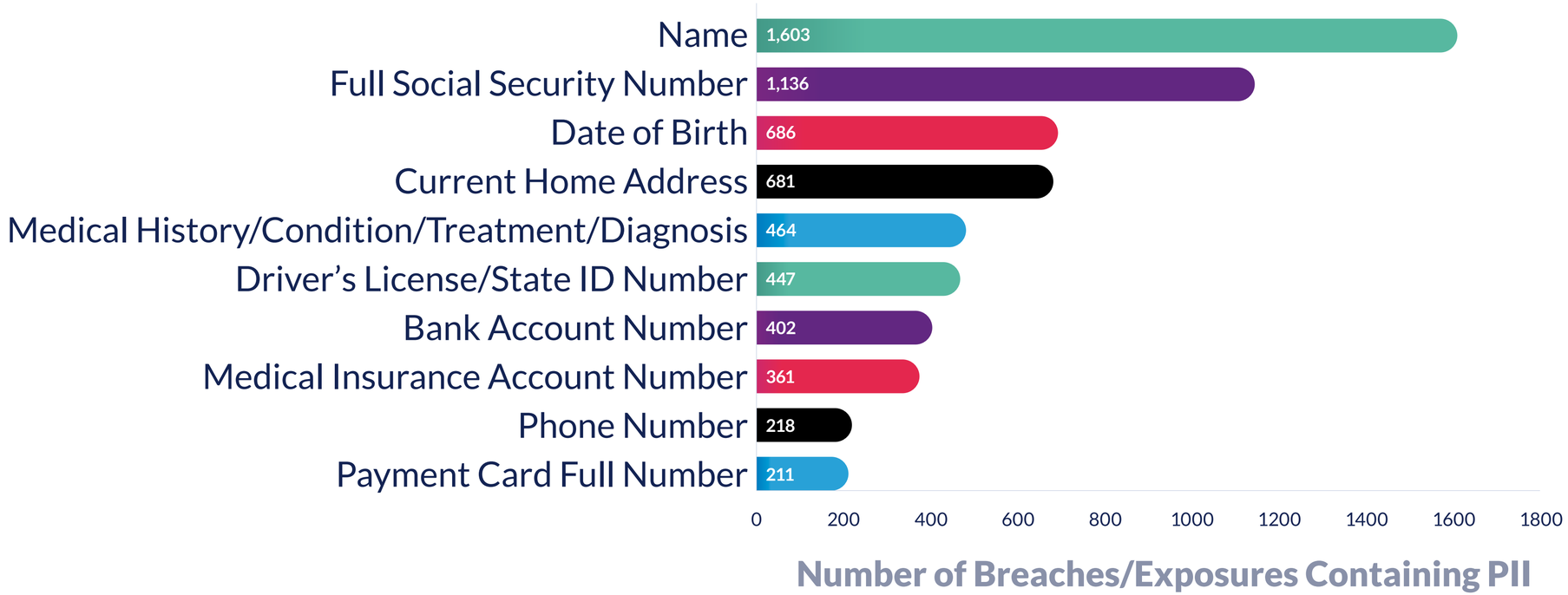
Compromises Involving Sensitive Records



Types of Data Compromised

Personally Identifiable Information

2021 Top 10 Breached Data Attributes



Number of Breaches/Exposures Containing PII

ALL DATA ATTRIBUTES

Name	1,603	Bank Account Routing Number	90	Friends/Family	6	Hometown	n/a
Full Social Security Number	1,136	Income/Wages/Earnings/Compensation	39	Employer Site/System Access Credentials	6	Personal Email Account Credentials	n/a
Date of Birth	686	Other Account Credentials	39	Financial Account PIN	6	Voter Registration Info/Preferences/Etc.	n/a
Current Home Address	681	Work Email Address	30	Insurance Account Details or Credentials	5	Work Email Account Credentials	n/a
Medical History/Condition/Treatment/Diagnosis	464	Employee ID Number/Credentials/Position/Etc.	24	Loan Account Details or Credentials	5	Web History/Preferences	n/a
Driver's License/State ID Number	447	Student ID Number/Student Login/Student Details	21	Merchant Login	5	Credit Dispute Info	n/a
Bank Account Number	402	Employer Contact Information	16	Bank Account Login Credentials	4	Non-Debit Payment Account Credentials	n/a
Medical Insurance Account Number	361	Employer Name	15	Phone Account Credentials	4		
Phone Number	218	Medical Provider Login Credentials	15	Prior Home Address	3		
Payment Card Full Number	211	Medical Insurance Account Credentials	14	Education	3		
Undisclosed Records	205	Payment Card Partial Number	13	W2 Other Info	3		
Personal Email Address	205	Partial Social Security Number	13	Location	2		
Medical Provider Account Number/Medical Record Number	198	Biometric/Authentication Data	12	Utility Account Number	2		
Payment Cardholder Name	177	Other Biographical	12	Social Media Login Credentials	1		
Payment Card Expiration Date	175	IP Address/Device ID	12	Utility Account Credentials	1		
Payment Card Security Code	170	Tax ID Number	9	Security Clearance/Access	n/a		
Passport Number/Visitor Status/Green Card	118	Investment Account Details or Credentials	7	Affiliations	n/a		

Supply Chain Attack Data 2017 through 2021

SUPPLY CHAIN ATTACKS TRENDS

	2021	2020	2019	2018	2017
Number of Third-party/ Supply Chain Attacks	93	69	104	82	103
Number of Entities Impacted by Third-party/ Supply Chain Attacks	559	694	232	101	119

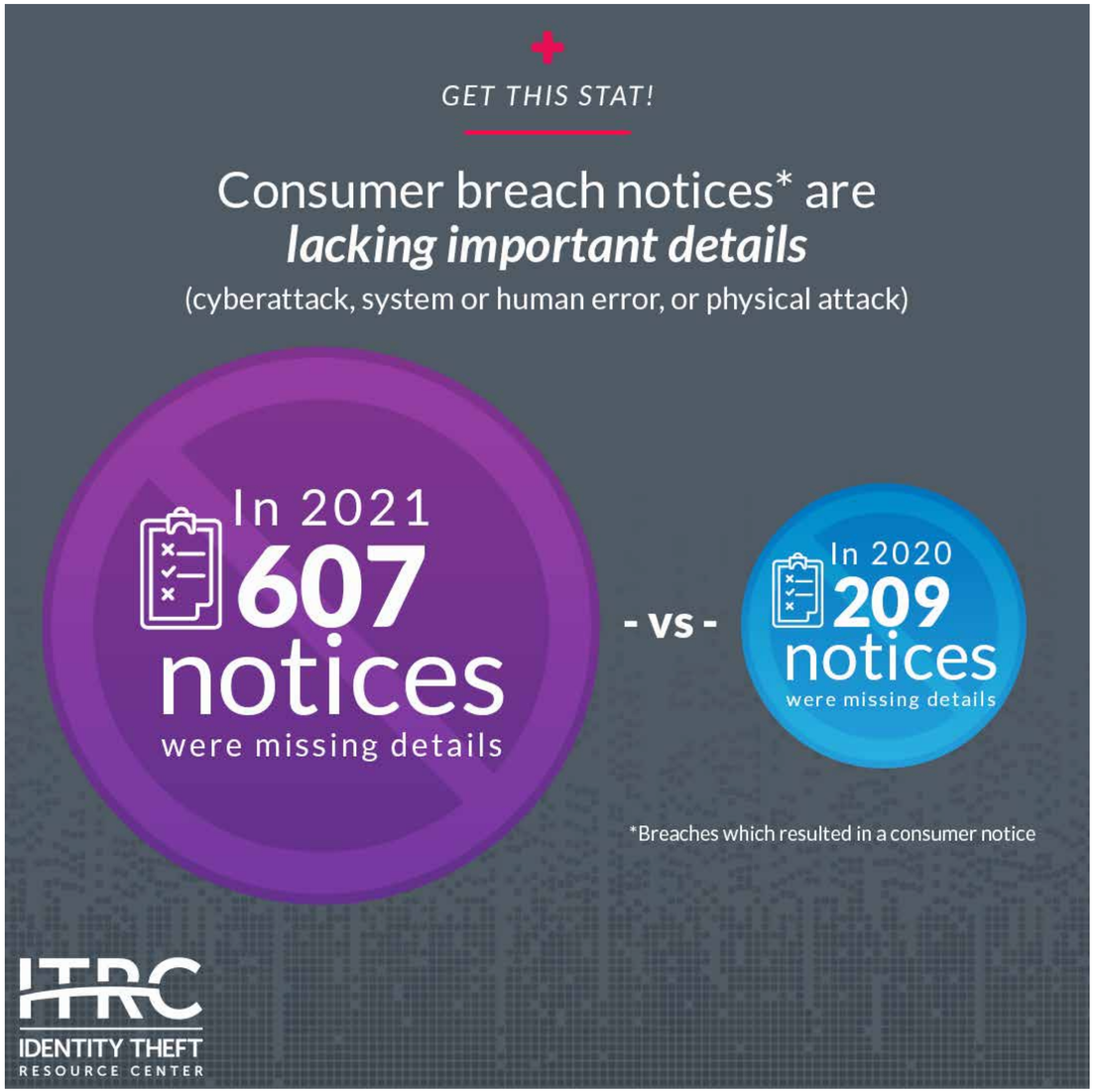
NOTEWORTHY SUPPLY CHAIN ATTACKS (All data was recorded by ITRC as of 1/6/2022)

+ **Blackbaud (2020):** 122 entities with 254,029 individual victims reported in 2021 in addition to the 480 entities with 12,561,072 individual victims of reported in 2020. The total number of entities is 602, with 12,815,101 individual victims
+ **CaptureRX:** 162 entities impacted
+ **Accellion:** 38 entities impacted
+ **Netgain Technologies, LLC (2020):** 24 entities impacted
+ **ParkMobile:** 19 entities impacted
+ **Automatic Funds Transfer Services, Inc.:** 14 entities impacted
+ **Elekta, Inc.:** 13 entities impacted
+ **Herff Jones:** 12 entities impacted
+ **North American Dental Management:** 11 entities impacted
+ **Vertafore:** 6 entities impacted
+ **Med-Data:** 6 entities impacted

Notable Trends

Breach notice **transparency** is decreasing

+ **Why this is important:** The lack of actionable information in breach notices prevents consumers from effectively judging the risks they face of identity misuse and taking the appropriate actions to protect themselves. A decrease in timely notices posted by states, including one state that updated breach notices in December 2021 for the first time since the Fall of 2020, also prevents consumers from taking action to protect themselves and organizations that assist identity crime victims from offering timely, effective advice.

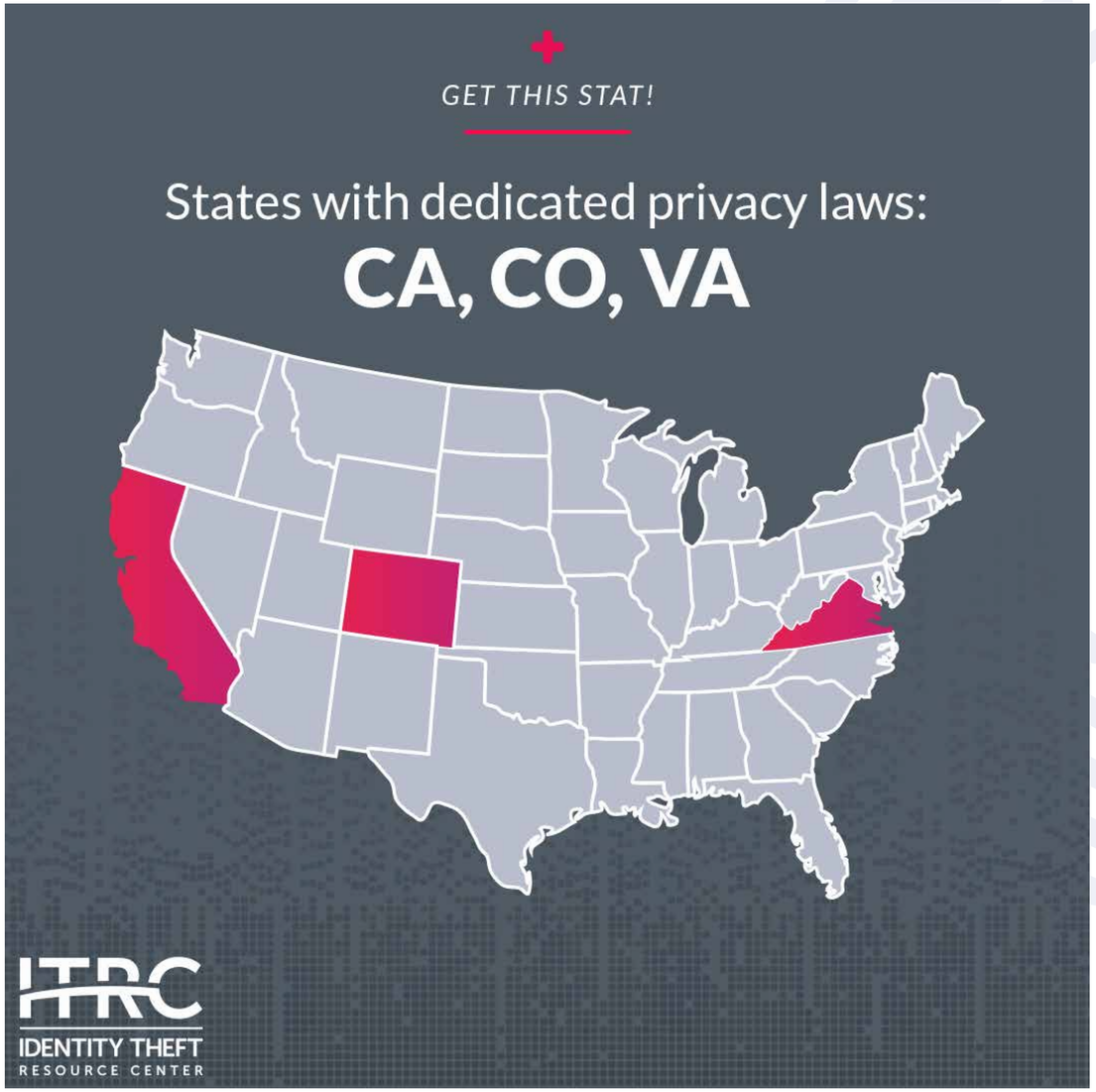


Notice **effectiveness** is low.

+ **Why this is important:** The form and substance of existing notices fail to prompt breach victims into taking actions that can significantly reduce the risk of their compromised identity information being misused.

New state privacy laws are helpful, but still result in **different victim protections** depending on where you live.

+ **Why this is important**: Every state defines personal information differently and every state has a different standard for if, when, and how a victim is notified that their information has been compromised. That means residents of one state may get a data breach notice when a resident across the border in a neighboring state may not receive an alert for the same data breach.



Case Studies

A. Supply Chain Attack
   – Accellion

B. Social Engineering
   – Robinhood

C. Vulnerable Security
   – T-Mobile

Accellion

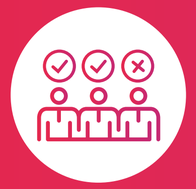
BREACH CAUSE: SUPPLY CHAIN ATTACK

An increasingly common attack method used by cybercriminals is known as a Supply Chain attack. Threat actors attack a single company that is part of a larger supply chain to access the information of multiple organizations.

In the case of Accellion, a U.S.-based software provider, cybercriminals targeted users of the company's 20-year old file sharing software. Accellion customers included law firms and cybersecurity companies that used the software to access sensitive client information that was compromised by ransomware gangs and cyber thieves. The cyberattacks targeted known flaws in Accellion software after the company alerted customers to a series of recently discovered vulnerabilities.

38 customers impacted
6,758,979 consumers at risk

Protect yourself:



Upgrade or Replace Legacy Software

Improve Vendor Compliance

BUSINESSES: *Cyberattacks seek to take advantage of weak or vulnerable security to gain access to the valuable data of multiple companies with a single attack. If you are a business leader, make sure your vendors' and partners' security is as good as your own.*

Robinhood

BREACH CAUSE: SOCIAL ENGINEERING

Social engineering attacks rely on individuals to share confidential information about themselves or their workplace. For example, ransomware operators manipulated a Robinhood customer service representative into giving a criminal access to the investment platform's customer support system.

7+ Million account holders impacted

Protect yourself:

Zero Trust Access model and updated processes

BUSINESSES: *Consider adopting a Zero Trust Access model for giving employees and customers access to information, especially sensitive personal information. That means implementing "never trust, always verify" processes.*

T-Mobile

BREACH CAUSE: VULNERABLE SECURITY

T-Mobile, one of the largest U.S. mobile telecommunications companies, has acknowledged six data breaches since 2018, including two in the last six months of 2021. In August 2021, T-Mobile's systems were attacked through an unprotected network access device in July. By August, the attacker had gained direct access to servers containing account and personal information on current, former, and prospective account holders. T-Mobile confirmed an additional compromise in late December 2021 that impacted an undisclosed number of customers.

53+ Million account holders impacted

Protect yourself:

Patching software flaws as soon as notified

BUSINESSES: *Make sure the security on your internet accessible devices is configured correctly with up-to-date patches to avoid security and data breaches.*

Use multi-factor authentication (MFA) when possible

CONSUMERS: *Make sure you use multi-factor authentication with an authentication app when possible rather than having a code sent to your phone.*

ITRC Breach Alert Service

Free Breach Alerts Coming Soon!

CONSUMER SERVICES

notified™

Later in Q1, 2022, the ITRC will launch a free, data breach alert service for consumers where individuals can create a limited list of companies where they do business. If an organization on the list is added to the ITRC's ***notified***™ data compromise database, a subscriber will receive an email alert.

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 may not receive a direct notification of a data breach with actionable information so they can take steps to protect themselves.

To receive information on how to subscribe to the ***notified*** Consumer Breach Alert Service when it's available, sign-up for our monthly newsletter. We'll publish details on the new service in upcoming newsletters.

Register Today to Get notified™

ITRC's Breach Alert Service

Breach Tracking for Risk Assessment!

BUSINESS SERVICES

notified™

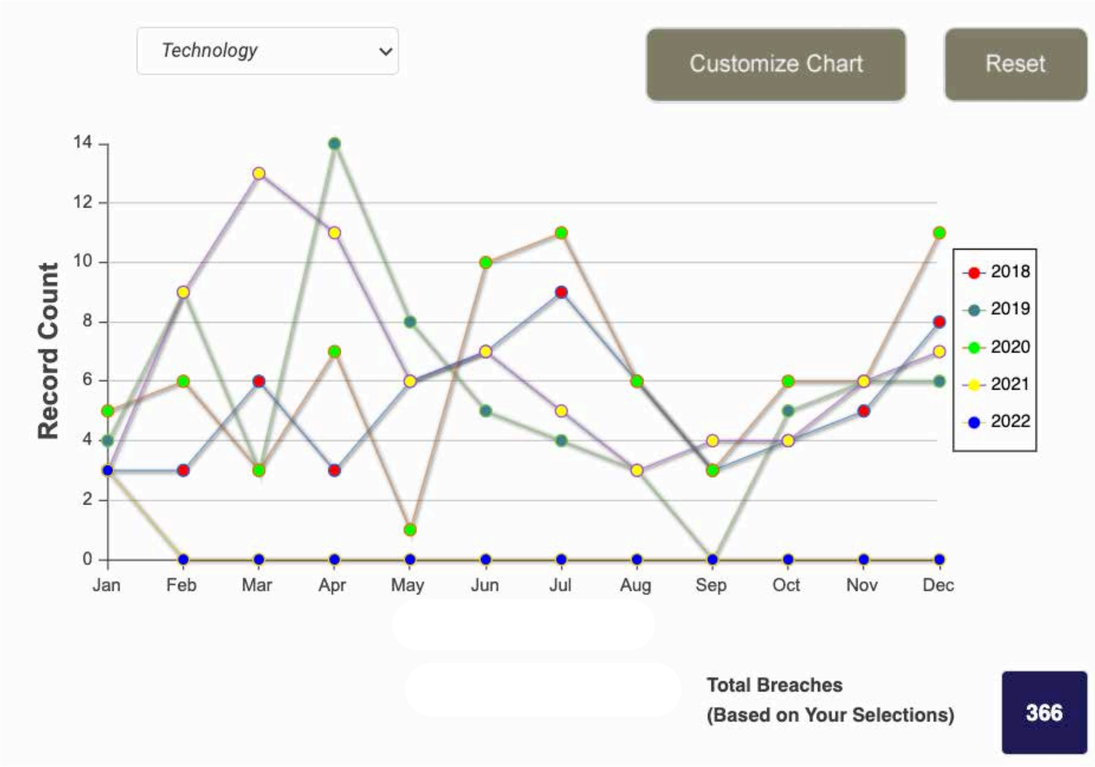
The ITRC launched our ***notified*** data compromise tracking tool in 2020 as a free service to consumers and as a batch or subscription service for businesses. ***notified*** helps people and organizations assess the risks associated with data breaches, exposures, and leaks.

A paid Breach Alert Service subscription for businesses seeking to comply with new corporate and government cybersecurity and vendor due diligence requirements will be available later in 2022. For more information about ***notified***'s business services, contact us at **notifiedbyITRC@idtheftcenter.org.**

Want More **Data**?

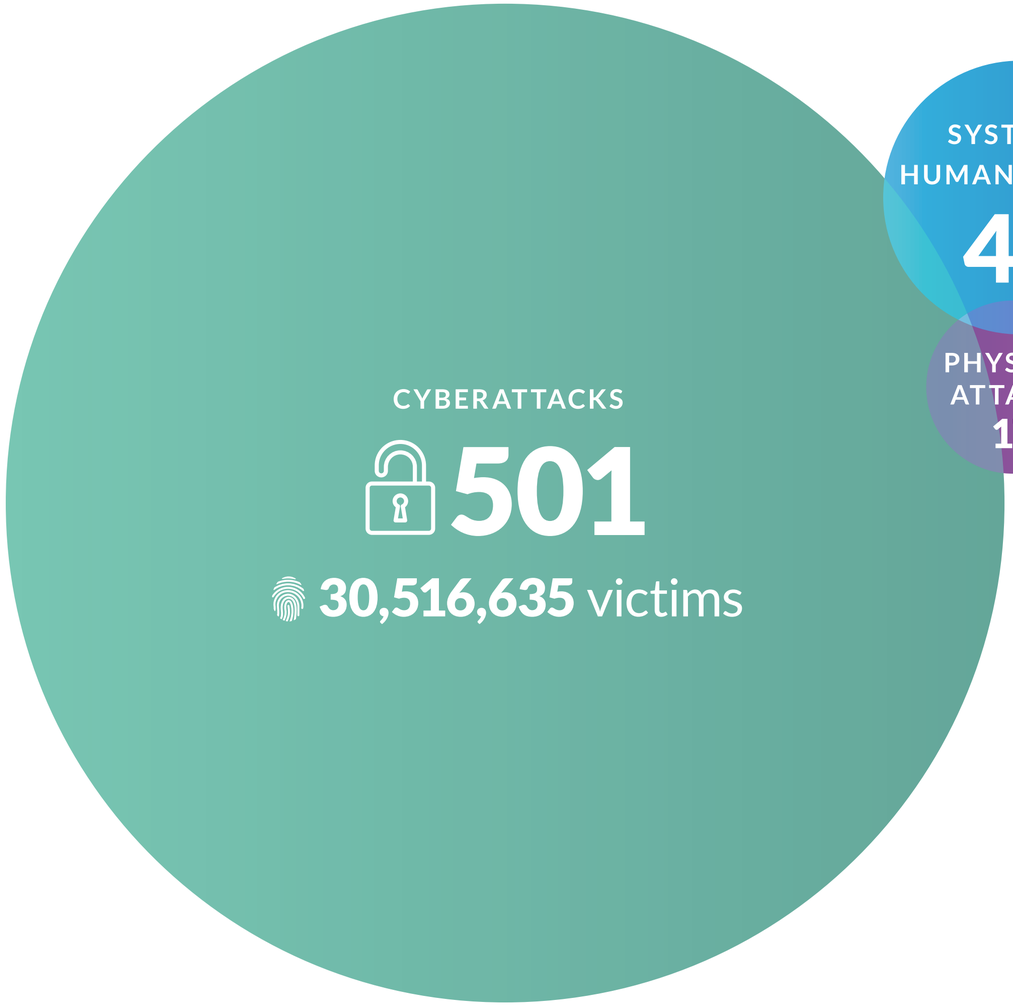
Contact Us to Upgrade Your Subscription Today!

Create your custom chart like the one below!



Appendix

Data Breaches/Exposures Q4



4,189,453 victims

9,739 victims

CYBERATTACKS
+ 164 Phishing/smishing/BEC
+ 104 Ransomware
+ 34 Malware
+ 4 Non-secured Cloud Environment
+ 2 Credential Stuffing
+ 2 Unpatched software
+ 2 Zero Day Attack
+ 94 Other – not specified
+ 95 NA

HUMAN & SYSTEM ERRORS
+ 26 Correspondence (email/letter)
+ 6 Failure to configure cloud security
+ 5 Lost device or document
+ 4 Misconfigured firewalls
+ 4 Other – not specified

PHYSICAL ATTACKS
+ 6 Document Theft
+ 5 Device Theft
+ 2 Improper Disposal
+ 1 Skimming Device
+ 3 Other – not specified

SUPPLY CHAIN ATTACKS *(Included in the attack vectors above)*

69 entities were impacted by **24 third-party/supply chain attacks**, including 4 attacks that were reported in previous months; **271,193 individuals were impacted in Q4 2021**

+ **63** entities affected **270,652** individuals impacted by cyberattacks
+ **4** entities affected; **541** individuals impacted by system & human errors
+ **2** entity affected; **unknown number** of individuals impacted by physical attacks

Data Breaches/Exposures Q3

99,488,464 victims

9,882 victims

CYBERATTACKS
- + 124 Phishing/smishing/BEC
- + 93 Ransomware
- + 33 Malware
- + 6 Non-secured Cloud Environment
- + 4 Credential Stuffing
- + 2 Unpatched software
- + 1 Zero Day Attack
- + 126 Other – not specified

HUMAN & SYSTEM ERRORS
- + 10 Correspondence (email/letter)
- + 20 Failure to configure cloud security
- + 4 Misconfigured firewalls
- + 2 Lost device or document
- + 7 Other – not specified

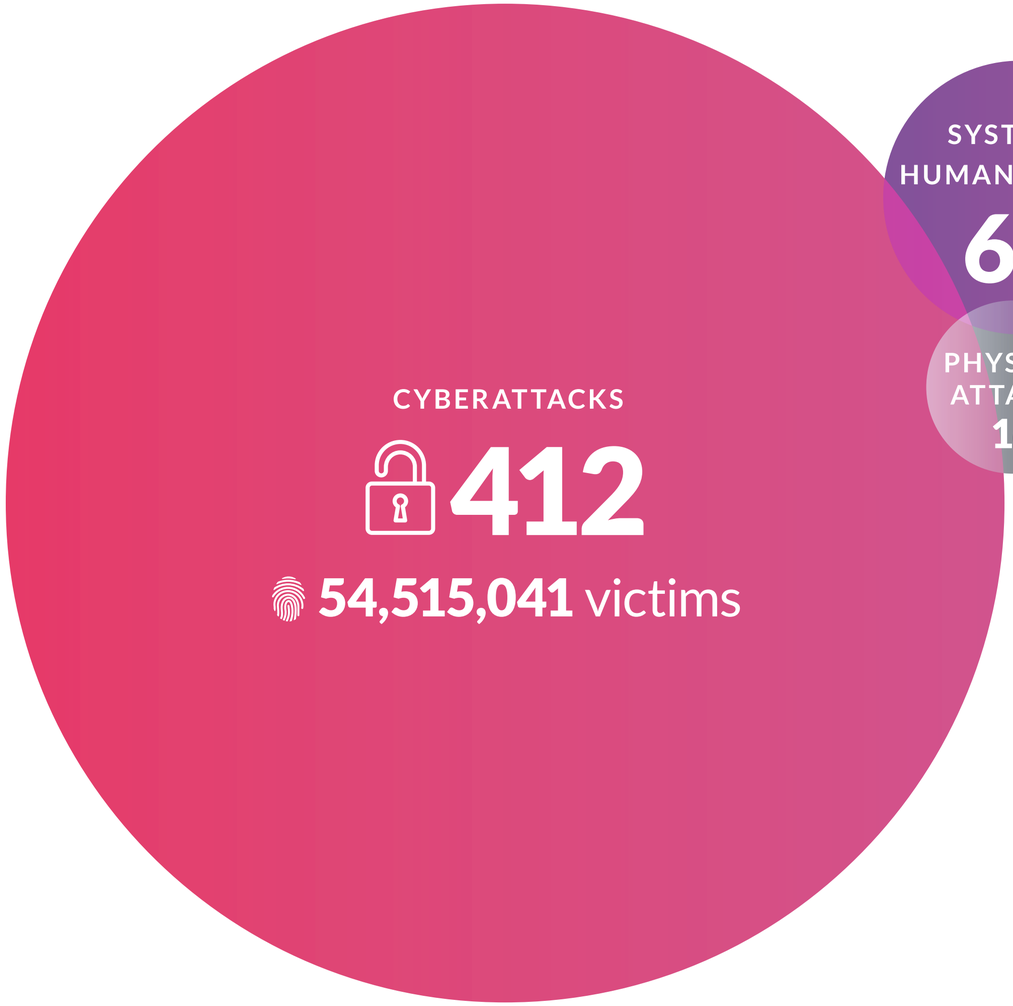
PHYSICAL ATTACKS
- + 1 Device Theft
- + 2 Document Theft
- + 3 Other – not specified

SUPPLY CHAIN ATTACKS *(Included in the attack vectors above)*

60 entities were impacted by **23 third-party/supply chain attacks**, including **8 attacks** that were reported in previous months; **793,052 individuals were impacted in Q3 2021**

- + **57** entities affected **673,447** individuals impacted by cyberattacks
- + **2** entities affected; **2,707** individuals impacted by system & human errors
- + **1** entity affected; **116,898** victims impacted by physical attacks

Data Breaches/Exposures Q2



728,041 victims

77,720 victims

CYBERATTACKS
+ 132 Phishing/smishing/BEC
+ 92 Ransomware
+ 38 Malware
+ 9 Non-secured Cloud Environment
+ 6 Credential Stuffing
+ 129 Other – not specified
+ 6 NA

HUMAN & SYSTEM ERRORS
+ 20 Failure to configure cloud security
+ 18 Correspondence (email/letter)
+ 5 Misconfigured firewalls
+ 3 Lost device or document
+ 14 Other – not specified

PHYSICAL ATTACKS
+ 8 Device Theft
+ 3 Improper Disposal
+ 5 Other – not specified

SUPPLY CHAIN ATTACKS *(Included in the attack vectors above)*

291 entities were impacted by **25 third-party/supply chain attack**s, including **7 attacks** that were reported in previous quarters; **6,124,080 victims were impacted in Q2 2021**

+ **284** entities affected **6,114,697** victims impacted by cyberattacks
+ **6** entities affected; **9,319** victims impacted by system & human errors
+ **1** entity affected; **64** victims impacted by physical attacks

Data Breaches/Exposures Q1

485,801 victims

35,638 victims

CYBERATTACKS
+ 117 Phishing/smishing/BEC
+ 61 Ransomware
+ 34 Malware
+ 4 Non-secured Cloud Environment
+ 2 Credential Stuffing
+ 1 Zero Day Attack
+ 87 Other – not specified

SYSTEM & HUMAN ERRORS
+ 12 Correspondence (email/letter)
+ 8 Failure to configure cloud security
+ 2 Lost device or document
+ 9 Other – not specified

PHYSICAL ATTACKS
+ 3 Device Theft
+ 1 Document Theft
+ 8 Other – not specified

SUPPLY CHAIN ATTACKS *(Included in the attack vectors above)*

139 entities were impacted by **21 third-party/supply chain attacks**, including **6 attacks** that were reported in previous quarters; **18,008,63 individuals were impacted in Q1 2021**

+ **135** entities affected **17,945,554** individuals impacted by cyberattacks
+ **3** entities affected; **63,085** victims impacted by system & human errors
+ **1** entity affected; **unknown number** of victims impacted by physical attacks

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 -** In 2021 the ITRC added a new category of data compromise: Data Leaks. Leaks involve 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).

Data Sources & Methodology

The ITRC gathers information about publicly reported 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.

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

Different states have different reporting requirements. This often results in lags 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.

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.

2021 in review

Data Breach

ANNUAL REPORT

Identity Compromises:
From the Era of Identity Theft to the Age of Identity Fraud

Consumer & Business Resources

For more information about low-cost identity education, protection, and recovery services for small businesses as well as the free services and education opportunities for consumers, visit **idtheftcenter.org** or by email at **notifiedbyITRC@idtheftcenter.org**.

The Identity Theft Resource Center is a 501(c)3 non-profit that does not endorse any particular company, product, or service.

ITRC | IDENTITY THEFT RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

The 2021 Data Breach Report is supported by:

SONTIQ™
A TransUnion® Company