Identity Compromises:
From the Era of Identity Theft to the Age of Identity Fraud
# Table of Contents

I. Letter from the CEO ................................................. 3

II. Executive Summary ............................................... 5
   A. Compromise Trends 2015 to 2021

III. Number of Compromises in 2021 ............................ 7

IV. Root Cause of Compromises ..................................... 8
   A. Cyberattacks
   B. Human & System Errors
   C. Physical Attacks

V. Types of Data Compromised ..................................... 11
   A. Exposed Data/ Breaches 2017 through 2021
   B. Compromises Involving Sensitive Records
   C. 2021 Breached Data Attributes
   D. Supply Chain Attack Data 2017 through 2021

VI. Notable Trends ..................................................... 15

VII. Case Studies ....................................................... 18
   A. Accellion – Supply Chain Attack
   B. Robinhood - Social Engineering
   C. T-Mobile - Vulnerable Security

VIII. ITRC Breach Alert Services (notified™) ............... 22

IX. Appendix ............................................................. 24
   A. Data Breaches/Exposures Q4
   B. Data Breaches/Exposures Q3
   C. Data Breaches/Exposures Q2
   D. Data Breaches/Exposures Q1

X. Glossary of Terms ................................................. 28

XI. Data Sources & Methodology ................................. 29
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.
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

#### Compromise Totals

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

#### Sector Trends

<table>
<thead>
<tr>
<th>Year</th>
<th>Compromises // Victims</th>
<th>Compromises // Victims</th>
<th>Compromises // Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>71</td>
<td>5,161,005</td>
<td>5,161,005</td>
</tr>
<tr>
<td>2016</td>
<td>172</td>
<td>103,939,736</td>
<td>103,939,736</td>
</tr>
<tr>
<td>2017</td>
<td>64</td>
<td>1,193,791</td>
<td>1,193,791</td>
</tr>
<tr>
<td>2018</td>
<td>398</td>
<td>9,080,498</td>
<td>9,080,498</td>
</tr>
<tr>
<td>2019</td>
<td>103</td>
<td>70,265,156</td>
<td>70,265,156</td>
</tr>
</tbody>
</table>

#### Attack Vector Trends

<table>
<thead>
<tr>
<th>Year</th>
<th>Compromises // Victims</th>
<th>Compromises // Victims</th>
<th>Compromises // Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>125</td>
<td>1,680,300</td>
<td>1,680,300</td>
</tr>
<tr>
<td>2016</td>
<td>42</td>
<td>978,254</td>
<td>978,254</td>
</tr>
<tr>
<td>2017</td>
<td>279</td>
<td>19,745,846</td>
<td>19,745,846</td>
</tr>
<tr>
<td>2018</td>
<td>66</td>
<td>3,244,455</td>
<td>3,244,455</td>
</tr>
<tr>
<td>2019</td>
<td>330</td>
<td>28,045,658</td>
<td>28,045,658</td>
</tr>
</tbody>
</table>

#### Executive Summary

The document provides a comprehensive overview of data breaches from 2015 to 2021, highlighting trends in the number of compromises and victims, as well as sector-specific data breaches. It categorizes breaches into various types such as Cyberattacks, Phishing/Smishing/BEC, Ransomware, and others, along with physical attacks and human/system errors. The document also includes a comparison of trends from 2015 to 2021, showing a significant increase in the number of compromises and victims.
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

12 Unknown Compromises
2,555 individuals impacted

*Includes non-U.S victims
Root Cause of Compromises

Cyberattacks

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

1,613 breaches/exposures
188,900,415 victims
**Human & System Errors**

<table>
<thead>
<tr>
<th>Cause</th>
<th>Qty / %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Correspondence (email/letter)</td>
<td>66 / 37%</td>
</tr>
<tr>
<td>Failure to configure cloud security</td>
<td>54 / 30%</td>
</tr>
<tr>
<td>Misconfigured firewall</td>
<td>13 / 7%</td>
</tr>
<tr>
<td>Lost device or document</td>
<td>12 / 7%</td>
</tr>
<tr>
<td>Other - not specified</td>
<td>34 / 19%</td>
</tr>
</tbody>
</table>

- **179 breaches/exposures**
- **104,891,759 victims**
Root Cause of Compromises

Physical Attacks

<table>
<thead>
<tr>
<th>Cause</th>
<th>Qty</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Theft</td>
<td>17</td>
<td>33%</td>
</tr>
<tr>
<td>Document Theft</td>
<td>9</td>
<td>18%</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>5</td>
<td>10%</td>
</tr>
<tr>
<td>Skimming Device</td>
<td>1</td>
<td>2%</td>
</tr>
<tr>
<td>Other - not specified</td>
<td>19</td>
<td>37%</td>
</tr>
</tbody>
</table>

51 breaches/exposures

132,979 victims
Types of Data Compromised

Exposed Data/Breaches 2017 through 2021

5 YEAR TOTAL (2017 - 2021)

- Social Security Number: 3,839
- Personal Health Information: 2,170
- Driver’s License: 1,181
- Bank Account: 1,280
- Email/Password: 961
- Other: 1,013
Types of Data Compromised

Compromises Involving Sensitive Records

- compromises
- vs -

Sensitive records exposed

© 2022 ITRC Annual Data Breach Report | IDTheftCenter.org
2021 Top 10 Breached Data Attributes

- Name: 1,603
- Full Social Security Number: 1,136
- Date of Birth: 686
- Current Home Address: 681
- Medical History/Condition/Treatment/Diagnosis: 464
- Driver’s License/State ID Number: 447
- Bank Account Number: 402
- Medical Insurance Account Number: 361
- Phone Number: 218
- Payment Card Full Number: 211

Number of Breaches/Exposures Containing PII
Supply Chain Attack Data 2017 through 2021

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Third-party/Supply Chain Attacks</th>
<th>Number of Entities Impacted by Third-party/Supply Chain Attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017</td>
<td>103</td>
<td>119</td>
</tr>
<tr>
<td>2018</td>
<td>82</td>
<td>101</td>
</tr>
<tr>
<td>2019</td>
<td>104</td>
<td>232</td>
</tr>
<tr>
<td>2020</td>
<td>69</td>
<td>694</td>
</tr>
<tr>
<td>2021</td>
<td>93</td>
<td>559</td>
</tr>
</tbody>
</table>

Note: All data was recorded by ITRC as of 1/6/2022.

Types of Data Compromised

**Types of Data Compromised**

**Supply Chain Attacks Trends**

**NOTEWORTHY SUPPLY CHAIN ATTACKS**

- **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.
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.
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.

**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, 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.
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.
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!
Data Breaches/Exposures Q4

4,189,453 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

9,739 victims

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

© 2022 ITRC Annual Data Breach Report | IDTheftCenter.org
Data Breaches/Exposures Q3

**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

© 2022 ITRC Annual Data Breach Report | IDTheftCenter.org
Data Breaches/Exposures Q2

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 attacks, 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
Appendix

Data Breaches/Exposures Q1

**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

© 2022 ITRC Annual Data Breach Report | IDTheftCenter.org
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.
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.

The 2021 Data Breach Report is supported by: