Third Quarter 2021 Data Breach Analysis:  
Number of 2021 Data Compromises Surpasses  
Total Number of Compromises In 2020

Key Takeaways

• The number of publicly-reported data compromises through September 30, 2021 has exceeded the total number of events in full-year (FY) 2020 by 17 percent, even though the number of compromises dropped by nine (9) percent compared to the second quarter (Q2) of 2021. The trendline continues to point to a record-breaking year for data compromises.

• The number of data compromise victims dramatically increased in the third quarter (Q3) ~160M individuals primarily due to a series of data exposures\(^1\) in the Quarter.

• The total number of cyberattack-related data compromises year-to-date (YTD) is up 27 percent compared to FY 2020, with Phishing and Ransomware far and away the primary attack vectors.

• There have been no publicly reported data compromises to date in 2021 attributed to payment card skimming devices.

• There is a disturbing trend developing where organizations and state agencies do not include specifics about data compromises or report them on a timely basis. One state has not posted a data breach notice since September 2020.

Discussion

• The total number of publicly reported data compromises dropped slightly in Q3 ending September 30, 2021 (446 in Q3 vs. 491 in Q2). However, the total number of data compromises YTD has surpassed the total of publicly-reported data events in 2020: 1,291 compared to 1,108, a 17 percent increase. The current trendline indicates the total number of data compromises in 2021 will exceed the previous all-time high set in 2017 of 1,529. The current delta is 238.

• Cyberattacks remained the primary cause of data compromises, including data breaches, data exposures, and data leaks. Phishing and related attacks in 2021 (370 to date) will likely exceed the 383 similar attacks reported in 2020. The 244 ransomware-related data compromises reported to date in 2021 exceed the 241 similar events in 2020 and 2019 combined.

• Meanwhile, the number of individuals impacted by a data compromise in Q3 surpassed the total number of victims reported in the first six months of 2021 – ~160M victims in Q3 compared to ~121M in Q1 and Q2 2021 combined. The dramatic rise in the number of victims was directly related to 26 instances where cloud databases were not secured. Six (6) cyberattacks against unsecured databases impacted ~48M victims. Twenty (20) organizations failed to secure a cloud database exposing the personal information of 99M individuals. Data exposures due to a system or human error are generally lower risk because there is no indication the information was accessed, copied, or removed from the exposed database.
• There have been zero (0) data compromises attributed to skimming devices so far in 2021. Skimmer-related data breaches have been steadily declining since 2015 with the introduction of chipped payment cards as required by PCI security standards.

• Supply Chain attacks continue to have a meaningful impact on both companies and individuals. Although Supply Chain attacks only count as a single attack, they impact multiple organizations and the individuals whose data is stored by them. Sixty (60) entities were impacted by 23 third-party/supply chain attacks, including eight (8) attacks that were reported in previous Quarters. Nearly 793K individuals were impacted in Q3.

• There has been an increase in a lack of transparency in breach notices at both the organization and government level that, if it continues, could lead to a significant impact on individuals. See the categories in the charts below that indicate the growth in the number of events with little or no detail (Other). Academic research 3, 4 shows that the majority of individuals already fail to acknowledge or act on data breach notices. Withholding important information or failing to post notices on a timely basis may serve to prevent individuals from taking actions to protect their identities. For example, one state has not posted a new data breach notice on its website since September 2020.

• Adjusting for the large increase in victims of data exposures and unsecured cloud database attacks, ~13M individuals were impacted by all other forms of data compromises. That corresponds to the continuing macro trend of fewer individuals being impacted by mass data breaches related to cyberattacks.

• Data compromises were up in 10 out of 13 sectors in Q3 2021 compared to Q3 2020, and nine (9) out of 13 sectors saw more compromises compared to FY 2020. Financial Services, Manufacturing & Utilities, and Education have seen the largest increases; Healthcare and Professional Services have seen slight decreases.
Q3 2021 Data Compromise Details

Number of Compromises Q3

- **Data Breaches**: 417 data breaches; 61,003,474 victims
- **Data Exposures**: 20 data exposures; 99,128,886 victims; 189,552,977 total records exposed
- **Data Leaks**: One (1) data leak(s); 700,000,000 victims (includes non-U.S. victims)
- **Unknown Attack Vector**: Eight (8) unknowns; 3,172 victims

Attack Vectors Q3 2021

- **Cyberattacks**: 389 breaches/exposures; 60,866,744 victims
  - 124 Phishing/Smishing/BEC
  - 91 Ransomware
  - 33 Malware
  - Six (6) Non-secured cloud environment
  - Four (4) Credential Stuffing
  - Two (2) unpatched software flaw
  - One (1) Zero Day Attack
  - 128 Other – not specified

- **System & Human Errors**: 43 breaches/exposures; 99,256,777 victims
  - 20 Failure to configure cloud security
  - 10 Correspondence (email/letter)
  - Four (4) Misconfigured firewalls
  - Two (2) Lost device or document
  - Seven (7) Other – not specified

- **Physical Attacks**: Six (6) breaches/exposures; 9,882 victims
  - Two (2) Document Theft
  - One (1) Device Theft
  - Three (3) Other – not specified
• **Supply Chain Attacks**: *(included in the attack vectors above)*

  o 60 entities were impacted by 23 third-party/supply chain attacks, including eight (8) attacks that were reported in previous Quarters; 793,052 victims in Q3
    - 57 entities affected; 673,447 victims from third-party/supply chain cyberattacks
    - Two (2) entities affected; 2,707 victims from third-party/supply chain systems and human errors
    - One (1) entity affected; 116,898 victims from third-party/supply chain physical attacks

  o **Noteworthy Supply Chain Attacks**
    - **Blackbaud (2020)**: The ITRC has recorded 580 entities with 12,813,995 victims from the Blackbaud data breach. One-hundred (100) (of the 580) entities with 252,923 victims reported in 2021.
    - **CaptureRX**: The ITRC has recorded 162 entities impacted
    - **Accellion**: The ITRC has recorded 38 entities impacted
    - **Netgain Technologies, LLC (2020)**: The ITRC has recorded 23 entities impacted
    - **ParkMobile**: The ITRC has recorded 19 entities impacted
    - **Herff Jones**: The ITRC has recorded 12 entities impacted
    - **Med-Data**: The ITRC has recorded six (6) entities impacted

Charts

**Compromise Year-over-Year Totals**

<table>
<thead>
<tr>
<th>Month</th>
<th>Compromises</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>2021 YTD*</td>
<td>1,291</td>
<td>281,451,400</td>
</tr>
<tr>
<td>2020</td>
<td>1,108</td>
<td>310,116,907</td>
</tr>
<tr>
<td>2019</td>
<td>1,279</td>
<td>883,558,186</td>
</tr>
<tr>
<td>2018</td>
<td>1,175</td>
<td>2,227,849,622</td>
</tr>
<tr>
<td>2017</td>
<td>1,529</td>
<td>1,827,986,798</td>
</tr>
<tr>
<td>2016</td>
<td>1,105</td>
<td>2,541,588,745</td>
</tr>
<tr>
<td>2015</td>
<td>785</td>
<td>318,276,407</td>
</tr>
</tbody>
</table>

*As of 9/30/2021

**Compromises YTD 2021 by Month**

<table>
<thead>
<tr>
<th>Month</th>
<th>Compromises</th>
<th>Victims</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAN</td>
<td>100</td>
<td>7,385,411</td>
</tr>
<tr>
<td>FEB</td>
<td>111</td>
<td>35,320,708</td>
</tr>
<tr>
<td>MAR</td>
<td>144</td>
<td>23,309,513</td>
</tr>
<tr>
<td>APR</td>
<td>151</td>
<td>25,667,485</td>
</tr>
<tr>
<td>MAY</td>
<td>137</td>
<td>21,393,693</td>
</tr>
<tr>
<td>JUN</td>
<td>203</td>
<td>8,239,058</td>
</tr>
<tr>
<td>JUL</td>
<td>163</td>
<td>7,363,216</td>
</tr>
<tr>
<td>AUG</td>
<td>158</td>
<td>151,670,581</td>
</tr>
<tr>
<td>SEP</td>
<td>124</td>
<td>1,101,735</td>
</tr>
<tr>
<td>TOTAL YTD</td>
<td>1,291</td>
<td>281,451,400</td>
</tr>
</tbody>
</table>

*As of 9/30/2021
METHODOLOGY NOTES: For purposes of quarterly and annual reporting, the ITRC aggregates data events based on the date the breach, exposure, or leak was entered into the database rather than the date the event occurred. This avoids the confusion and data conflicts associated with the need to routinely update previous reports and compromise totals. The date of the original compromise, if known, and the date of the event report are noted in the ITRC's notified data compromise tracking database.

The number of victims linked to individual compromises are updated as needed and can be accessed in the ITRC's notified breach tracking solution.

Unless otherwise noted, all data reported on October 6, 2021, as entered through September 30, 2021.

FOOTNOTES:

1 Data exposures are not generally not data breaches under the ITRC’s definition. Generally, a Data Exposure means personal information was accessible by unauthorized people, but there is no evidence the information was viewed, copied, or removed from the database where it is stored. A data exposure carries a lower risk of identity theft or fraud.

2 The number of data compromises has been adjusted as part of a data audit.

3 University of Michigan: Data breaches - Most victims unaware when shown evidence of multiple compromised accounts

4 Carnegie Melon University: After a breach, users rarely change their passwords, and when they do, they’re often weaker