

Expertise you can trust

## By the Numbers: Second Quarter 2023

The potential for a record-setting 2023 continues. In **176** breaches reported this quarter to the Department of Health and Human Services (HHS), over **27 million** records were impacted. This was the highest number of individuals affected reported in the **previous three years!**

### Hacking and Unauthorized Access

This quarter, **99.9%** of all individuals were impacted by breaches due to hacking and unauthorized access.

### Network Servers are #1 for Hackers

Network Servers were the primary source of data breaches this quarter, with **123** reported events. Of the **27.8** million individuals whose data was compromised, **27.4** of them were due to hacked network servers.

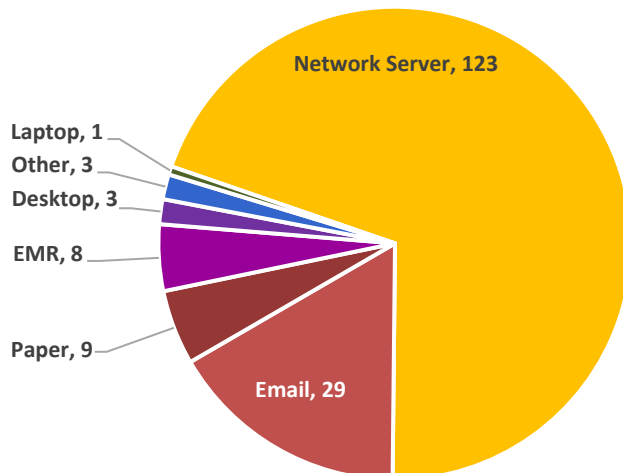
### Compromised with a Click

Email was once again the second most common entry point for data breaches this quarter.

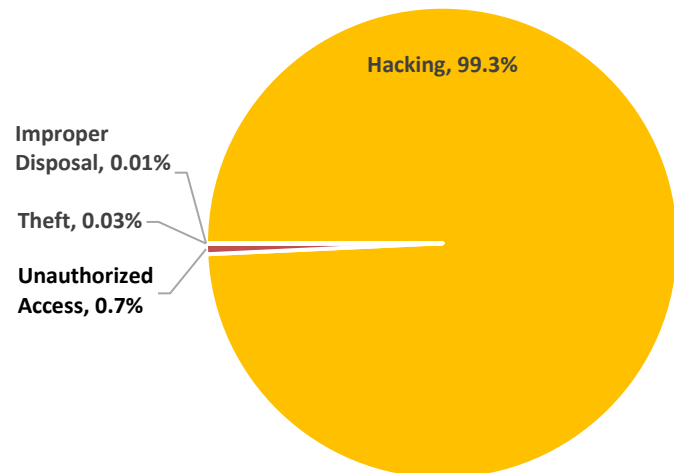
### Business Associates: A Favorite Target

Business Associates were the source of **35%** of breaches, slightly lower this quarter. However, because of the size of these breaches, they accounted for fully **52.7%** of the total. Hacking was the cause of **99.8%** of these breaches.

Q2 '23 Breaches - Data Location



Q2 '23 Breaches - Patient Impact



## By the Numbers: Total to Date

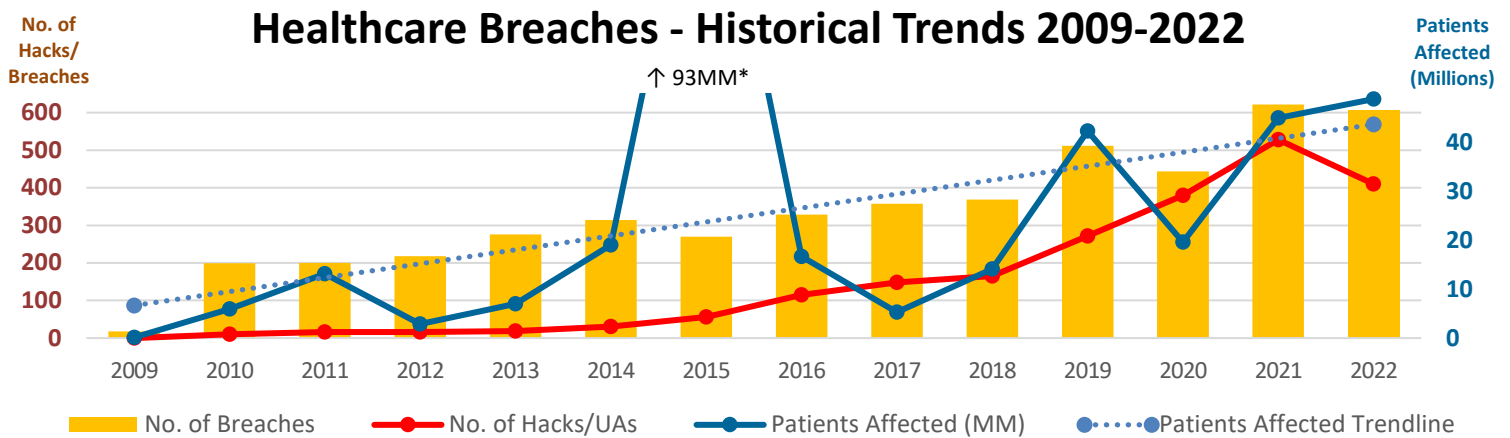
In the period since reporting began in 2009 to **June 30, 2023** there have been **5,129 breaches** reported to HHS that impacted 500 patients or more, affecting **395,187,924** individuals.

The trend emerging over the past several years is that the impact of events attributed to theft, loss, and other causes is being dwarfed by the impact of large data breaches attributed to hacking and unauthorized access. These now account for fully **89%** of all reported events.

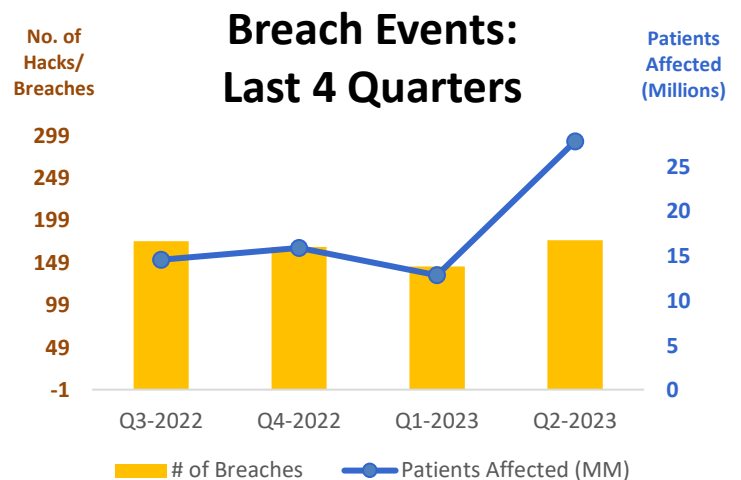
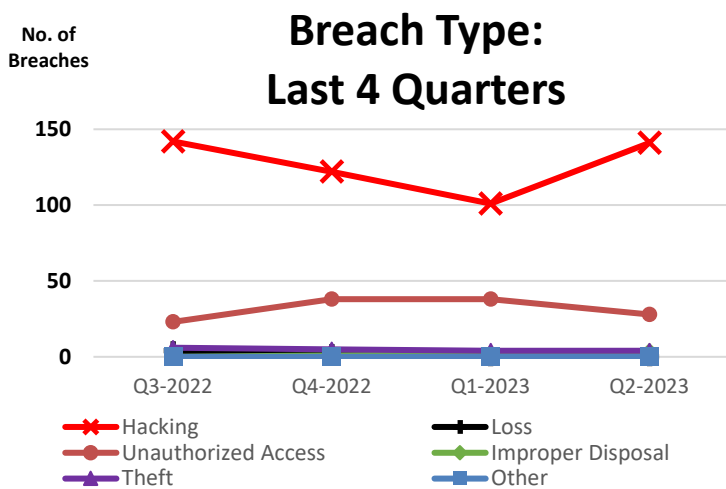
Business Associates and Business Partners have been involved in **1255** incidents since reporting began, which remains steady at **24%** of all reported events. But **132,933,727** patients have been affected, which is now **34%** of the total.

# Key Takeaways

- The number of individuals affected by large data breaches has more than doubled since last quarter.
- Hacking is the primary threat for Business Associates. Their vulnerability to attack demonstrates the critical need for continuous information security vetting to minimize the risk of a BA-based data breach.
- When a facility posts a breach to the HHS website, “hacking” and “unauthorized access” tend to be used interchangeably. And when email is termed the “source” of a data breach, it likely refers to a phishing attack.
- Therefore, since network servers and email are the two leading sources of data breaches, we see why 99% of individuals affected by data breaches are described as victims of hacking and unauthorized access.



\*Off chart due to 78.8 million members impacted by 2015 Anthem breach



## Breach Breakdown – 2009 to Present

| Exploit Type               | Number of Incidents | % Total Incidents | Number of Patients | % of Patients |
|----------------------------|---------------------|-------------------|--------------------|---------------|
| <b>Hacking</b>             | <b>2,465</b>        | <b>48%</b>        | <b>324,583,096</b> | <b>81%</b>    |
| <b>Unauthorized Access</b> | <b>1,234</b>        | <b>24%</b>        | 30,151,985         | 8%            |
| <b>Theft</b>               | 1002                | 20%               | <b>26,830,774</b>  | <b>7%</b>     |
| <b>Loss</b>                | 226                 | 4%                | 8,327,940          | 2%            |
| <b>Improper Disposal</b>   | 113                 | 2%                | 2,130,630          | 1%            |
| <b>Other*</b>              | 89                  | 2%                | 3,163,499          | 1%            |

Source: [https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf)

\* Category discontinued in 2010