KROLL

# Data Breach Outlook:

## Finance Surpasses Healthcare as Most Breached Industry in 2023

# Data Breach Outlook: Finance Surpasses Healthcare as Most Breached Industry in 2023

*By David White,*
*Global Head of Breach Notification, Cyber Risk*

While businesses might have become more prepared for direct cyberattacks, 2023 demonstrated that unfortunately a business is only as secure as the organizations within their environment. Third-party risk, which is to say any risk to an organization by external parties in its ecosystem or supply chain, was the headline culprit in 2023. This was greatly due to the extensive impact of the CLOP ransomware gang's exploitations of the MOVEit Transfer vulnerability as well as the rise of social engineering attacks like business email compromise (BEC).

Kroll handles thousands of incidents every year and saw evidence of this breach having a significant impact on the most breached industries. In this year's Data Breach Outlook, Kroll has ranked which industries continue to top the charts.

## The Finance Sector Overtakes Healthcare for Most Breached Industry

In 2023, finance was the most breached industry, accounting for 27% of the breaches handled by Kroll, compared to 19% in 2022. While in the spotlight for 2022, healthcare dropped to second place, yet still accounted for 20% of breaches. This is only slightly less than in 2022 where it accounted for 22% of breaches.

The financial sector is an attractive target for cyber criminals not only for the immediate financial gain but also due to the wealth of sensitive customer information it holds. However, the 2023 increase in data breaches is likely due to the CLOP ransomware activity impacting small- to mid-sized regional banks. Further, Kroll observed several cases in

which financial institutions were affected by the CLOP exploitation when a third party they worked with was posted to the victim shaming site, exposing data related to their customers. This type of activity and its impact underscores the fragility of organizational interdependence and the extent of third-party risk.

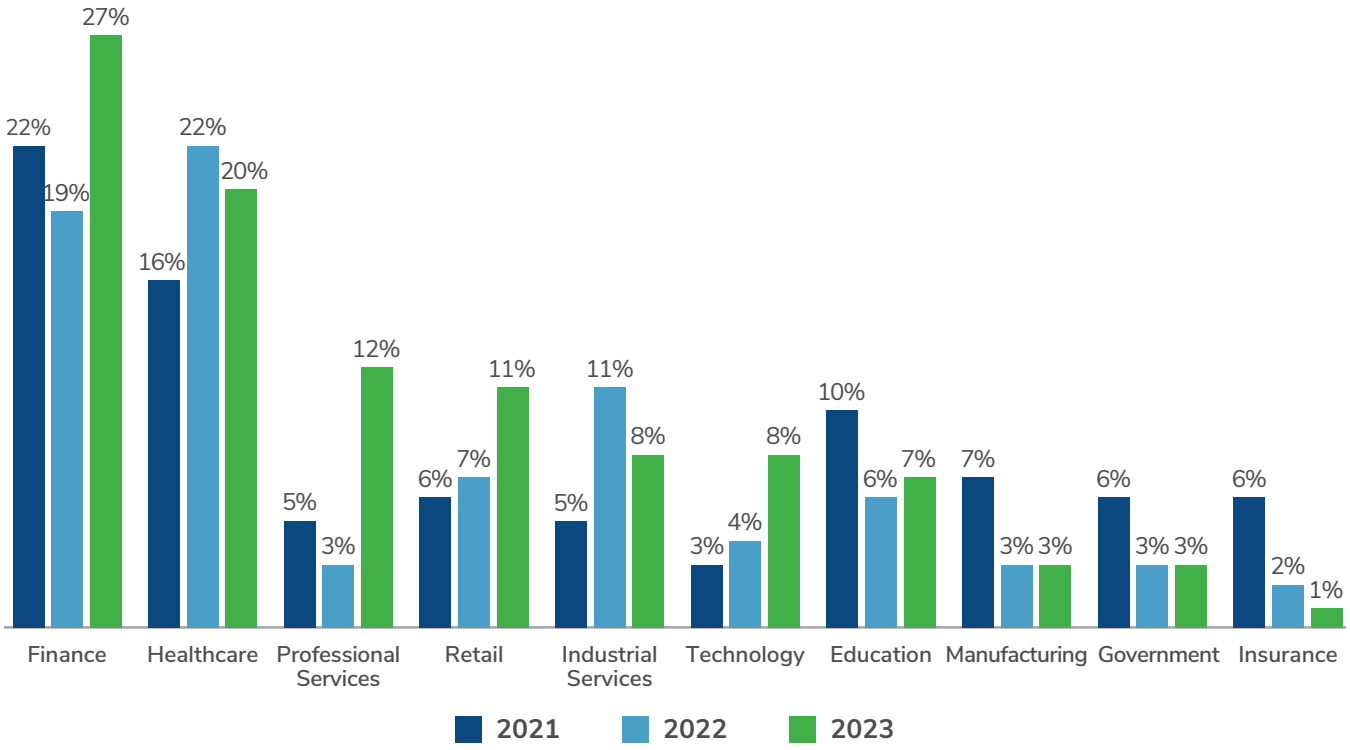
Further, the professional services moved up from fifth most targeted industry to third in 2023. This could be due to the steady rise in BEC cases particularly affecting this industry, with a high concentration of this activity related to legal firms from the BLACKCAT ransomware gang. Indeed from Q1 to Q3 of 2023, Kroll saw BEC attacks increase by 21%.

| 2023 Rank | Industry |
|---|---|
| 1 ↑ | Finance |
| 2 ↓ | Healthcare |
| 3 ↑ | Professional Services |
| 4 → | Retail |
| 5 ↓ | Industrial Services |
| 6 ↑ | Technology |
| 7 ↓ | Education |
| 8 ↑ | Manufacturing |
| 9 ↑ | Government |
| 10 ↓ | Insurance |

## Third-Party Security Risks Caused Ripples Across Multiple Industries

While the finance and healthcare sectors battle it out for a gold and silver medal yet again, perhaps a more interesting story is found in the middle of the chart.

### Percentage of Data Breaches From 2021 to 2023, by Industry




**Notable shifts in 2023:**

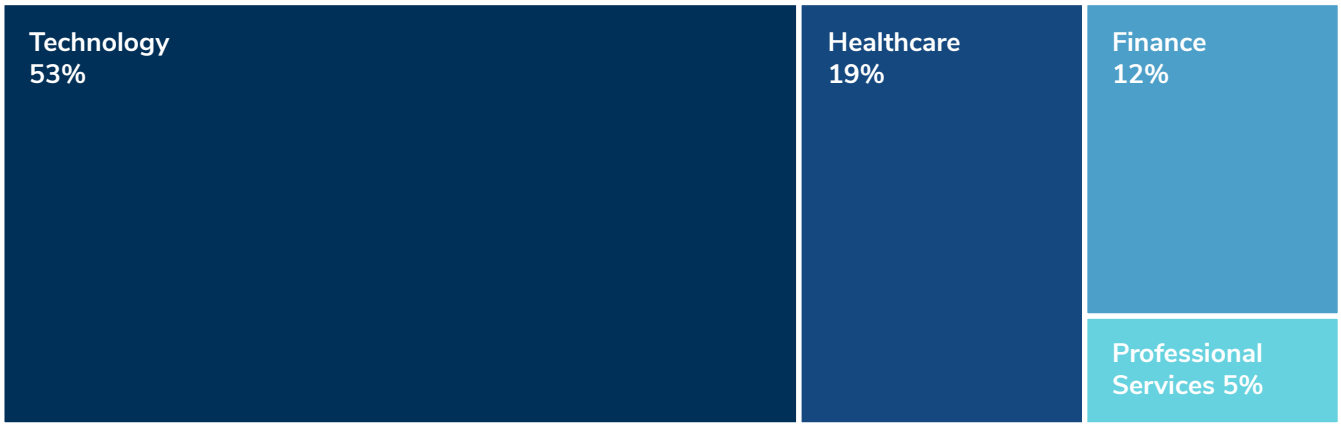
- While ranking third in 2022, industrial services dropped down to fifth place, and professional services took the bronze position on the podium. In fact, there was a 45% year-over-year (YoY) drop in data breach cases observed by Kroll in the industrial services sector.
- Further, data breaches in the professional services sector increased from 3% in 2022 to 12% in 2023.
- While remaining in fourth place, the retail industry is seeing a steady increase in data breaches over the last few years accounting for 11% of data breaches.
- Data breaches on manufacturing and government remain low, with industrial services looking likely to follow the same trend.
- Breaches in the insurance sector fell even lower in the top 10 table of most breached industries, going from the top five in 2021, to 10th place in 2023, an 81% drop in breaches YoY when compared to 2022.
- An industry that has made a huge impact in the data breach space is technology. While just missing out on a top five spot, the technology sector saw a YoY increase of 40%.

## I'm a Technology Company, and I've Just Been Breached

Further investigation into the data unveils some insights into how concerned consumers are in these respective industries about the data breaches in question. While the financial sector might have experienced the most data breaches in 2023, it was in fact the technology sector that seemed the most concerned. Indeed, the highest number of incoming calls related to these data breaches came from the technology sector as well as the highest number of consumers who took up identity protection – often a combination of identity and credit monitoring.

In fact, in 2023, Kroll saw over a quarter of a million calls from the technology sector and provided over a million identity monitoring service activations activations.

### Percentage of Calls Following Data Breaches in 2023




### Percentage of Identity Monitoring Service Activations Taken Up Following Data Breaches in 2023

**Findings include:**

- Fifty-three percent of enquiries coming from consumers in 2023 following being notified of a breach were related to the technology industry; only 12% were in the finance industry.
- Of all the credit and identity monitoring taken up by consumers, 68% were involved in technology breaches, compared to only 13% in healthcare and 10% in finance.
- Technology saw a 47,264% YoY increase in the number of calls following a breach, whereas finance saw a drop of 53%.
- Technology also saw a 31,219% YoY increase in the amount of identity monitoring taken up, compared to a drop of 55% in the finance sector.
- Healthcare also showed YoY increases in both the number of enquiries following a breach (14%) and in the amount of credit or identity monitoring taken up (99%).

This astronomical increase in calls and monitoring for the technology sector all point to the same glaring cyberattack from 2023 – the MOVEit transfer vulnerability.

The MOVEit vulnerability was a perfect example of the ripple effect one attack can have on an ecosystem of connected companies. Indeed, third-party risk is now presenting as a key area of concern due to shifting threat actor behaviors and priorities.

Within the technology sector group observed by Kroll were businesses that deal with pensions and benefits. This could account for the sharp increase in phone calls made following being notified of a breach as the age demographic of this particular industry could be more inclined to call a helpline in order to ensure their pensions and benefits remain safe.

This could also be of interest to insurers looking to estimate the financial exposure of data breaches. A more engaged population of consumers impacted by a data breach could result in more identity monitoring and higher costs for the insurer and/or organization.

Interestingly, Kroll data shows that in total, over 91 million people were notified of a data breach in 2023. This can be broken down in the below communication channels:

**65,658,461**
**physical letters sent**

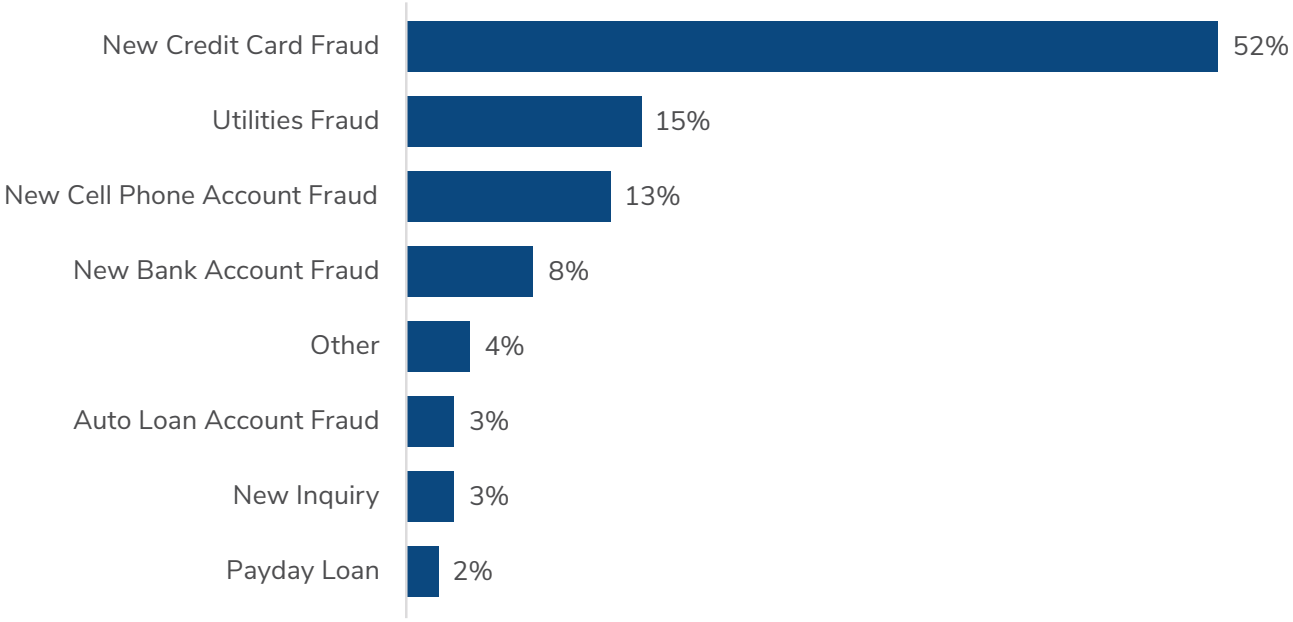
**19,187,822**
**emails sent**

**7,122,441**
**SMS texts sent**

## The Types of Scams Remain Consistent

When looking at the identity theft trends and how victims are being targeted, one method in particular continues to be the most common; new credit card fraud. Utilities fraud and new cell phones fraud were also trending in 2023.

### Percentage of Identify Theft Cases by Type of Fraud




Understanding the drivers behind the Data Breach Outlook figures is subjective, and it is important that businesses combine this data with their own insight from talking to customers and market research. It is also true that while an industry may make up less of the overall number of data breach cases, it is not immune from the impact of a data breach and should similarly have playbooks if an incident was to occur.

To understand more about how the data breach notification process works and what you can do ahead of time to ensure it runs as smoothly as possible with minimal financial and reputational damage, please reach out to our data breach experts.

You may also be interested in reading our 2022 Data Breach Outlook – Healthcare is the Most Breached Industry of 2022.

For more insights, visit the Cyber Blog at **kroll.com/cyberblog**

KROLL

## TALK TO A KROLL EXPERT TODAY

**North America**
T: 877 300 6816

**UK**
T: 808 101 2168

**Brazil**
T: 0800 761 2318

**Additional hotlines at:**
kroll.com/hotlines

**Or via email:**
CyberResponse@kroll.com

---

**About Kroll**

As the leading independent provider of risk and financial advisory solutions, Kroll leverages our unique insights, data and technology to help clients stay ahead of complex demands. Kroll's global team continues the firm's nearly 100-year history of trusted expertise spanning risk, governance, transactions and valuation. Our advanced solutions and intelligence provide clients the foresight they need to create an enduring competitive advantage. At Kroll, our values define who we are and how we partner with clients and communities. Learn more at Kroll.com.

*M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.*