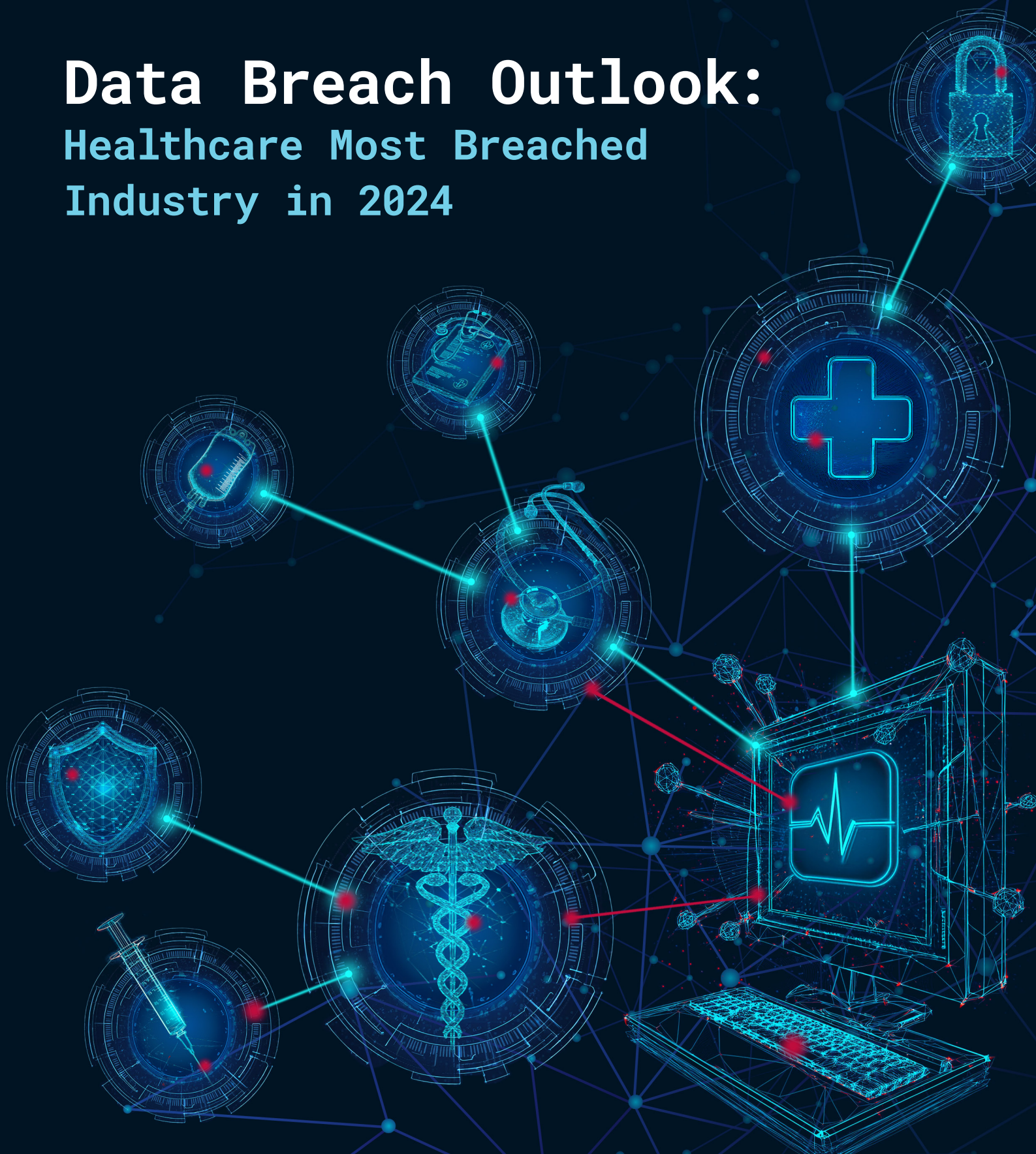
KROLL

Data Breach Outlook:

Healthcare Most Breached Industry in 2024



Data Breach Outlook: Healthcare Most Breached Industry in 2024

By Denyl Green,
Global Head of Breach Notification, Kroll

When it comes to security, 2024 was unfortunately a standout year for the healthcare sector. Kroll found that the healthcare industry was the most breached, had fairly immature incident response practices, and unfortunately suffered numerous cyberattacks culminating in a year that left healthcare boards thinking deeply of the overall risk to their businesses.

According to The HIPAA Journal, "*2024 was the worst-ever in terms of breached healthcare records, which jumped by 9.4% from last year's record-breaking total to 184,111,469 breached records.*"

This is due to the largest healthcare data breach of the year, Change Healthcare. In February of last year, a ransomware group breached the Change Healthcare network and exfiltrated the health information of reportedly an estimated 100 million individuals, and then encrypted the files. Change Healthcare disclosed that the attack started when members of the BLACKCAT ransomware group used stolen credentials to log into the company's Citrix remote access service. This event demonstrated the widespread disruption a breach can cause due to the number of healthcare organizations that relied on Change Healthcare's systems. Though Kroll did not handle the Change Healthcare breach response, Kroll assisted with numerous large third-party breaches and saw firsthand the impact to organizations recovering from these incidents.

Kroll handles thousands of incidents every year and, in review of breach event data for 2024, found this trend prevailed. In its Data Breach Outlook—Year in Review, it has ranked which industries continue to top the charts.

Healthcare Overtakes Finance as Most Breached Industry

In 2024, healthcare was the most breached industry, accounting for nearly a quarter (23%) of breaches handled by Kroll, compared to 18% in 2023.

While in the spotlight for 2023, the finance sector dropped to second place. However, the difference between most and second-most breached industry is very small.

Breaches in the finance sector accounted for 22% of breaches handled by Kroll. However, this is still a decrease in the proportion of breaches compared to last year, when the finance sector accounted for 26% of breaches handled by Kroll.

This is not surprising considering the breaches that affected the industry this year, and the fact that the healthcare industry remains an attractive target for cyber criminals.

As Kroll reported in Q3 of 2024, the impact of a breach in an increasingly interconnected and cloud-dependent world can have a large-scale domino effect.

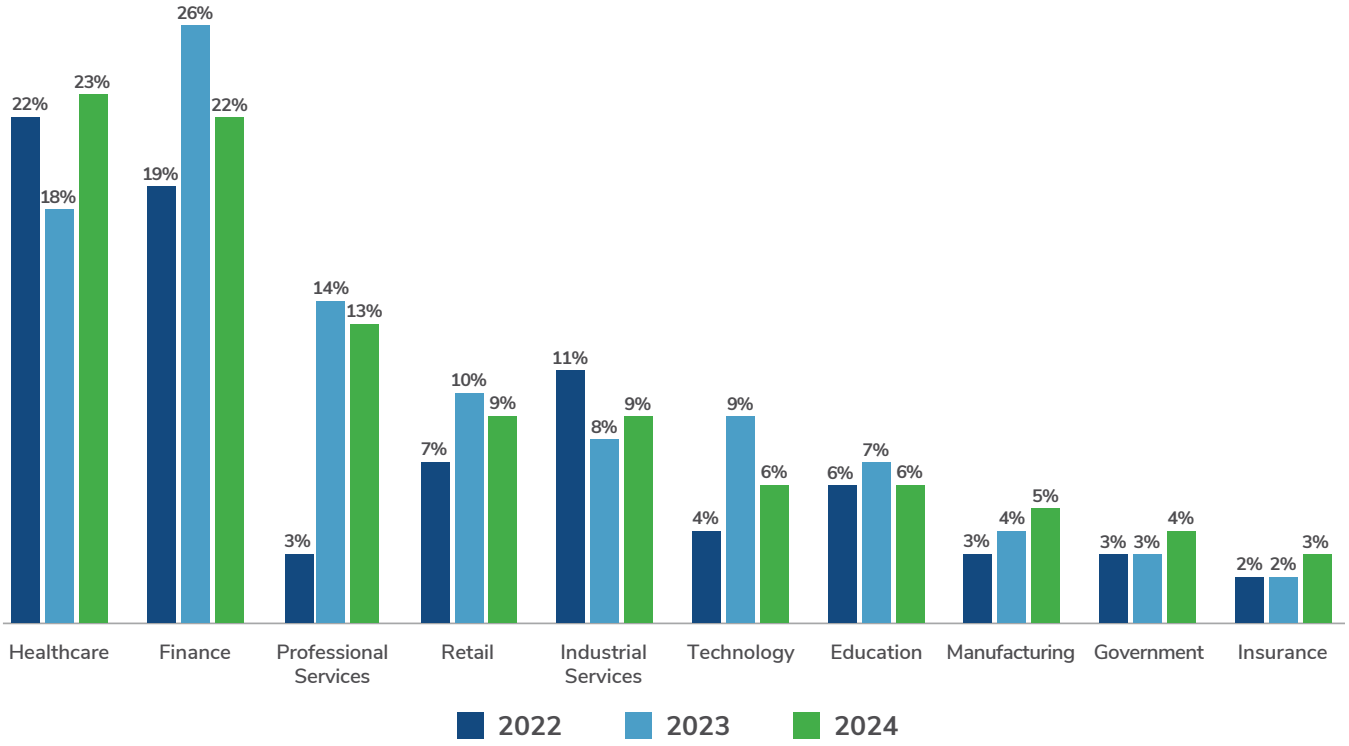
Looking at the rest of the most-breached leaderboard, a lot of the rankings remain the same from 2023. YoY breaches decreased in all industries compared to 2023, except for in the manufacturing and the government sectors, which increased by 4% and 10%, respectively.

2025 Rank	Industry
1 ↑	Healthcare
2 ↓	Finance
3 →	Professional Services
4 →	Retail
5 ↑	Industrial Services
6 ↓	Technology
7 →	Education
8 →	Manufacturing
9 →	Government
10 →	Insurance

Targets Remain Consistent for Data Breaches

While it seems the finance and healthcare sectors will continue vying for first and second place in the most-breached chart, the shifts—or lack thereof—among the rest of the industries perhaps tell a story about the tactics of threat actors.

Percentage of Data Breaches From 2022 to 2024, by Industry



Notable Changes in 2024:

- There was a significant drop in the number of data breaches in the technology sector, down by 46% compared to 2023. This could be due to the extensive impact of the CLOP ransomware gang's exploitations of the MOVEit Transfer vulnerability we saw in 2023 diminishing.
- Technology wasn't alone in having significant decreases in Kroll-observed breaches. The education and retail sectors also had significant decreases, at 38% and 33%, respectively.
- Despite ranking last in the table above, and not moving from that spot YoY, the insurance sector saw a notable increase in breaches of 25%.
- Data breaches on manufacturing and government remain low, with industrial services continuing a steady decline in the number of data breaches.

The Healthcare Industry Takes Action

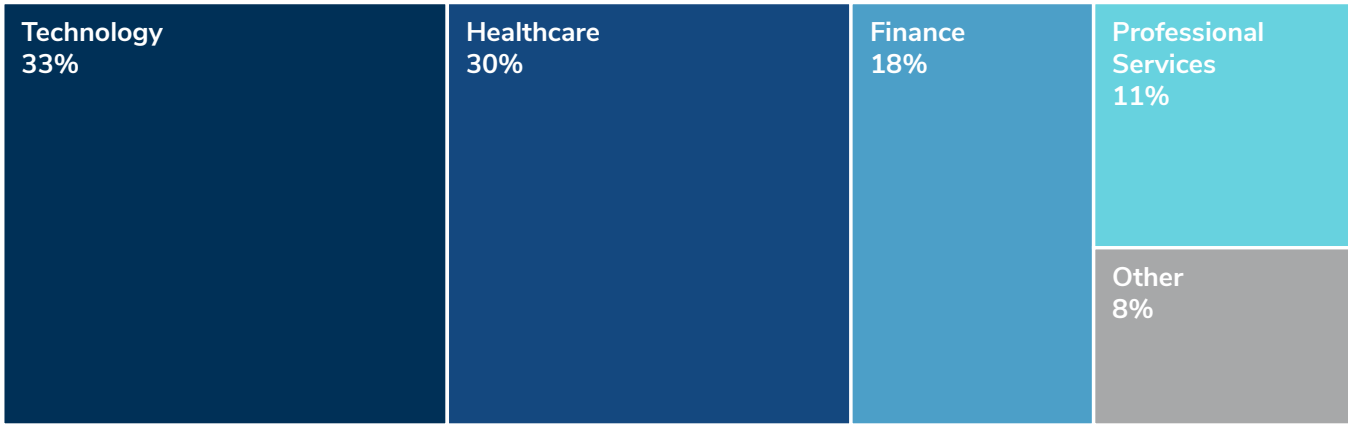
Further investigation into the data unveils some insights into how concerned these industries' consumers are about the data breaches in question.

Similar to in 2023, despite the healthcare sector experiencing the most data breaches in 2024, it was in fact the technology sector that seemed most concerned. Indeed, the highest number of incoming calls related to these data breaches came in the technology industry.

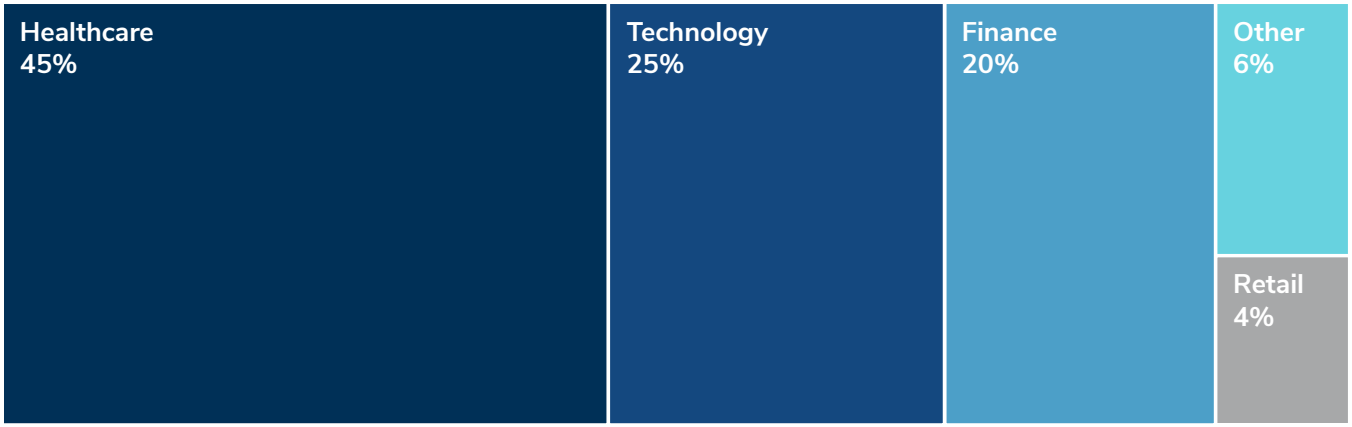
However, it was the healthcare industry that ranked highest in the number of consumers who took up identity protection—often a combination of identity and credit monitoring. This could be due to the highly publicized breaches in that area causing businesses to want to protect themselves quickly.

This information 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.

Percentage of Calls Following a Data Breach in 2024



Percentage of Identity Monitoring Service Activations Taken Up Following Data Breaches in 2024



Key findings include:

- A third (33%) of inquiries coming from consumers in 2024 after being notified of a breach were related to the technology industry, compared to 30% from the healthcare industry and only 18% from the finance industry.
- Of all the credit and identity monitoring that consumers activated, 45% were involved in healthcare breaches, compared to 25% in technology and 20% in finance.
- Technology saw a 69% YoY decrease in the number of calls following a breach, whereas calls in the government sector increased by 352%. This is even more interesting when looking at the YoY figures from 2022 to 2023, when the government sector's post-breach calls declined by 99%.
- Despite the intense focus on the healthcare industry in 2024, the industry saw a 21% drop in the number of calls following a breach.
- Healthcare showed a YoY increase of 85% in the amount of credit or identity monitoring activated. Finance saw a small increase of 9%.
- Professional services saw an even greater YoY increase (128%) in the amount of identity monitoring activated.

Despite not leading the charts, it's not surprising that a third of inquiries coming from consumers in 2024 were from the technology sector, because of the continued prevalence of third-party risk. A breach in one industry can make waves in another, often due to the interconnectedness of business today. Indeed, as we saw this summer, even faulty software updates can lead to massive outages and unintended cyber consequences.

The healthcare industry is a target-rich environment and companies need to be looking at their medium-and long-term programs to ensure they can remain safe and secure. Understanding who your adversaries are, and what their capabilities are, is key. From there, you can build a comprehensive risk strategy to understand the edges of your exposure, take down what you can and understand what you can't.

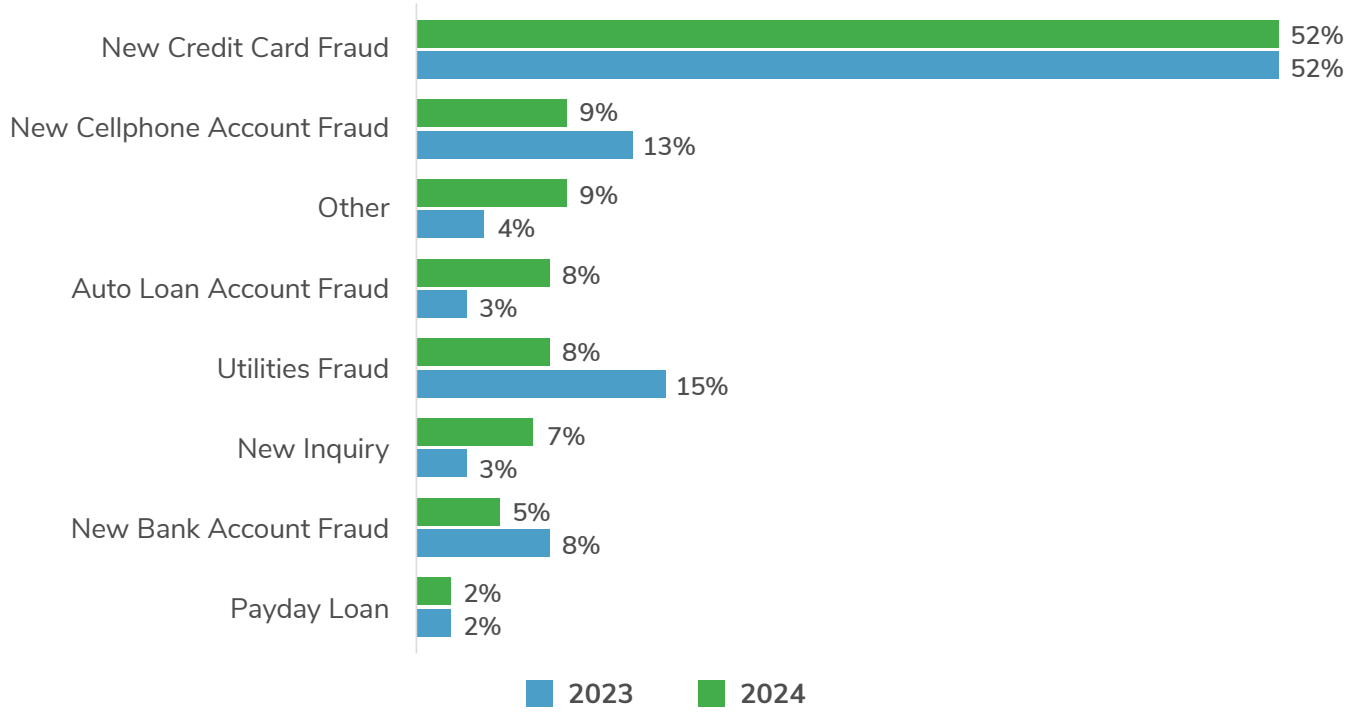
New Credit Card Fraud Remains Most Prevalent

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. This type of identity theft has been prevalent for years, partially due to the ease of creating these types of fraudulent accounts. Consumer protections such as credit freezes are available but still under-utilized.

New cellphone fraud and auto loan account fraud were also trending in 2024. Interestingly, there was a significant decrease in utilities fraud.

Notably, while less common than other types of fraud, Kroll investigators report an increase in rental fraud and criminal identity theft, reflected in the case type category. These issues are especially difficult and complex to resolve, often requiring legal assistance, and are an alarming trend to see.

Percentage of Kroll Identity 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 customer conversations 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 were 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, reach out to our our data breach experts.

You may also be interested in reading our 2023 *Data Breach Outlook:* Finance Surpasses Healthcare as Most Breached Industry in 2023.

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 financial and risk 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.