Recent Snowflake Data Breach Exposes Dangers of Third-Party Data Platforms: Your 5-Step Plan After Suffering a Data Breach

Insights
8.23.24

When a prominent cloud storage company recently suffered a critical data breach that quickly developed into one of the largest data breaches of all time, it served as a wake-up call to companies to ensure that their data compliance efforts are up to date – and to pay careful attention to which third-parties have access to their data. The Snowflake hack, announced in May, resulted in the theft and disclosure of customer data from companies across a variety of industries. This data breach demonstrates that even the most technologically savvy companies are still vulnerable and that a small breach can quickly cascade to impact millions of customers. What do you need to know about this event, and what are the 5 things you should do if you suffer a data breach?

Snowflake Suffers Major Data Breach

Snowflake – a cloud-based data platform that offers data storage, processing, and analysis services – suffered a critical data breach that was announced on May 30. The hackers exploited a weakness in the company's customer account security systems, which allowed them to access and steal millions of bank account numbers, credit card numbers, and other customer and staff data from Snowflake's high-profile client accounts. Since the attack, cybercriminals have been extorting victims and selling stolen data on the dark web.

Snowflake became a huge target when it went public in 2020, raising more than $3 billion in the biggest initial public offering ever for a software company. Since then, it has worked with many high-profile companies to store and analyze their data. The Snowflake platform services over 10,000 customer accounts globally and receives billions of data queries each day. With the sheer number of user data, lucrative earnings, and industry notoriety, it is easy to see why Snowflake was an attractive target for hackers.

You've been Breached – What Now?

Unfortunately, the key question surrounding a data breach at your business is not a question of "if," but "when." Therefore, while prevention is an important duty, it is not the only one that matters. Your response in cases of breach is just as important. Although not an exhaustive list, at the minimum, businesses should consider the following steps when dealing with data breach.

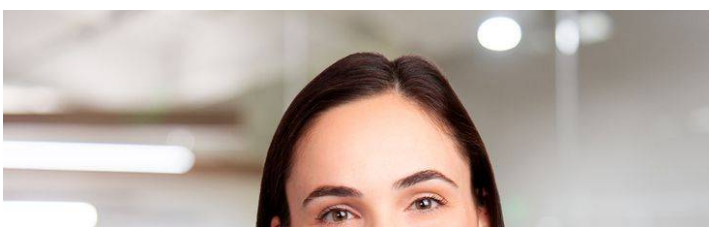
- **Stop The Breach and Take It Offline:** Take immediate action to secure the network and change network access authorization to prevent the breach from getting worse.
- **Initiate Your Incident Response Plan:** If you have an incident response plan, be sure to implement it promptly, including mobilizing your breach response team. Your protocols should include procedures to enable prompt investigation and remediation of the breach. You may also want to consider whether to notify law enforcement. Legal counsel can help you with this step.
- **Contact Your Counsel:** Legal counsel can help you analyze and comply with applicable data breach notification and other reporting obligations resulting from the breach, and also help supervise and direct outside vendors conducting investigation of the breach. Having counsel direct vendors may create privilege in the communications regarding the investigation, which can be useful if there is subsequent litigation relating to the breach.
- **Identify The Type of Information Affected:** Determine the nature of the data at issue and how it was impacted by the breach to assess what legal requirements or regulations may apply. Consult counsel when making that determination.
- **Contact Your Service Provider:** If a service provider is responsible for the breach (such as your web security company, website builder, third-party payment processor, or similar companies), review any applicable agreements to determine the obligations of the parties. If appropriate, ensure that the provider is investigating, remedying, and responding to the breach. You should also reassess their access privileges and verify that vulnerabilities were indeed remedied by the provider.

Conclusion

As technology continues to evolve, there are an increasing number of ways for data breaches to occur. The bottom line is that, regardless of your industry, you must always be prepared to adjust and revise your data security and privacy practices to stay ahead of legal obligations and defend against increasingly sophisticated cyberattacks.

If you have any questions about best practices for addressing data breach threats, please consult your Fisher Phillips attorney, the author of this Insight, or a member of our Privacy and Cyber Practice Group. To ensure you stay up to speed with the latest developments, make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

Related People



Madison Keller
Associate
617.532.6936
Email

Monica Snyder Perl
Partner
617.532.9327
Email

Service Focus

Privacy and Cyber

Counseling and Advice