



July 16, 2024

Sridhar Ramaswamy
Chief Executive Officer
Snowflake, Inc.
106 East Babcock Street
Suite 3A
Bozeman, M.T., 59715

Dear Mr. Ramaswamy,

We write demanding information regarding the series of data breaches targeting clients of Snowflake, which has led to compromise by cybercriminals of hundreds of millions of customer records and sensitive information from AT&T, Ticketmaster, and other high-profile companies.

On May 28, 2024, the cybercrime group ShinyHunters announced the sale of customer records of 560 million Ticketmaster users on a private marketplace for stolen data.¹ ShinyHunters has continued to attempt to extort Ticketmaster and sell data stolen from fans and musicians, as recently as this month offering to sell ticket information for Taylor Swift concerts and leaking tens of thousands of ‘print-at-home’ tickets for upcoming concerts.

The theft of Ticketmaster data appears to be connected with a series of breaches of client accounts of Snowflake, your cloud service designed to help companies analyze business data. In addition to Ticketmaster, other companies including Advance Auto Parts and Santander Bank have announced the theft of customer or employee information. Most recently, on July 12, 2024, AT&T announced that six months of customer data hosted on its Snowflake services were illicitly accessed, including phone call and text message records — information that can easily provide cybercriminals, spies, and stalkers a logbook of the communications and activities of AT&T customers.²

Disturbingly, the Ticketmaster and AT&T breaches appears to have been easily preventable. While Snowflake, AT&T, Ticketmaster, and other clients have avoided taking

¹ “Ticketmaster Data Breach: Hackers Selling 560 Million Users Data for \$500,000.” Hackread. <https://hackread.com/hackers-ticketmaster-data-breach-560m-users-sale/>

² “Unlawful access of customer data.” AT&T. <https://www.att.com/support/article/my-account/000102979>

direct responsibility, according to the cybersecurity firm Mandiant, it appears that the cybercrime group behind the breaches obtained companies' passwords from malware infections, including malware bundled with pirated software. Compounding this basic cybersecurity failure, the hacked accounts had often kept the same passwords for several years, failed to implement firewall access, and failed to turn on multi-factor authentication — additional basic cybersecurity failures that seemingly reflect gross negligence, particularly in light of the sensitivity of the data stolen in many of the breaches.

The recent AT&T disclosure — three months after the breach and following other announced breaches — raises concerns that we still do not know the full scope or impact of the campaign targeting Snowflake customers. Based on its assessment of stolen Snowflake passwords, Mandiant reported that 160 other organizations could have been targeted in the hacking campaign.³


Given this alarming and seemingly preventable theft of highly-sensitive customer information, we ask for your responses to the following questions by July 29, 2024:

1. Please provide a detailed accounting and timeline of all events related to the breach of Snowflake customers by the cybercrime group ShinyHunters, including the date and background on the discovery, response, and remediation of compromised accounts or disabled services.
2. What investigation has Snowflake done into the scale of targeting of its customers, and what effort has it taken to identify which companies or accounts were breached in the hacking campaign? What were the results of that investigation?
3. What notification has Snowflake provided to clients whose accounts were breached, what steps has it taken to prevent further access or theft of private information from vulnerable accounts?
4. Given that multiple accounts containing a significant amount of data were illicitly accessed, why did Snowflake not detect the breaches in time to prevent the theft of customer data?
5. Why did Snowflake not enforce multi-factor authentication and other basic cybersecurity measures for its clients, and has it made changes to its security policies and customer requirements since the breaches?

Thank you for your attention to this important matter.

³ “UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion.” Mandiant. <https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion>

Sincerely,



Richard Blumenthal
Chair
Subcommittee on Privacy, Technology,
and the Law
United States Senate



Josh Hawley
Ranking Member
Subcommittee on Privacy, Technology,
and the Law
United States Senate