



Update on a Security Incident Involving Third-Party Customer Service

 Discord
October 3, 2025

Updated: October 9, 2025

TL;DR:

- Discord recently discovered an incident where an unauthorized party compromised one of our third-party vendors.
- This was *not* a breach of Discord, but rather a breach of a third party service provider, 5CA, that we used to support our customer service efforts.
- This incident impacted a limited number of users who had communicated with our Customer Support or Trust & Safety teams.
- Of the accounts impacted globally, we have identified approximately 70,000 users that may have had government-ID photos exposed, which our vendor used to review [age-related appeals](#).
- No messages or activities were accessed beyond what users may have discussed with Customer Support or Trust & Safety agents.
- We immediately revoked the customer support provider’s access to our ticketing system and continue to investigate this matter.
- We’re working closely with law enforcement to investigate this matter.
- We are in the process of emailing the users impacted.

At Discord, protecting the privacy and security of our users is a top priority. That’s why it’s important to us that we’re transparent with them about events that impact their personal information.

Recently, we discovered an incident where an unauthorized party compromised one of Discord’s third-party customer service providers. The unauthorized party then gained access to information from a limited number of users who had contacted Discord through our Customer Support and/or Trust & Safety teams.

As soon as we became aware of this attack, we took immediate steps to address the situation. This included revoking the customer support provider’s access to our ticketing system, launching an internal investigation, engaging a leading computer forensics firm to support our investigation and remediation efforts, and engaging law enforcement.

We are in the process of contacting impacted users. If you were impacted, you will receive an email from noreply@discord.com. We will not contact you about this incident via phone – official Discord communications channels are limited to emails from noreply@discord.com.

What happened?

An unauthorized party targeted our third-party customer support services to access user data, with a view to extort a financial ransom from Discord.

What data was involved?

- The data that may have been impacted was related to our customer service system. This may include:
- Name, Discord username, email and other contact details if provided to Discord customer support
 - Limited billing information such as payment type, the last four digits of your credit card, and purchase history if associated with your account
 - IP addresses
 - Messages with our customer service agents
 - Limited corporate data (training materials, internal presentations)
 - The unauthorized party also gained access to a small number of government-ID images

If your ID may have been accessed, that will be specified in the email you receive.

What data was not involved?

- Full credit card numbers or CCV codes
- Messages or activity on Discord beyond what users may have discussed with customer support
- Passwords or authentication data

What are we doing about this?

- Discord has and will continue to take all appropriate steps in response to this situation. As standard, we will continue to frequently audit our third-party systems to ensure they meet our security and privacy standards. In addition, we have:
- Notified relevant data protection authorities.
 - Proactively engaged with law enforcement to investigate this attack.
 - Reviewed our threat detection systems and security controls for third-party support providers.

Taking next steps

Looking ahead, we recommend impacted users stay alert when receiving messages or other communication that may seem suspicious. We have service agents on hand to answer questions and provide additional support.

We take our responsibility to protect your personal data seriously and understand the inconvenience and concern this may cause.



Language

English 

Social



- Product
- [Download](#)[Nitro](#)[Status](#)[App Directory](#)

- Company
- [About](#)[Jobs](#)[Brand](#)[Newsroom](#)

- Resources
- [College](#)[Support](#)[Safety](#)[Blog](#)[StreamKit](#)[Creators](#)[Community](#)[Developers](#)[Quests](#)[Official 3rd Party Merch](#)[Feedback](#)

- Policies
- [Terms](#)[Privacy](#)[Cookie Settings](#)[Guidelines](#)[Acknowledgements](#)[Licenses](#)[Company Information](#)

