



[Recipient Name]
[Recipient Address]
[City, State, Zip]

November 24, 2025

Notice of Data Incident

Dear [First Name] [Last Name]:

You may have received an email about this incident from us on or around October 3 and we are following up with additional information.

We take the protection of your personal information seriously, so we are writing to let you know about an incident that involved your personal information. While we have not identified evidence of the misuse of this data in a manner that may cause harm to you, we are nevertheless providing you with this notice so you are aware of what happened, the measures we have taken, and the steps you can take.

What Happened?

On September 25, 2025, Discord Inc. (***We*** or ***the Company***) discovered that your data was impacted when a third party obtained unauthorized access to our customer service platform through a compromised vendor device. Upon discovery, we promptly initiated our incident response procedures, took immediate steps to address the situation, including revoking the customer support provider's access to our customer service platform, and engaged a leading digital forensics firm to assist with the investigation and remediation. The investigation revealed that the third party initially obtained unauthorized access to our customer service platform between September 20 and 22, 2025, but was successfully removed from the customer service platform on September 22, 2025.

What Information Was Involved?

The personal information that may have been accessed could include your name, certain contact information (such as address, phone number, and/or email address) that you have provided to Discord, your Discord username, date of birth, a photo of your driver's license or other state or government-issued ID if provided, limited payment information (including payment type, last four digits of your credit card, and Discord purchase or refund history if associated with your account), IP addresses, and messages and attachments sent to our Customer Support or Trust & Safety agents.

What We Are Doing.

Following the incident, the Company notified law enforcement and continues to assist in the investigation. The Company is committed to the protection of the data it handles and will continue to review its safeguards and implement appropriate measures. In addition, although we have no evidence that any personal information has been misused in a manner that could harm you, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for 12 months. This service is provided by Experian, specializing in fraud assistance and remediation services. You can find information about the service and how to enroll in Attachment A to this letter.

What You Can Do.

In addition to signing up for complimentary credit monitoring, you can also review Attachment B, which provides further information about steps you can take to protect your identity in general, should you feel it may be appropriate to do so. We also suggest that you remain vigilant when receiving emails that are unexpected, originate from unfamiliar sources, or otherwise appear suspicious, and that you confirm that the message is legitimate before downloading attachments or clicking on links.

Other Important Information.

If you have any questions, you can contact us through our dedicated support channel at <http://dis.gd/support> or privacy@discord.com and we will be happy to assist you. You can also contact 833-918-7475 for support.

Yours sincerely,

Discord Inc.
444 De Haro Street, Suite 200
San Francisco, CA 94107

ATTACHMENT A

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [##] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [##] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [##]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** [Enrollment End Date] by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by [Enrollment End Date] at [TFN] Monday – Friday, 8 am – 8 pm Central Time (excluding major U.S. holidays). Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [##]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

ATTACHMENT B

GENERAL STEPS TO TAKE TO PROTECT YOUR PERSONAL INFORMATION

- You should be vigilant against possible “phishing” communications, including from emails that appear to be (but are not) sent from a particular organization.
- Regularly review your account statements and credit history for any signs of unauthorized transactions or activity, and remain vigilant against threats of identity theft or fraud.

STEPS YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS

Ordering Free Credit Report. Please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alert. When you place a “fraud alert” on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A “security freeze” or “credit freeze” goes further than an alert and lets you restrict access to your credit report entirely. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit. A credit freeze does not affect your credit score, but you may need to lift the freeze temporarily, either for a specific time or for a specific party if you are opening a new account, applying for a job, renting an apartment or buying insurance.

To place a freeze, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, social security number and other personal information. Credit reporting agencies are required to place/remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. They can provide additional resources about preventing or remedying identity theft, including by setting up fraud alerts/security freezes and by reviewing your credit report. Fees may be required for some services.

EQUIFAX

P.O. Box 105069
Atlanta, GA 30348-5069
866-478-0027
www.equifax.com/personal/credit-report-services

EXPERIAN

P.O. Box 9554
Allen, TX 75013
888-397-3742
www.experian.com/freeze

TRANSUNION

P.O. Box 160
Woodlyn, PA 19094
800-916-8800
freeze.transunion.com

INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission. You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

1-877-ID-THEFT (877-438-4338)
www.identitytheft.gov

PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. Your major rights under the FCRA include:

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.

You can obtain more information, including information regarding additional rights at www.ftc.gov/credit, or at https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf.

IF YOU ARE A RESIDENT OF CERTAIN STATES, YOU HAVE ADDITIONAL RIGHTS:

District of Columbia

You can reach the Attorney General of the District of Columbia at:

400 6th Street NW
Washington, D.C. 20001
Phone: (202) 727-3400
<https://oag.dc.gov/>

Maryland

You may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an email to idtheft@oag.statemd.us, or calling 1-410-576-6491. You can call the Maryland Attorney General toll-free at 1-888-743-0023. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General by mail at:

Identity Theft Unit
Office of the Attorney General
200 St. Paul Place
25th Floor
Baltimore, MD 21202

Massachusetts

Under Massachusetts state law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

New York

For more information, you may visit the following websites: New York Department of State Division of Consumer Protection at www.dos.ny.gov/consumer-protection, or NYS Attorney General at www.ag.ny.gov. For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at <https://dos.nysits.acsitefactory.com/consumer-protection>.

North Carolina

You can reach the Attorney General of the State of North Carolina by mail at:

9001 Mail Service Center
Raleigh, NC 27699-9001
+1 (919) 716-6400
<http://www.ncdoj.gov>

Oregon

You can reach the Attorney General of the State of Oregon at 1-877-877-9392 or by mail at help@oregonconsumer.gov.

Rhode Island

You have the right to file or obtain a police report in regard to this incident. You can reach the Attorney General of the State of Rhode Island by phone at (401) 274-4400 or online at www.riag.ri.gov.