

■

On June 16, 2024, Gemini Trust Company, LLC (“Gemini”) became aware of a security incident involving one of our third-party ACH banking partners. Specifically, an unauthorized actor gained access to an internal collaboration tool on the banking partner’s system, which may have resulted in the potential disclosure of certain transactional data between June 3 and June 7, 2024. For some Gemini customers, transactional information including customer name, as well as the bank account number and routing number the customer provided to Gemini for transferring funds, may have been affected. Gemini’s internal systems were not affected.

Since then, the banking partner has launched an investigation, implemented measures to contain the incident, and engaged outside forensic experts. The banking partner has also notified law enforcement and its regulator of the incident. Gemini provided notice to the 233 affected Maryland residents by email and intends to provide notice by US Mail in the days ahead. An exemplar of that notice is attached. Gemini will provide updated notification to this office if additional information becomes available.

--
Betsy Sochar
Senior Corporate Counsel
betsy.sochar@gemini.com





Fwd: Important Information Regarding Gemini's Banking Partner

1 message

Wed, Jun 26, 2024 at 10:38 AM

to: [REDACTED]

----- Forwarded message -----

From: **Gemini** <hello@news.gemini.com>

Date: Tue, Jun 25, 2024 at 2:02 PM

Subject: Important Information Regarding Gemini's Banking Partner

To: [REDACTED]



Hi [REDACTED],

We are writing to inform you that one of Gemini's third-party ACH banking partners recently became aware of a security incident involving one of its service providers. Gemini partners with this bank to facilitate the transfer of funds from your Gemini wallet to your bank account. In order to perform this function for you, the banking partner processes certain Gemini customer data.

What Happened

Our banking partner has notified us that a subset of some Gemini customers' banking information was potentially impacted as part of the incident. Specifically, an unauthorized actor gained access to an internal collaboration tool on the bank partner's system, which may have resulted in the potential disclosure of certain transactional data between June 3 and June 7, 2024. Unfortunately, information including your name, as well as the bank account number and routing number you provided to Gemini for transferring funds, may have been affected.

Please note that no other sensitive information, such as date of birth, address, social security number, email address, phone number, username, or password, was part of the incident. No Gemini account information or systems were impacted as a result of this third-party incident, and the incident did not affect the security of any Gemini systems.

What We Are Doing

Upon learning of the incident, the banking partner immediately launched an investigation and implemented measures to contain the incident. In addition, it engaged outside forensic experts to conduct an investigation, which is ongoing. It also notified law enforcement of the incident.

What Can You Do

We wanted to make you aware of this incident as soon as possible so that you can take appropriate next steps. We encourage you to take the following actions:

- Contact your bank to inquire about steps you can take to help protect your account, including obtaining a new account number.
- Enable Multi-Factor Authentication on the bank account you provided to Gemini.
- Closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity.
- Stay vigilant and be aware of scams that may operate based on knowledge of your financial data.

More Information

Please see below for additional steps you can take to further protect your information. We are committed to providing relevant information as quickly as possible. We appreciate your patience and support as we continue working around the clock with our partner to resolve this issue. Please reach out to our support team [here](#) with any questions.

Gemini Security Team

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can access the request form at <https://www.annualcreditreport.com/requestReport/landingPage.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 www.experian.com 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 888-4213 www.transunion.com 2 Baldwin Place P.O. Box 1000 Chester, PA 19022
---	--	--

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <https://www.annualcreditreport.com/index.action>.

Consider Placing a Security Freeze on Your Credit File

In some U.S. states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent.

As a result, using a security freeze may interfere with or delay your ability to obtain credit. Additionally, if you request a security freeze from a consumer reporting agency, there may be a fee up to \$10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to \$5).

In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, a recent utility bill, bank statement, or insurance statement, and, if you are a victim of identity theft, a copy of the police report, investigative report, or complaint to a law enforcement agency. You must separately place a security freeze on your credit file with each credit reporting agency by sending a written request to:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000
---	---	---



gemini.com

Gemini Trust Company, LLC
(d/b/a Gemini Exchange, LLC in AZ, CA, DE, FL, ID, IL, KS, KY, MA, MI, MN, NC, ND, NM, OH, OR,
SC, SD, UT, and VA; d/b/a Gemini Exchange in AK and WA)
[600 Third Avenue, 2nd Floor](#)
New York, NY 10016
+1 (866) 240-5113

[Unsubscribe from this list](#)

Copyright 2024 Gemini Trust Company, LLC . All rights reserved.