



Notice of Recent Vendor Incident



7/15/24

Hello Coinbase Customer,

We are writing to notify you of an incident that occurred on the systems of one of our vendors (a third party bank), which may have affected the security of some of your information. Importantly, Coinbase's systems and your Coinbase account were not compromised.

We take the privacy and security of your personal information extremely seriously and regret that this incident occurred. We are sharing available details and offering you recommended resources and actions you can take to further protect your information and accounts.

What Happened

Coinbase uses a third party bank to process payments transactions. The bank recently notified us of a security incident at the bank that could potentially have impacted a small amount of Coinbase data. Since learning of the incident, Coinbase has been coordinating with the bank as the bank undertakes its forensic investigation. Their investigation has revealed that a file containing transaction data, including some of your personal information, was mistakenly uploaded to an external location from which an unauthorized actor may have accessed it. The bank's investigation to date has not reflected that the file was in fact accessed by an unauthorized third party, nor has the investigation identified any indication of identity theft or fraud in relation to this incident. Again, this incident only impacted the bank's systems.

What Information Was Involved

The personal information included in the file included your name, bank account number, and bank routing number.

What We Are Doing

Since learning of the incident, Coinbase has been working closely with the bank as it undertakes a forensic investigation. We understand that the bank has also contacted law enforcement authorities. While the bank has identified no evidence of identity theft or fraud involving your personal information, we are contacting you out of an abundance of caution to offer support and provide resources.

What You Can Do

Please review the attached *Steps You Can Take to Help Protect Your Information*, which provides guidance on how to protect your identity and accounts, by doing things like monitoring your accounts and

implementing a free 'credit freeze' if you discover suspicious activity. It is also always good practice to be vigilant against identity theft and fraud by reviewing account statements across all of your financial accounts on a regular basis, monitoring any available credit reports for unauthorized or suspicious activity, and contacting your bank if you identify any suspicious activity on your account. Additionally, you should also take care in response to any email, telephone or other contacts that ask for personal or sensitive information (e.g., phishing). Finally, you should never open links or attachments sent from untrusted sources. Please review this [blog post](#) for more resources and information about how to protect your account.

For More Information

We are fully committed to protecting your information, and deeply regret that this incident occurred. If you have questions or concerns regarding this incident, please contact us at dpo@coinbase.com

Regards,
Coinbase Support

Steps You Can Take to Help Protect Your Information

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file with the credit reporting bureau. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

If you discover any suspicious items on your credit reports or from the fraud alert and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, free of charge, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to

federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information.

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency filed by you concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/	https://www.experian.com/	https://www.transunion.com/
1-888-378-4329	1-888-397-3742	1-800-916-8800
Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	Experian Fraud Center P.O. Box 9554 Allen, TX 75013	TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016
Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud (this letter alone does not suggest that you are a victim of or at risk of identity theft or fraud). Please note that in order for you to file a police report for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Florida residents, the Florida Attorney General can be contacted at PL-01, The Capitol, Tallahassee, FL 32399-1050, <https://www.myfloridalegal.com/>, 850-414-3300.

For California residents, the California Office of Privacy Protection (www.oag.ca.gov/privacy) may be contacted for additional information on protection against identity theft. The California Attorney General can be contacted at 1300 I Street, Sacramento, CA 95814, www.oag.ca.gov, 800-952-5225.

For Maryland residents, the Maryland Attorney General can be contacted at 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, 410-576-6300.

For North Carolina residents, the North Carolina Attorney General can be contacted at Consumer Protection Division, Mail Service Center 9001, Raleigh, NC 27699, www.ncdoj.gov, 877-566-7226.

For Iowa residents, the Iowa Attorney General can be contacted at 1305 E. Walnut Street, Des Moines, Iowa 50319, <https://www.iowaattorneygeneral.gov/>, 515-281-5926 or 888-777-4590.

For New York residents, the New York Attorney General may be contacted at the Capital, Albany, NY 12224, www.ag.ny.gov, 800-771-7755.

For Oregon residents, the Oregon Attorney General may be reached at 1162 Court Street NE, Salem, OR 97301, <https://www.doj.state.or.us>, 503-378-4400.

For South Carolina residents, the South Carolina Department of Consumer Affairs may be reached at 293 Greystone Blvd., Ste. 400, Columbia, SC 29210, www.consumer.sc.gov, 800-922-1594.

For Kentucky residents, the Kentucky Attorney General may be contacted at 700 Capital Avenue, Suite 118, Frankfurt, KY 40601, www.ag.ky.gov, 502-696-5300.

For Massachusetts residents, You have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-2200, <https://www.mass.gov/contact-the-attorney-generals-office>.