Appendix A

[Template Individual Notification Letter]

[NAME]

[ADDRESS]

Subject: **Notice of Data Breach**

Dear [NAME]:

At Coinbase, we actively monitor our systems to ensure customer information is only accessed when necessary and in accordance with our strict security standards. During this monitoring, we detected that a small number of individuals performing services for Coinbase accessed customer information and may have shared it with a third party. This included information related to your account. We published a blog today providing additional details.

What Happened?

We discovered that a small number of individuals, performing services for Coinbase at our overseas retail support locations, improperly accessed customer information. This included information related to your account.

What Information is Involved?

This information did not include your password, seed phrase, private keys, or any other information that would allow someone to directly access your account or your funds and Coinbase Prime was untouched. But it could have included information like:

- Personal identifiers (e.g., name, date of birth, masked social security numbers (last 4 digits), masked bank account numbers and some bank account identifiers, address, phone number, email address)
- Images of Government identification information (e.g., driver's license number, passport number, national identity card number)
- Account information (e.g., transaction history, balance, transfers, date you opened your account)

Attackers seek out this information because they want to conduct social engineering attacks, using this information to appear credible to try and convince victims to move their funds. This week—after we fired the individuals involved and added even more stringent security measures—a third party claimed they had access to our customer data, and attempted to extort a $20 million payment.

What We're Doing

Our teams have been tirelessly working to respond to this issue and protect our customers. This includes:

- **Making Customers Whole—**We will reimburse eligible retail customers who were socially engineered into sending funds to the threat actor as a direct result of this incident after we complete our review to confirm the facts.
- **Extra Customer Safeguards**—Flagged accounts now require additional ID checks on large withdrawals and include mandatory scam-awareness prompts.
- **Tracing Stolen Funds—**Working with industry partners, we've tagged the attackers' addresses so the authorities can track and work to recover assets.
- **$20 Million Reward Fund—**Instead of paying the $20 million ransom, we're creating a fund in the same amount to reward information leading to the attacker's arrest and conviction. Email security@coinbase.com.
- **Working with Law Enforcement—**Individuals involved were fired on the spot; we've referred the case to U.S. and international agencies and are pressing for criminal charges.
- **Securing Support Operations—**Opening a new support hub in the U.S. and adding stronger security controls and monitoring across all locations.
- **Hardening Defenses**—We have increased our investment in insider-threat detection, automated response, and simulating similar security threats to find failure points in any internal system.
- **Keeping You Informed**—We are further educating our customers so they can protect themselves against fraud, including through our Consumer Protection series, and transparently providing our customers with information.
- **Credit Monitoring and Identity Theft Protection Services**—We are offering you free one-year credit monitoring and identity protection services provided by IDX. The services include credit monitoring, a $1,000,000 insurance reimbursement policy and identity restoration, in the event that you are a victim of identity theft, and dark web monitoring to identify if any of your information is made available through illegal online forums. To activate the services, please follow the instructions included in the attached "How To Protect Your Information."

What You Can Do

Be hyper vigilant. If you suspect something, say something and reach out to our support in-app or security@coinbase.com.

Remember:

- Coinbase will ***never*** call to ask for your login credentials, API key, seed phrase or two-factor authentication code
- Coinbase will ***never*** call you and instruct you on the phone to transfer or move your assets or funds to a specific destination

- Coinbase will ***never*** ask you to contact an unknown number to reach us

If someone calls or texts you claiming to be from Coinbase and requests your account information or asks you to transfer assets, do not do it - it is a scam.

Here are additional steps you can take to further protect your information and your account:

- **Expect Imposters—**Remain cautious of unsolicited calls, text messages, or emails requesting sensitive information or urging immediate action (i.e., phishing and/or smishing attempts). Never click on unfamiliar links and avoid providing personal details over the phone.
- **Enable Strong 2FA**—Hardware keys are best.
- **Turn on Withdrawal Allow Listing**—Only permit transfers to wallets that you are confident you fully control and where the seed phrase is secure and was not provided or shared with anyone.
- **Lock First, Ask Questions Later**—If something feels off, lock your account in-app and email security@coinbase.com.
- **Hang Up**—If someone calls you asking you to manipulate or transfer your funds in any way and for any reason.
- **Review our Security Tips**—Find the latest best practices at coinbase.com/security and stay up to date on avoiding social engineering scams.
- **Enroll in credit monitoring services**—Follow the instructions in the attached "How To Protect Your Information" to take advantage of the free credit monitoring and identity protection services we offer.

Crypto adoption depends on trust. To the customers affected, we're sorry for the worry and inconvenience this incident caused. If you have any questions regarding the above or need support, please call our dedicated call center at [NUMBER] between Monday to Friday, 9 am to 9 pm Eastern Time.

Thank you for being a valued part of Coinbase.

How To Protect Your Information

Enroll in IDX Credit Monitoring and Identity Protection Services

Go to [URL] and follow the instructions to enroll in the identity protection services being provided by IDX. Your person Enrollment Code is provided at the top of this letter. Please note the deadline to enroll is [DATE].

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 services, 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 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 District of Columbia residents, the District of Columbia Attorney General can be contacted at 400 6th Street NW, Washington, DC 20001, www.oag.dc.gov, 202-727-3400.

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

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.

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 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 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 Rhode Island residents, the Rhode Island Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400. You have the right to file or obtain a police report regarding this incident.

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 New Mexico residents, you have the right to obtain a police report regarding 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. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting

Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf, or by writing to the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.