Bitcoin Depot, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

Bitcoin Depot
2870 Peachtree Rd #327
Atlanta, GA 30305
678-435-9604
Bitcoindepot.com

P
<<First name>> <<Last name>>
<<Address 1>>
<<Address 2>>

July 7, 2025

NOTICE OF DATA BREACH

Dear <<First name>> <<Last name>>:

We are writing to inform you of a data security incident that may have impacted some of your personal information. Bitcoin Depot, Inc. ("Bitcoin Depot") takes data security very seriously, and we sincerely regret that this occurred. Importantly, we are not aware of misuse of any customer information. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?
On June 23, 2024, Bitcoin Depot, Inc. detected unusual activity on its information systems and immediately commenced an investigation, which included engaging third-party incident response experts to assist in determining the extent of any unauthorized activity. On July 18, 2024, the investigation was complete, and we identified your personal information contained within documents related to certain of our customers that the unauthorized individual obtained. Unfortunately, we were not able to inform you sooner due to an ongoing investigation. Federal law enforcement requested that Bitcoin Depot wait to provide you notice until after they completed the investigation. Law enforcement advised Bitcoin Depot on June 13, 2025, that their investigation was complete.

What Information was Involved?
The incident involved your name, phone number, and driver's license number and may have included your address, date of birth, and/or email.

What We Are Doing.
Bitcoin Depot is cooperating fully with law enforcement in relation to this incident. We take the security of all information in our systems very seriously, and we want to assure you that we've already taken steps to prevent a reoccurrence by enhancing security measures and security monitoring and increasing company awareness of data security protection.

What You Can Do
We recommend that you review the additional information enclosed, which contains important steps you can take to protect your personal information.

For More Information
Representatives are available to assist you with questions about this incident between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays for 90 days from the date of this letter. Please call the help line at 1-833-367-3704.

Protecting your information is important to us. We appreciate your patience and understanding.

Sincerely,

Bitcoin Depot, Inc.

Additional Important Information

Monitoring: You should always remain vigilant for incidents of fraud and identity theft, especially during the next 12-24 months, by reviewing financial account statements and monitoring your credit reports for suspicious or unusual activity and immediately report any suspicious activity or incidents of identity theft. You have the right to obtain or file a police report. You can contact the Federal Trade Commission (FTC) for more information on preventing identity theft. We encourage you to report any incidents of identity theft to the FTC.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.identitytheft.gov

Credit Reports: You may obtain a copy of your credit report, for free, whether or not you suspect any unauthorized activity on your account, from each of the three nationwide credit reporting agencies. To order your 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 Alerts: You have the right to place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. To place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be needed to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348-5788	Allen, TX 75013-9544	Woodlyn, PA 19094
www.equifax.com/personal/credit-report-services/credit-freeze/	http://www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
1-866-478-0027	1-888-397-3742	1-800-916-8800

For residents of *Iowa* and *Oregon*: You are advised to report any suspected identity theft to law enforcement or to the state Attorney General and Federal Trade Commission.

For residents of *New Mexico:* You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:
You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the FTC about fraud alerts, security freezes, and steps you can take to prevent identity theft. There were 45 Rhode Island residents notified in this incident.

District of Columbia Attorney General	**Maryland Office of Attorney General**	**New York Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
400 6th Street NW	200 St. Paul Pl	120 Broadway, 3rd Fl	9001 Mail Service Ctr	150 South Main St
Washington, DC 20001	Baltimore, MD 21202	New York, NY 10271	Raleigh, NC 27699	Providence RI 02903
1-202-442-9828	1-888-743-0023	1-800-771-7755	1-877-566-7226	1-401-274-4400
www.oag.dc.gov	https://www.marylandattorneygeneral.gov/	www.ag.ny.gov	https://ncdoj.gov/	www.riag.ri.gov