[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[CREDIT MONITORING PROMOTION CODE]
[DATE]

NOTICE OF DATA BREACH

Dear [INDIVIDUAL NAME]:

We value your business and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your information. Some of this information may be considered "personal information" under the laws in your jurisdiction. However, in the interests of being transparent with our valued customers, we are providing this notice to all of our customers whom we believe may have been affected by this incident.

WHAT HAPPENED?

Between August 2026 and October 23, 2026, we discovered that an unauthorized third party accessed the server that runs our web-based File Manager at files.dreamhost.com. The unauthorized third party exploited a vulnerability in that software and was able to access the FTP/SFTP usernames and passwords of individuals who logged into this File Manager between approximately August 2026 and October 23, 2026. The unauthorized third party was also able to reach certain webmail systems, which may have exposed the session information (the data that keeps a user signed in, including session credentials) of a limited number of webmail users. We believe this as a deliberate attack, and our team worked around the clock to contain it.

WHAT INFORMATION WAS INVOLVED?

The data accessed may have included personal information such as your username and password used to access the File Manager or your webmail. Other information such as the contents of your email and files in the FTP/SFTP server may have also been accessed.

Based on our investigation to date, we have found no evidence that the unauthorized third party accessed control panel login information or customer billing details. DreamHost does not store full payment card numbers. Payments through payment cards are handled by a third-party payment processor, and we retain only a secure token representing the payment card information that cannot be used to make purchases elsewhere. However, our investigation is ongoing, and if we discover any significant additional information, we will update this post.

WHAT WE ARE DOING

After the incident was discovered, we took steps to stop the unauthorized third party's access, to address the exploited vulnerability, and remediate the impacts of the unauthorized access. DreamHost is conducting a thorough review of the potentially affected computer systems and will notify you if there are any significant developments. We also terminated active sessions of users who may have been affected and reset their password. DreamHost has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy and security of our users and their information.

DreamHost also is working closely with outside legal advisors and security and forensics experts to ensure the incident is properly addressed.

WHAT YOU CAN DO

Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information) for further information on steps you can take to protect your information, and how to receive free identity theft protection services for one year]

FOR MORE INFORMATION

For further information and assistance, visit https://www.dreamhost.com/support/#form and select "Account security" as your topic. You should also see the attached information regarding steps that you may take and how to get free credit monitoring for one year. Please note that DreamHost will never ask you for your password by email.

Sincerely,

The DreamHost 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 website files for any unexpected changes and/or review your email accounts carefully for any changes to your account settings, such as forwarding rules and filters, for any unrecognized changes. If you detect any suspicious activity on an account, you should promptly notify us. 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). You should also consider the contents of your emails or files to determine if any other accounts should be reviewed for unexpected activity. We recommend that you also immediately change the password on any and all other accounts that may have used the same or similar username and password and review such accounts for any suspicious activity.

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

If your username and password may have been used for any other financial account or if the contents of your email or website files may contain information that could be used to access a financial account, 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/requestForm.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	Experian	TransUnion	Innovis
(866) 349-5191	(888) 397-3742	(800) 888-4213	(800) 540-2505
www.equifax.com	www.experian.com	www.transunion.com	www.innovis.com
P.O. Box 740241 Atlanta, GA 30374	P.O. Box 4500 Allen, TX 75013	2 Baldwin Place P.O. Box 1000 Chester, PA 19016	PO Box 1689 Pittsburgh, PA 15230-1689

Consider Placing a Fraud Alert on Your Credit Report

If you used the same username and password for other sites or if the contents of your email or website files may contain information that could be used to access another account, you may want to consider placing a fraud alert on your credit report. You have the right to place an initial or extended “fraud alert” on your file at no cost by contacting any of the nationwide credit reporting

agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, https://www.innovis.com/personal/fraudActiveDutyAlerts, 1-800-540-2505

Credit Report Monitoring/Identity Theft Protection Services

In addition, DreamHost has arranged with Equifax to provide you with identity theft protection services for one year, at no cost to you. More information about these services are attached.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

- **For California Residents**: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.
- **Iowa residents:** You are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, tel.: (515) 281-5926 or (888) 777-4590.

- **For Maryland Residents**: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx, Telephone: 1-410-576-6491 or 1-888-743-0023.

- **New Mexico residents:** Consumers have rights pursuant to the Fair Credit Reporting Act ("**FCRA**"), such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their rights pursuant to the FCRA by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

- **For New York Residents**: You may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General at https://ag.ny.gov/ or by calling 1-800-771-7755; the New York State Police at http://troopers.ny.gov/ or by calling 1-518-457-6721; and/or the New York Department of State at https://www.dos.ny.gov or by calling 1-800-697-1220.

- **For North Carolina Residents**: You may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, by calling 1-877-566-7226, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

- **Rhode Island residents:** You may contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; http://www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. There are approximately <<RI#>> Rhode Island residents who may be impacted by this event.

- **Vermont residents:** If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-828-3171.

- **For Oregon Residents**: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

OTHER IMPORTANT INFORMATION

Security Freeze

In some US states, you have the right to place, lift, or remove a "security freeze" on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze.

You must place your request for a freeze separately with each of the three (3) consumer reporting agencies listed below. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit- freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or up to three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through

a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

<First Name> <Last Name>
Enter your Activation Code: **<Activation Code>**
Enrollment Deadline: **<Expiration Date>**

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **<Activation Code>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".

   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

   Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.

   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.

   Click "View My Product" to access the product features.

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.* [2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.* [3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com* [4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*