

Sample Individual Notification Letter

Subject line of email: Notice of Security Incident Affecting Your GoDaddy Managed WordPress Service

Dear <name>:

We are writing to inform you of a security incident impacting your GoDaddy Managed WordPress hosting service.

On November 17, we identified suspicious activity in our WordPress hosting environment and immediately began an investigation with the help of a third-party IT forensics firm and have contacted law enforcement. Our investigation is ongoing, but we have determined that, on or about September 6, 2021, an unauthorized third party gained access to certain authentication information for administrative services, specifically, your customer number and email address associated with your account; your WordPress Admin login set at inception; and your sFTP and database usernames and passwords. What this means is the unauthorized party could have obtained the ability to access your Managed WordPress service and make changes to it, including to alter your website and the content stored on it. The exposure of your email address may also present a heightened risk of phishing attacks.

We are taking several steps to protect you and your data. First, we have blocked the unauthorized third party from our systems.

Second, we have rotated your WordPress Admin login credentials, sFTP password and your database password. Your website is still up and running, but you won't be able to edit content until you reset your passwords.

Here are the instructions on how to reset each password:

- WordPress Admin Login, please visit: <https://www.godaddy.com/help/a-26916>.
- sFTP or data password, please visit: <https://www.godaddy.com/help/a-40804>.
- WordPress database password, please visit: <https://www.godaddy.com/help/a-24573>.

If you use the same password for other accounts, we recommend you change your password to those accounts and adopt data security best practices, such as choosing a strong unique password, regularly changing it, and enabling multi-factor authentication where available. We also recommend that you remain vigilant for potentially fraudulent communications sent to your email address purporting to be from GoDaddy or other third parties.

Finally, because the private key of your existing Managed WordPress SSL certificate was exposed, the certificate will need to be revoked. We are in the process of installing a free DV SSL certificate on your website for one year to minimize potential site downtime.

If you would like to continue using your existing SSL certificate product, please follow the directions below to rekey a new certificate: <https://www.godaddy.com/help/rekey-my-certificate-4976>.

If you have any other questions, or you need further assistance, please call 480-505-8870.

For residents living in California, Colorado, Delaware, Illinois, New York, New Jersey, Oregon, Vermont, Washington, and Wyoming, please visit <https://www.godaddy.com/help/a-41004> for additional resources that describe additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Thank you,

Demetrius Comes

Chief Information Security Officer