



Jason Cherry
2029 Century Park East
Suite 1100
Los Angeles, California 90067
jcherry@constangy.com
Direct: 207.745.1397

December 18, 2023

VIA ELECTRONIC SUBMISSION

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete LLP (“Constangy”) represents Gnome, Inc. dba Gnome Landscapes (“Gnome”) based in Falmouth, Maine, in conjunction with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maine data breach notification statute.

1. Nature of the Security Incident

On October 23, 2023, Gnome discovered unusual activity in its digital environment. Following discovery, it immediately took steps to secure the network and engaged a dedicated team of external cybersecurity experts to assist in responding to and investigating the incident. As a result of the investigation, Gnome learned that an unauthorized actor acquired certain files and data stored within its systems. Upon learning this, Gnome launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, Gnome confirmed on December 14, 2023, that personal information was contained in the affected data. Since that time, Gnome has been working diligently to gather contact information and preparing to provide individual notice.

2. Type of Information and Number of Maine Residents Notified

The data sets potentially acquired by the malicious actor(s) responsible for this incident included individuals’ names and Social Security numbers. On December 18, 2023, Gnome notified 39 Maine residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

Gnome has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Gnome

has offered individuals 12 months of complimentary services through IDX, a Zero Fox Company, which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services, along with access to a call center for support for 90 days.

4. Contact Information

Gnome remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at jcherry@constangy.com.

Very truly yours,

Jason Cherry of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl: Sample Adult Consumer Notification Letter




<<Sample>>
<<Address>>

<<Date>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:
<https://app.idx.us/account-creation/protect>

Notice of Data Breach

Dear <<Sample>>:

We are writing to inform you of a recent data security incident experienced by Gnome, Inc. dba Gnome Landscapes (“Gnome”) that may have involved your personal information. Please read carefully as this letter contains background information about the incident, the type of information involved, and steps you can take to protect your information.

What Happened? On October 23, 2022, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, we confirmed on December 14, 2023, that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information Was Involved? Following our review of the contents of the impacted data, on December 14, 2023, we determined that your name and Social Security number were included. We emphasize that we have no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as we discovered this incident, we took measures to further secure the network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

Out of an abundance of caution, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include 12 months credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time. Please note the deadline to enroll is November 1, 2024. We also recommend that you review the guidance included with this letter about how to protect your information.

For More Information. If you have any questions about this letter, please call 1-800-939-4170 Monday through Friday from 9:00 a.m. – 9:00 p.m. Eastern Time.

The privacy and protection of personal and protected health information is a top priority for Gnome, which deeply regrets any inconvenience or concern this incident may cause.

Sincerely,
Gnome, Inc. dba Gnome Landscapes

ADDITIONAL 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 account statements and monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Copy of Credit Report: You may 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 print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary proof. An extended fraud alert is also free and will stay on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. Military members may also place an Active-Duty Military Fraud Alert on their credit reports while deployed. An Active-Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment.

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit.

You must separately place a security freeze on your credit file with each credit reporting agency. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the Federal Trade Commission identified above. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state attorney general about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the attorney general in your state.

Additional information:

District of Columbia: The Office of the Attorney General for the District of Columbia can be reached at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov

California: California Attorney General can be reached at: 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; <http://oag.ca.gov/>

Massachusetts: Massachusetts Attorney General can be reached at: 1 Ashburton PI Boston, MA 02108; 617-727-8400; <https://www.mass.gov/orgs/office-of-the-attorney-general>

Maine: Maine Attorney General can be reached at: 6 State House Station Augusta, ME 04333; 207-626-8800; <https://www.maine.gov/ag/>

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; <https://ag.ny.gov/>

Rhode Island: Rhode Island Attorney General can be reached at: 150 South Main Street Providence, RI 02903, <http://www.riag.ri.gov>.

Texas: Texas Attorney General can be reached at: 300 W. 15th Street, Austin, Texas 78701; 800-621-0508; texasattorneygeneral.gov/consumer-protection/

Vermont: Vermont Attorney General's Office can be reached at: 109 State Street, Montpelier, VT 05609; 802-828-3171; ago.info@vermont.gov