

December 5, 2024

VIA REGULAR MAIL

Maryland Office of the Attorney General
Attn: Data Breach Notification
200 St. Paul Place
Baltimore, MD 21202



Re: Notice of Data Security Incident

To Whom It May Concern,

Brown Rudnick LLP is legal counsel for Generator Hostels Limited, 27-29 Glasshouse Street, London W1B 5DF United Kingdom ("Generator"), in connection with a data security incident. We write to notify you of the incident in accordance with Maryland's data breach notification statute, Md. Code Com. Law § 14-3501 *et seq.*

1. Nature of the Incident

The earliest evidence of the incident is February 7, 2024, when a bad actor accessed the Microsoft 365 email account of a Generator employee ("Employee 1"). The bad actor accessed the account intermittently until April 23, 2024, when the password was changed. Thereafter, Generator's vendor ("Kroll") was performing a technical and financial audit, which included reviewing Generator's log records, when the unauthorized access was first identified. An application programming interface ("API") was utilized by the bad actor to access attachments in the Employee 1 account, which may have allowed files to be downloaded, but Kroll was unable to determine if any download/exfiltration actually occurred. Kroll was unable to determine the actual date of the Employee 1 incident because the log files before February 7, 2024 had been destroyed in accordance with Generator's standard practice.

As part of the forensic investigation that followed detection of the incident, Kroll also identified unauthorized logins by one of the same flagged IP addresses (that accessed the Employee 1 account) for the email account of another Generator employee ("Employee 2") beginning on February 23, 2024. Similar to the Employee 1 incident, the bad actor accessed this account from time to time until April 29, 2024, when the password for Employee 2's account was changed. There are no indications that an API was used with this account, or that any data was downloaded or exfiltrated from the Employee 2 account.

Based on Kroll's analysis, it is believed that the bad actor used a spoofed email domain based on the domain of a legitimate vendor of Generator, and once the bad actor gained access to the Employee 1 account, it created three (3) email rules to hide emails from the legitimate domain.

2. Notice to Maryland Residents

In total, thirty (30) Maryland residents were affected by this breach. The information involved in the incident includes the name, physical address, and social security number of individuals. The affected individuals will receive a notice of the incident and providing steps they can take to protect their information. A sample of the notification letter is attached. The notification letters will be sent via USPS Mail, or by email if the mailing address of the affected individual is not available.

3. Additional Measures Taken to Address the Incident

Generator has implemented the following steps after the incident: changing the passwords of the affected accounts; implementing multifactor authentication for the Microsoft 365 accounts of its employees; and removing the mailbox rules.

4. Contact Information

Generator is dedicated to protecting the personal information in its control. Our role in this matter requires us to state that nothing included or omitted in this letter, or the enclosed documents, is intended to acknowledge the violation of any law or regulation. We look forward to working with you to address these matters in more detail. Should you have any questions regarding this notification or other aspects of the incident, please contact me at (202) 536-1747 or at MRichardson@brownrudnick.com.

Sincerely,

BROWN RUDNICK LLP
601 Thirteenth Street NW
Washington, D.C. 20005

Generator Hostels Limited

27-29 Glasshouse Street
London
W1B 5DF United Kingdom

Date: December 5, 2024

NOTICE OF DATA BREACH

What Happened?

In the spring of 2024, we identified that an unauthorized (and unknown) person gained access to the email account of two of our employees by using a deceptive email address. We determined that the unauthorized access lasted from February 7, 2024 until April 29, 2024, when the affected employee's account password was changed. It is possible the access began before February 7, but our records only went back as far as that date. There is no evidence that any files were downloaded by this unauthorized person.

What Information Was Involved?

Your name, mailing address, and social security number were involved in this data breach.

What We Are Doing.

Since becoming aware of the breach, we have taken the following steps to ensure that such an incident does not happen again: changed the passwords of the affected accounts; and enabled multifactor authentication for all employee accounts.

What You Can Do.

Stay vigilant and alert for phishing attempts that attempt to impersonate the tone, imagery, and branding of legitimate Generator attempts to contact you. We will never call you and ask for your personal information. Enable Two-Factor Authentication for all your accounts. Keep in mind that Generator will never ask you to share your any password or two-factor authentication. Monitor your account statements and free credit reports (typically offered annually by major consumer reporting agencies). You can also obtain information on preventing identity theft from the regulatory sources provided below, including, but not limited to, how to register and obtain fraud alerts and security freezes at no charge.

Other Important Information

While we genuinely do not believe there is a risk of harm to any of our customers because of this breach, below please find the contact information for relevant consumer reporting agencies and federal and state-based regulators who can provide you with additional information and resources to better avoid any further incidents occurring. Please note that the issuance of this notice has not been delayed by any law enforcement

investigation.

Major Consumer Reporting Agencies

Equifax

1550 Peachtree Street N.W.
Atlanta, Georgia 30309
<https://www.equifax.com/personal/contact-us/>
Toll Free: 1-888-378-4329

Experian

475 Anton Blvd.
Costa Mesa, California 92626
<https://www.experian.com/help/>
Toll Free: 1-888-397-3742

TransUnion

555 West Adams Street
Chicago, Illinois 60661
<https://www.transunion.com/customer-support/contact-us-consumers?atvy=%7B%22201363%22%3A%22Experience+B%22%7D>
Toll Free: 1-888-806-1627

Federal Trade Commission

Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580
<https://www.ftc.gov/about-ftc/bureaus-offices/bureau-consumer-protection/about-bureau-consumer-protection>
Toll Free: 1-877-382-4357

For More Information. Our contact information is above, but you can learn more about the breach by calling Cyberscout (toll-free) at 1-800-405-6108.