Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Name 1>>
<<Name 2>>
<<Company>>
<<Address 1>>
<<Address 2>>
<City>, <State> <ZIP>

<<Maildate>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

On behalf of the GreenWaste family of companies, we are writing to inform you of a data-security incident that involved your personal information. We want to make you aware of this situation, inform you of the steps we have taken, and provide you an opportunity to enroll in complimentary credit monitoring.

WHAT HAPPENED

On November 27, 2023, we identified suspicious activity on our network systems. We took immediate steps to secure our network systems and to investigate the incident. We subsequently determined that an unauthorized third party gained access to a portion of our computer network that contained files with personal information. Based on our investigation, we believe the unauthorized access occurred from November 22 to 27, 2023. Once we identified the affected files, we promptly engaged a data-review firm to determine what information was contained in those files. We received the results of that review on February 27, 2024. We have been working since then to identify the affected individuals and the correct addresses for them.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that some combination of the following types of personal information related to you may have been impacted: full name, date of birth, driver's license number, Social Security number, financial-account information, health-insurance information, and/or limited medical information (such as COVID test results and vaccination status).

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures reduced the scope of the unknown party's activity. We also hired third-party experts to investigate and remediate any unauthorized activity in our systems, and we notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

Enclosed with this letter you will find steps you can take to protect yourself. In addition, we are offering a complimentary, <<one-year/two-year>> membership to Experian's IdentityWorks. This product helps detect possible misuse of personal information. To register, please:

- Ensure that you **enroll by: <<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <<Activation code>>

If you have questions or want an alternative to enrolling in Experian IdentityWorks online, please contact Experian at 877-288-8057 by <<Enrollment Deadline>> and provide them engagement number <<Engagement #>>.

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions. You can contact the call center at 888-542-7017, and one of our representatives will be happy to assist you. We appreciate your patience as we work through this process.

Sincerely,

John Henriksen
Vice President of IT
610 E. Gish Rd.
San Jose, CA 95112

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

<<Name 1>>
<<Name 2>>
<<Company>>
<<Address 1>>
<<Address 2>>
<City>, <State> <ZIP>

<<Maildate>>

NOTICE OF DATA BREACH

Dear <<Name 1>>,

On behalf of the GreenWaste family of companies, we are writing to inform you of a data-security incident that involved your personal information. We want to make you aware of this situation, inform you of the steps we have taken, and provide you some steps you may take to help protect yourself.

WHAT HAPPENED

On November 27, 2023, we identified suspicious activity on our network systems. We took immediate steps to secure our network systems and to investigate the incident. We subsequently determined that an unauthorized third party gained access to a portion of our computer network that contained files with personal information. Based on our investigation, we believe the unauthorized access occurred from November 22 to 27, 2023. Once we identified the affected files, we promptly engaged a data-review firm to determine what information was contained in those files. We received the results of that review on February 27, 2024. We have been working since then to identify the affected individuals and the correct addresses for them.

WHAT INFORMATION WAS INVOLVED

Our investigation determined that the affected data includes full name and financial information, such as a bank account and routing numbers.

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our systems. Those measures reduced the scope of the unknown party's activity. We also hired third-party experts to investigate and remediate any unauthorized activity in our systems, and we notified law enforcement, which did not delay this notice.

WHAT YOU CAN DO

We encourage you to remain vigilant for incidents of fraud and identity theft by reviewing your account statements (if any) and monitoring free credit reports. Promptly report any fraudulent activity or any suspected incidents of identity theft to your financial institutions or company with which the account is maintained, as well as applicable authorities, including local law enforcement, your state attorney general, and the Federal Trade Commission ("FTC"). Enclosed with this letter you will find additional steps you can take to protect yourself. If you have questions about this matter, please call us at the phone number below.

FOR MORE INFORMATION

We have established a toll-free call center to support you and answer your questions. You can contact the call center at 888-542-7017, and one of our representatives will be happy to assist you. We appreciate your patience as we work through this process.

Sincerely,

John Henriksen
Vice President of IT
610 E. Gish Rd.
San Jose, CA 95112

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.IdentityTheft.gov/.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.

- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.

- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com

For Maryland Residents: the Maryland Attorney General may be contacted at: Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov.

For North Carolina Residents: the North Carolina Attorney General may be contacted at: Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27669; (919) 716-6400; www.ncdoj.gov.

For New York Residents: the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224; 1-800-771-7755; www.ag.ny.gov.

You can also find your Attorney General's contact information at: https://www.usa.gov/state-attorney-general.

Review the Fair Credit Reporting Act – You also have certain rights under the Fair Credit Reporting Act (FCRA), including 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, and your rights pursuant to the FCRA, please visit: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.