April 10, 2024

VIA Website Portal
Consumer Protection & Antitrust Bureau
Office of the Attorney General
1 Granite Place South
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP represents Rapid Granulator, Inc., ("Rapid") a Pennsylvania company that manufactures recycling equipment, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Indiana's data breach notification statute N.H. RSA § § 359-C:19 to 359-C:21.

1. **Nature of the Security Incident**

On March 12, 2024, Rapid learned that information related to its employees may have been accessed by an unauthorized person. In February 2024, Rapid learned from an overseas affiliate that it had detected unusual activity on its system and within its email environment. Rapid immediately terminated its access to the internet and began an investigation to determine what happened. That investigation eventually revealed that an unauthorized person may have gained access to some personal information, including some personal information of its current and former employees. Rapid then worked to ascertain the identities of the potentially involved individuals and the types of their information that may have been involved in this incident, and then to locate current contact information if the information involved necessitated notification. This work was completed on March 12, 2024.

To date, Rapid has no reason to believe that personal information of the individuals involved has been misused as a result of this incident. Out of an abundance of caution, Rapid has mailed notifications to all individuals involved, providing them with steps they can take to protect their personal information, and offering them free identity monitoring services.

2. **Number of Affected New Hampshire Residents & Information Involved**

The incident involved personal information for one (1) New Hampshire resident. The information involved in the incident included the individual's . Again, Rapid has no reason to believe that the information involved has been or will be misused.

3. **Notification to Affected Individuals**

On April 9, 2024, a notification letter was sent to the affected NH resident by USPS First Class Mail. The notification letter provides resources and steps the individual can take to help protect their information. The notification letter also offers of complimentary identity protection services including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter is enclosed.

4. **Measures Taken to Address the Incident**

Rapid terminated the unauthorized access on its network and began an investigation into what happened. Rapid has sent notice to the potentially affected individual and is providing them with steps they can take to protect their personal information as discussed above. Rapid is also examining its cyber environment in order to consider what steps might prevent a similar incident from happening in the future.

5. **Contact Information**

If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at .

Sincerely,

Richard Goldberg
Constangy, Brooks, Smith & Prophete LLP

RG:KD
Encl.: Sample Notification Letter
cc: Kim Detwiler, Constangy (kdetwiler@constangy.com)

4145 SW Watson Avenue, Suite 400
Beaverton, OR 97005

<<First Name>> << Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

April 9, 2024

Subject: Notice of Security Incident

Dear <<First Name>> << Last Name>>:

We are writing to you about the data incident we advised you of last month. This letter contains information regarding the incident and steps you can take to help protect your personal information in addition to the free identity protection we offered last month.

What Happened. On March 12, 2024, we learned that your personal information may have been involved in connection with a computer network incident in which there was unauthorized access to our network. This is the same incident that was discovered in our network on February 4, 2024 which we advised everyone about last month. We immediately took systems offline and engaged experts to help us secure the cyber network and investigate what happened. Although we have no information that anyone's data has been misused, we provided free identity protection to individuals whose information may have been involved in the incident. If you did not enroll before, this letter contains instructions on how to enroll now.

What Information Was Involved. The potentially involved information may have included your

What We Are Doing. As soon as we discovered the incident, we took the steps described above and took steps to minimize the risk of a similar incident occurring in the future. We have also reported the incident to law enforcement and will cooperate with their investigation.

As you recall, we previously offered the opportunity to enroll in complimentary identity protection services through IDX, an identity protection and assistance expert. These services include of credit monitoring and CyberScan (dark web) monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do. If you have not yet done so, you can enroll in the complimentary services offered to you through IDX identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You will need to reference the enrollment code in this letter when calling or enrolling online, so please do not discard this letter. Please note the deadline to enroll is .

There is no need to re-enroll if you have already enrolled.

For More Information: You can contact IDX at 1-800-939-4170 if you have questions about the incident or the enrollment.

We take this event and the security of information in our care seriously. We deeply regret any concern or inconvenience that this incident may cause you.

Sincerely,

Jim Hoffman
President
Rapid Granulator, Inc.
555 West Park Road
Leetsdale, PA 15056

IDX
A ZEROFOX COMPANY

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland**,** Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, https://consumer.ftc.gov, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.