LEWIS BRISBOIS
LEWIS BRISBOIS BISGAARD & SMITH LLP

Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, CA 92626
kamran.salour@lewisbrisbois.com
Direct: 714.966.3184

January 31, 2025

VIA ONLINE FORM

Attorney General Anthony G. Brown
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Email: IDTheft@oag.state.md.us

Re: Notification of Data Security Incident

To Whom It May Concern:

Lewis Brisbois represents ITO EN, a company specializing in the sale of matcha drink powder, in conjunction 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 the Maryland data breach notification law.

1. Nature of the Security Incident

On or around December 2, 2024, ITO EN detected an incident in which an unauthorized third party attempted to enter ITO EN's network and exfiltrate data. Upon detecting the incident, ITO EN moved quickly to secure its network and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any personal information. The investigation concluded on December 26, 2024.

2. Type of Information and Number of Maryland Residents Affected

ITO EN notified six (6) residents of Maryland of this data security incident via first class U.S. mail on January 31, 2025. The information accessed and potentially acquired by the unauthorized actor responsible for this incident may have included name mailing address, Social Security number, and financial account information. A sample copy of the notification letter sent to these individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

ITO EN has implemented additional security features in an effort to prevent a similar incident from occurring in the future. ITO EN also notified the major credit reporting agencies, TransUnion, Equifax, and Experian, of the incident. Further, ITO EN has offered all individuals whose information was involved twelve (12) months of complimentary services through IDX, a ZeroFox company, which includes credit monitoring, dark web monitoring, a $1 million identity fraud loss reimbursement policy, fully-managed identity theft recovery services, and ninety (90) days access to a call center.

4. Contact Information

ITO EN 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 (714) 966-3184 or by email at Kamran.Salour@lewisbrisbois.com.

Regards,

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

ITO EN

P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

January 31, 2025

Notice of Data <<Variable Data 1: Incident/Breach >>

To <<FirstName>> <<LastName>>,

We write to inform you of a data security incident that may have exposed your personal information. This letter provides information about the incident and the steps that you can take to help protect your information.

What Happened?

On or around December 2, 2024, ITO EN (North America) INC. detected an incident in which an unauthorized third party attempted to enter ITO EN's network and exfiltrate data. Upon detecting the incident, ITO EN moved quickly to secure its network and launched an investigation. The investigation was performed with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to our systems and any personal information. The investigation concluded on December 26, 2024.

What Information Was Involved?

While we currently have no evidence that any of your personal information has been specifically accessed for misuse, the investigation determined that your name, mailing address, Social Security Number, and bank account information may have been exposed during this incident. As of this writing, ITO EN has not received any reports of related identity theft since the date of this incident.

What We Are Doing

ITO EN engaged external cybersecurity experts and is taking steps to prevent a similar event from occurring in the future by implementing additional safeguards and enhanced security measures.

Additionally, in response to the incident, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<Membership Offering Length: 12/24>> months of 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.

How do I enroll for the free services?

To enroll in identity protection services at no charge, please go to https://app.idx.us/account-creation/protect or call 1-833-903-3648 and use the Enrollment Code provided above. Please note the deadline to enroll is May 1, 2025. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday, excluding holidays. Please call the help line at 1-833-903-3648 and be prepared to supply the fraud specialist with your unique code listed within.

You are encouraged to take full advantage of these services. Enclosed you will find additional materials regarding the resources available to you, and the steps you can take to further protect your personal information.

Again, ITO EN values the security of the personal data it maintains, and understand the frustration, concern, and inconvenience that this incident may have caused.

Sincerely,

ITO EN (North America) INC.

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 1-833-903-3648 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, https://www.marylandattorneygeneral.gov/, 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: 1-877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400.

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.