EXHIBIT 1

By providing this notice, Hoshino (U.S.A.) Inc. ("Hoshino") does not waive any rights or defenses regarding the applicability of Nebraska law, the applicability of the Nebraska data event notification statute, or personal jurisdiction.

Nature of the Data Event

Hoshino recently became aware of suspicious activity related to two employee email accounts. Hoshino immediately took steps to secure the two email accounts and launched an investigation to determine the nature and scope of the activity. Hoshino's investigation determined that there was unauthorized access to one of the affected email accounts at various times between June 20, 2024 and August 5, 2024, and to the second account at various times between July 15, 2024 and August 12, 2024. Although Hoshino has no evidence to indicate that any information was actually misused, Hoshino is providing notice of this event out of an abundance of caution.

Upon becoming aware of the unauthorized access, Hoshino began a diligent and comprehensive review process to identify sensitive information that may have been contained within the impacted email accounts, and to identify the individuals whose information may have been impacted. Hoshino then worked to identify appropriate contact information for the impacted individuals. That process recently completed, at which point Hoshino promptly notified the potentially impacted individuals whose information was contained within the impacted email accounts.

The potentially impacted types of information includes name and Social Security number.

Notice to Nebraska Resident

On or about April 3, 2025, Hoshino began providing written notice of this incident to approximately one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon becoming aware of the event, Hoshino moved quickly to investigate and respond to the same, assess the security of Hoshino systems, and identify potentially affected individuals. Hoshino is also working to implement additional safeguards and training for its employees. Hoshino is also providing access to credit monitoring services for twelve (12) months through IDX to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Hoshino is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Hoshino is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Hoshino is providing written notice of this incident to relevant state regulators, as necessary. Hoshino is also providing notice of this event to the three major credit reporting agencies.

EXHIBIT A

HOSHINO (U.S.A.) INC.
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:

SCAN ME

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

<<First Name>> <<Last Name>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

April 3, 2025

NOTICE OF <<Variable Data 2:DATA BREACH/SECURITY INCIDENT>>

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

Hoshino (U.S.A.) Inc. ("Hoshino") writes to inform you of a recent incident that may impact the privacy of some of your information. While we are unaware of any attempted or actual misuse of your information, we are sending this letter proactively, in line with our values of treating data privacy with the utmost caution and care.

What Happened? We recently became aware of suspicious activity related to two employee email accounts. We immediately took steps to secure the two email accounts and hired professional forensic investigators to determine the nature and scope of the activity. The investigation found unauthorized access to those email accounts at various times between June 20, 2024 and August 12, 2024, but found no evidence of actual misuse of any sensitive personal information contained within those email accounts.

What Information Was Involved? The investigation determined that the following information related to you was present in the impacted email account(s): your name and <<Variable Data 1: Impacted Elements>>. However, the investigation found no evidence that your information was subject to actual or attempted misuse.

What Are We Doing? Once the investigators completed their process, we worked to identify contact information for any potentially impacted individuals. This notice followed. As a precaution, we are also providing <<Membership Offering Length: 12/24>> months of complimentary access to credit monitoring services through IDX. Individuals who wish to receive these services may enroll by following the enclosed instructions.

What Can You Do? As a best practice, we encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity over the next <<Membership Offering Length: 12/24>> months. You may also enroll in the complimentary credit monitoring services provided. Please note the deadline to enroll is July 3, 2025.

For More Information. Please see the enclosed *Steps You Can Take to Help Protect Personal Information* for further tips to protect your personal information. Additionally, we have set up a dedicated assistance line at 1-800-939-4170, toll-free, Monday through Friday from 9 am - 9 pm Eastern Time to answer any further questions.

Hoshino takes the privacy and security of the information in our care seriously, and we sincerely apologize for any inconvenience this incident may cause you.

Sincerely,

Hoshino (U.S.A.) Inc.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Theft Protection

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	www.transunion.com/credit-freeze www.transunion.com/fraud-alerts
1-888-298-0045	1-888-397-3742	1- 833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion LLC Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion LLC Credit Freeze, P.O. Box 2000, Chester, PA 19016

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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. We encourage consumers to review their 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.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov. You may also write to Hoshino at 1726 Winchester Road, Bensalem, PA 19020.