EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, SPE 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

SPE became aware of suspicious activity involving its computer network and promptly took steps to secure its systems. SPE also launched an investigation to determine the full nature and scope of the event. The investigation determined that an unknown actor accessed portions of the SPE network between February 19, 2026 and February 20, 2026, and accessed or acquired certain files while on the network. As a result, SPE undertook a thorough and time-intensive review of the involved files, with the assistance of third-party data review specialists, to determine the types of information contained within and to whom the information belonged. SPE recently completed this review. Although SPE has no evidence of any identity theft of fraud in connection with this incident, SPE is notifying those individuals whose information was potentially impacted.

The information that could have been subject to unauthorized access includes name and driver's license number.

Notice to Nebraska Residents

On or about June 17, 2026, SPE began providing written notice of this incident to eight (8) Nebraska residents. 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 discovering the event, SPE moved quickly to investigate and respond to the incident, assess the security of SPE systems, and identify potentially affected individuals. Further, SPE notified federal law enforcement regarding the event. SPE is also working to implement additional safeguards and training to its employees. SPE is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, SPE is providing impacted individuals with guidance on how to better protect against identity theft and fraud. SPE 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.

SPE is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Stanley Pearlman Enterprises, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS4156

0001084

7_0001084

[redacted]

June 17, 2026

NOTICE OF SECURITY INCIDENT

Dear [redacted],

Stanley Pearlman Enterprises, Inc. ("SPE") writes to inform you of a recent event that may have impacted the privacy of certain information related to you. While we are unaware of any identity theft or fraud associated with this event, we are providing you with information about our response and steps you may take to better protect your information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity involving our computer network and promptly took steps to secure our systems. We also launched an investigation to determine the full nature and scope of the event. The investigation determined that an unknown actor accessed portions of our network between February 19, 2026 and February 20, 2026, and accessed or acquired certain files while on the network. As a result, we undertook a thorough and time-intensive review of the involved files, with the assistance of third-party data review specialists, to determine the types of information contained within and to whom the information belonged. SPE completed this review on May 22, 2026 and determined that your information was included therein. Following the conclusion of the file review, SPE conducted additional review of its internal records to identify contact information for individuals to make this notification.

What Information Was Involved? The review determined your [redacted] were present in the involved files.

What We Are Doing. Upon learning of the event, we immediately took steps to secure our systems and conducted an investigation to confirm the nature and scope of the activity and determine who may be affected. Additionally, while we have safeguards in place to protect data in our care, we have taken steps to further enhance these protections and continue to monitor these safeguards as part of our ongoing commitment to data security.

As an added precaution, we are also offering you twelve (12) months of credit monitoring and identity restoration services at no cost to you through Cyberscout, a TransUnion company. Enrollment instructions are enclosed with this letter. Please note that while we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect against possible misuse of your information. You may also enroll in the free credit monitoring services we have provided for you.

For More Information. If you have additional questions, please contact our dedicated assistance line at [redacted] between the hours of 8:00 am and 8:00 pm EST, excluding U.S. holidays. You may also write to SPE at 7775 Chesapeake Bay Court, Jessup, MD 20794.

Sincerely,

Stanley Pearlman Enterprises, Inc.

0001084

Steps You Can Take To Help Protect Personal Information

Enroll in Credit Monitoring Services

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 one-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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, 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/	https://www.transunion.com/credit-help
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 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 Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a best practice, consumers should change all passwords to their personal accounts on a regular basis, use strong passwords, and refrain from using the same password for multiple accounts. Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your 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 state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov. SPE is located at 7775 Chesapeake Bay Court, Jessup, MD 20794.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. SPE is located at 7775 Chesapeake Bay Court, Jessup, MD 20794.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 2 Rhode Island residents that may be impacted by this event.