EXHIBIT 1

By providing this notice, ESP Associates, Inc. (“ESP”) 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

ESP recently became aware of suspicious activity within its computer network. Upon learning of the suspicious activity, ESP immediately took steps to secure its systems and launched an investigation into the nature and scope of the activity with the assistance of third-party cybersecurity and data privacy specialists. The investigation determined that an unauthorized actor accessed ESP’s network at various times between February 19, 2025 and February 27, 2025, and certain information contained on its network was viewed or copied by the unauthorized actor during that time.

Upon becoming aware of the unauthorized access, ESP began a diligent and comprehensive review process to identify sensitive information that may have been contained within its network, and to identify the individuals whose information may have been impacted. ESP also worked to identify appropriate contact information for the impacted individuals for the purposes of notification. That process recently completed, at which point ESP promptly notified the potentially impacted individuals because the investigation determined certain information related to those individuals was contained within the impacted files.

The impacted types of information may vary by individual, and includes name, Social Security number, and financial account information.

Notice to Nebraska Residents

On June 13, 2025, ESP began providing written notice of this incident to approximately two (2) 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 becoming aware of the event, ESP moved quickly to investigate and respond to the incident, assess the security of ESP systems, and identify potentially affected individuals. Further, ESP notified federal law enforcement regarding the event. ESP is also working to implement additional safeguards and training for its employees. ESP is providing access to credit monitoring services for 12 months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

ESP is also 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

ESP Associates, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1066

3_0000734

0000734

June 13, 2025

NOTICE OF SECURITY INCIDENT

Dear :

ESP Associates, Inc. ("ESP") writes to inform you of a recent event that may affect the privacy of some of your information. Although we are unaware of any identity theft or fraud in relation to the event, we are providing you with information about the event, our response, and resources available to help you protect your information, should you feel it appropriate to do so.

What Happened? ESP recently became aware of suspicious activity within our computer network. Upon learning of the suspicious activity, we immediately took steps to secure our systems and launched an investigation into the nature and scope of the activity with the assistance of third-party cybersecurity and data privacy specialists. The investigation determined that an unauthorized actor accessed our network at various times between February 19, 2025 and February 27, 2025, and certain information contained on our network was viewed or copied by the unauthorized actor during that time. Upon becoming aware of these findings, we undertook a comprehensive and time-intensive review of the data at risk to determine what information was affected, and to whom that information related. Those efforts recently completed, and ESP is notifying you because the investigation determined that certain information relating to you was contained within the impacted files.

What Information Was Involved? The following types of information related to you were found in the impacted files: your Social Security number, date of birth, driver's license number, Passport number, financial account information, health insurance policy number, health insurance group number, and medical information. At this time, ESP is not aware of your information being used to commit identity theft or fraud in relation to this incident.

What We Are Doing. We take this event seriously, and the confidentiality, privacy, and security of information in our care are among our highest priorities. Upon learning of this event, we moved quickly to investigate and respond, secure our network to ensure the threat was contained, and notify affected individuals. We also notified federal law enforcement of the event. As part of our ongoing commitment to information security, we are also reviewing existing security policies and have dedicated and are continuing to dedicate significant resources to implement additional cybersecurity measures to further protect against similar threats moving forward. We are also notifying impacted individuals, including you, so they may take steps to protect their information, should they feel it is appropriate to do so.

As an added precaution, we are offering you immediate access to credit monitoring and identity theft protection services for twelve (12) months at no cost to you, through Cyberscout, a TransUnion company.

You can find information on how to enroll in these services in the enclosed *Steps You Can Take To Help Protect Your Information*. We encourage you to enroll in these services as we are not able to do so on your behalf.

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 free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. As best practice, you should frequently change your password for all online accounts. If your username and password is potentially impacted by this event, we encourage you to change the passwords, along with the security questions and answers, for all your online accounts. You can review the enclosed *Steps You Can Take To Help Protect Your Information* to learn helpful tips on steps you can take to protect against possible information misuse, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-833-566-6374 from 8:00 a.m. ET to 8:00 p.m. ET, Monday through Friday, excluding major U.S. holidays. You may also write to us at 3475 Lakemont Boulevard Fort Mill, SC 29708.

Sincerely,

ESP Associates, Inc.

Steps You Can Take To HELP Protect YOUR Information

Enroll in 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: **.** 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 (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit https://www.annualcreditreport.com or call, toll-free, 1 (877) 322-8228. Consumers may also directly contact the three (3) 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 one (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 (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) 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 (2) to five (5) 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 consumers wish to place a credit freeze or fraud alert, please contact the three (3) 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/data-breach-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

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; https://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, the Federal Trade Commission, and the relevant 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 https://oag.dc.gov.

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.

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 https://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 https://www.ncdoj.gov.