EXHIBIT 1

By providing this notice, Steel Encounters, Inc. ("Steel Encounters") 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

Steel Encounters became aware of suspicious activity on their network and promptly began an investigation. The investigation determined between July 27, 2025 and August 1, 2025, an unauthorized actor gained accessed to and copied information from certain systems on the network. Steel Encounters took steps to identify the impacted data and on or around November 7, 2025 the preliminary review of the data was completed. Steel Encounters then took further steps to validate and enrich the data for purposes of providing notice to potentially impacted individuals. This review was recently completed identified personal information including name and Social Security number.

Notice to Nebraska Resident

On or about December 31, 2025, Steel Encounters provided written notice of this incident to one (1) Nebraska resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***. Steel Encounters also posted notice on its website and provided notice to relevant media outlets.

Other Steps Taken and To Be Taken

Upon becoming aware of the suspicious activity, Steel Encounters took steps to secure their systems, assess the security of Steel Encounters systems, and investigate the activity to determine what happened. Steel Encounters then took steps to identify potentially impacted information for purposes of providing notice. As part of Steel Encounters' ongoing commitment to the privacy of information in its care, Steel Encounters notified federal law enforcement regarding the incident and is reviewing and enhancing its existing policies and procedures relating to data and cyber security, as appropriate.

Steel Encounters is providing access to credit monitoring services for twenty-four (24) months, through Kroll, to potentially impacted individuals. Additionally, notice to these individuals provides guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their banking, credit card company, and any other applicable institutions Steel Encounters 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.

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

EXHIBIT A

STEELENCOUNTERS

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

SCAN TO ENROLL

<<Date>> (Format: Month Day, Year)

<<b2b_text_4 (Notice of Data Breach)>>

Dear <<First_name>> <<Middle_name>> <<Last_name>> <<Suffix>>:

Steel Encounters, Inc. ("Steel Encounters") writes to notify you of an incident that may affect the security of some of your information. This letter provides you with information about the incident, our response, and resources available to you to help protect your information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity on the Steel Encounters network and promptly began an investigation. The investigation determined between July 27, 2025 and August 1, 2025, an unauthorized actor gained accessed to and copied information from certain systems on the network. Steel Encounters took steps to identify the impacted data and on or around November 7, 2025 the preliminary review of the data was completed. We then took further steps to validate and enrich the data for purposes of providing notice to potentially impacted individuals. This review was recently completed and determined that your personal information may have been involved.

What Information Was Involved? The review identified the following types of information relating to you: <<b2b_text_1 ("name" and data elements)>><<b2b_text_2 (data elements 2)>><<b2b_text_3 (data elements 3)>>.

What We Are Doing. We take this matter and the security of personal information in our care seriously. Upon learning of the suspicious activity, we took steps to assess and secure the network, investigate the activity, and identify any impacted data. We notified federal law enforcement and are notifying relevant regulatory authorities. We are also notifying potentially impacted individuals of the incident and are providing them with resources that they may consider. As part of our ongoing commitment to the privacy of information in our care, we are reviewing and enhancing our existing policies and procedures as appropriate.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits forms and monitoring your free credit reports for suspicious activity and to detect errors. Any suspicious activity should be promptly reported to your bank, credit card company, and/or other applicable institution. Additional information and resources are included in the *Steps You Can Take to Help Protect Personal Information* section of this letter.

Out of an abundance of caution, we are also offering you complimentary access to 24 months of identity monitoring services through Kroll.. While we are covering the cost of these services, due to privacy restrictions, you will need to independently complete the activation process. Enrollment instructions are included in this letter below.

For More Information. If you have questions regarding this notice, please call our dedicated assistance line at 1-844-574-1138, between the hours of 9:00 a.m. and 6:30 p.m. EST, Monday – Friday, excluding major U.S. holidays. You may also write to Steel Encounters at 525 E 300 S, Salt Lake City, UT 84102.

Sincerely,

Steel Encounters

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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 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 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 consumers 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/	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 their 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 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 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 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.