EXHIBIT 1

By providing this notice, RFK Racing 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

On May 14, 2025, RFK Racing learned of suspicious activity on certain systems in its environment. Upon learning this, RFK Racing immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. As a result of the investigation, RFK Racing determined that certain files were accessed or taken without authorization. Thereafter, RFK Racing undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, and to whom it related. On August 4, 2025 RFK Racing confirmed the potentially impacted data contained limited information related to individuals.

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

Notice to Nebraska Residents

On September 12, 2025, RFK Racing provided written notice of this incident to approximately seven (7) 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, RFK Racing moved quickly to investigate and respond to the incident, assess the security of RFK Racing systems, and identify potentially affected individuals. Further, RFK Racing notified federal law enforcement regarding the event. RFK Racing is also working to implement additional safeguards and training to its employees. RFK Racing is providing access to credit monitoring services for twenty-four (24) months, through Cyberscout, a TransUnion company, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

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

RFK Racing 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

Roush Fenway Keselowski Racing, LLC
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1554

0004312

21_0004312

[redacted]

September 12, 2025

NOTICE OF SECURITY INCIDENT

Dear [redacted]

Roush Fenway Keselowski Racing, LLC ("RFK Racing") writes to notify you of an incident that may affect the privacy of some of your information. This letter provides details of the incident, our response, and steps you may take to better protect against the possible misuse of your information should you feel it is appropriate to do so. RFK Racing may be in possession of your information as part of joint business management services previously provided by Roush Management.

What Happened?

On May 14, 2025, RFK Racing learned of suspicious activity on certain systems in its environment. Upon learning this, RFK Racing immediately launched an investigation with the assistance of third-party forensic specialists to determine the nature and scope of the activity. As a result of the investigation, we determined that certain files were accessed or taken without authorization. Thereafter, RFK Racing undertook a comprehensive review of the data at risk to assess if any sensitive information could be affected, and to whom it related. On August 4, 2025, RFK Racing confirmed the potentially impacted data contained limited information related to you. After completing this review, we communicated with Roush Management in order to jointly provide you with notice.

What Information Was Involved?

The information identified in the affected files included your name and the following [redacted]

What We Are Doing. RFK Racing takes the confidentiality, privacy, and security of information in its care seriously. Upon learning of the incident, we immediately commenced an investigation and took steps to implement additional safeguards and review our policies and procedures relating to data privacy and security.

In an abundance of caution, RFK Racing is providing you with access to 24 months of credit monitoring and identity protection services through TransUnion at no cost to you. A description of the services and instructions on how to enroll can be found within the enclosed *Steps You Can Take to Protect Personal Information.* Please note that you must complete the enrollment process yourself, as we are not permitted to enroll you in these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your relevant account statements and monitoring your free credit reports for suspicious activity and to detect errors over the next twenty-four (24) months. We also recommend you review the *Steps You Can Take to Protect Personal Information* section of this letter. There you will find additional information regarding ways to monitor and protect your information.

For More Information. If you have questions, you can call our dedicated assistance line at [redacted] which is available Monday through Friday, between the hours of 8:00 a.m. and 8:00 p.m. Est, excluding major U.S. holidays. You can also write to us at RFK Racing 4600 Roush Place, Concord, NC 28027.

Sincerely,

Roush Fenway Keselowski Racing, LLC

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

In response to the incident, we are providing you with access to complimentary access to single bureau credit monitoring services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation 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 a free credit report, visit www.annualcreditreport.com or call, toll-free, [redacted]. 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 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, 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, 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; 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 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.

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.