Safetyfirst Systems, LLC
c/o Cyberscout
P.O. Box 3826
Suwanee, GA 30024

71 1 12633 ******************AUTO**All For SCF 060

July 23, 2026

Notice of Data

Dear :

At Safetyfirst Systems, LLC ("SFS," "we", "us," "our"), we take the privacy and security of our client's information seriously. SFS provides driver/employee compliance and Motor Vehicle Records services to businesses, including . We are writing to inform you that SFS experienced a data incident which may have affected your personal information ("Information"). Based on our current review, we have no indication that your Information has been or will be used inappropriately, but we wanted to make you aware of the incident, the measures we have taken in response, and to provide details on the steps you can take to help protect your Information including your ability to enroll in identity monitoring services that we are offering free of charge.

For More Information

Please know that the protection of your personal information is a top priority, and we understand the inconvenience and concern this incident may cause. Representatives can be reached at 1-833-289-5523 between the hours of 7:00 a.m. to 7:00 p.m. Eastern time, Monday through Friday, excluding holidays, and are available for ninety (90) days from the date of this letter to assist you with questions regarding this incident.

What Happened?

On January 19, 2026, a log review revealed suspicious activity associated with a portion of our environment. We secured and remediated the compromise, engaged additional third-party experts, hardened and enhanced our data security, and commenced an investigation. Unfortunately, these types of incidents have become commonplace and impact organizations of all sizes. A third-party forensic investigation determined the unauthorized actor had access to a limited portion of our environment between January 16, 2026, and January 19, 2026, and may have accessed some of your Information.

What Information Was Involved?

We determined that the following types of Information may have been impacted as a result of this incident: , and name. We are unaware of any fraud or identity theft stemming from the incident.

What We Are Doing

Upon discovering the incident, we promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and notified law enforcement. As part of our ongoing commitment to the security of information, we are evaluating opportunities to further secure our systems to prevent a similar event from occurring again in the future. Further, there have been no alerts of suspicious activity since the response began, and full containment has been documented.

Additionally, out of an abundance of caution, we have arranged for you to activate, at no cost to you, TransUnion Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for months from the date of enrollment when changes occur to your credit file. With this service, notification will be sent to you the same day that a 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.

What You Can Do

To enroll in the complimentary services we are offering you, please visit **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 ninety (90) days from the date of this letter.

Please note that to activate monitoring services, you will need an internet connection and e-mail account. Additionally, you may be required to provide your name, date of birth, and Social Security number to confirm your identity. Please note that the certain services might not be available for individuals who do not have a credit file with the credit bureaus or an address in the United States (or its territories) and a valid Social Security number. Activating this service will not affect your credit score.

At this time, we are not aware of anyone experiencing fraud or identity theft as a result of this incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of an Identity Protection PIN (IP PIN) with the IRS, fraud alerts, and security freezes.

Sincerely,

Safetyfirst Systems, LLC
PO Box 101
3299 US Highway 46
Parsippany, NJ 07054-9998

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian_(https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
equifax.com/personal/credit-report-services/	experian.com/freeze/center.html	transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Florida* and *West Virginia*: You may contact the call center number listed on the first page of this letter to learn whether and what types of information about what information we maintain about you and what may have been impacted.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:* You can obtain information from the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

Additionally, residents can obtain information about steps to take to avoid identity theft from:

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.gov

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

District of Columbia Office of the Attorney General 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft. There are 196 Rhode Island residents affected by this incident.