

EXHIBIT 1



Michael McLaughlin, Esq.
Co-Chair, Cybersecurity and Data Privacy
michael.mclaughlin@bipc.com

1700 K Street, N.W., Suite 300
Washington, D.C. 20006-3807
T 202 452 5463

July 31, 2025

The Attorney General Mike Hilgers
Office of the Attorney General
Consumer Protection Division
2115 State Capitol
Lincoln, NE 68509

Re: Notice of Data Security Incident

Dear Attorney General Hilgers:

I am writing to you on behalf of Phil Smith Automotive Group (“Phil Smith,” “We,” or “Our”) in accordance with Neb. Rev. Stat. § 87-303(2). Phil Smith experienced unauthorized access to its information technology (IT) systems. Based on our investigation, the personal information of one (1) Nebraska resident may be involved. This notice may be supplemented with any new significant facts learned subsequent to its submission.

In or around early February 2025, Phil Smith became the victim of a ransomware attack that affected its IT systems. Upon discovering this activity, we immediately took protective actions to stop the unauthorized access, notified U.S. federal law enforcement, including the Federal Bureau of Investigation (“FBI”), assessed the security of our network and systems, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation to date indicates that some personal information may have been accessed by an unauthorized party. The personal information that could have been subject to unauthorized access included individuals’ name and Social Security number.

On July 31, 2025, we began providing written notice of this incident to potentially affected individuals. The written notice is being provided in substantially the same form as the letter attached hereto as **Exhibit A**.

We have installed monitoring devices on our IT systems to detect suspicious activity. We are also working to implement additional safeguards and are providing the potentially affected individuals two (2) years of complimentary credit protection and monitoring services through Cyberscout at no cost to the individuals.

If you have any questions or if I may provide additional information, please contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "M. G. McLaughlin", followed by a horizontal line.

Michael G. McLaughlin
Outside Counsel for Phil Smith Automotive Group

With a copy to: tiffany.yeung@bipc.com; jacqueline.jonczyk@bipc.com

EXHIBIT A

Phil Smith Automotive Group
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



July 31, 2025

Notice of Data Incident

Dear 

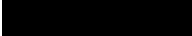
Phil Smith Automotive Group (“Phil Smith,” “we,” or “us”) is writing to inform you about a recent cybersecurity incident that may have impacted some of your personal information. The security of your personal information is very important to us, and we take the trust you place in us very seriously. We wanted to advise you about the incident and to offer you some resources you may find helpful.

What Happened? Phil Smith detected unauthorized activity in our information technology (IT) systems. Upon discovering this activity, we immediately took protective actions to stop the unauthorized access, notified U.S. federal law enforcement, and launched an investigation with the assistance of leading cybersecurity specialists. The investigation indicated that some of your personal information may have been accessed by an unauthorized party in early February 2025. At this time, we have no reason to believe your information has been misused; however, we are providing you notice out of an abundance of caution.

What Personal Information May Be Involved? The affected personal information may have included your .

What We Are Doing. We are taking this incident very seriously. Upon detecting unauthorized activity in our IT systems, we took immediate protective actions to contain the activity and retained industry-leading cybersecurity specialists to investigate the incident, ensure the unauthorized access ceased, and use lessons learned to improve our systems’ security posture. It is our priority to continue to evaluate and deploy the level of robust security protocols, continuous monitoring, and staff training needed to prevent and defend against sophisticated cybersecurity threats.

What You Can Do. Because our investigation indicated that some of your personal information may have been affected, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for twenty-four (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 the 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:  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.

For More Information. We sincerely regret any inconvenience this incident may cause you. If you have questions regarding this incident or the services available to you, representatives are available for 90 days from the date of this letter between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-397-5381 and supply the fraud specialist with your unique code listed above.

Sincerely,

Phil Smith Automotive Group

RECOMMENDED STEPS FOR IDENTITY THEFT PROTECTION

Review Your Credit Reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You have the right to file a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General's office in your home state.

Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

Security Freeze. By placing a security freeze, someone who fraudulently acquires your personally identifiable information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission (FTC) also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia Residents: Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, <https://oag.dc.gov>, or by phone at (202) 442-9828.



Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division Office, 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, Telephone: 1-888-743-0023, or at <https://www.marylandattorneygeneral.gov/Pages/contactus.aspx>

Massachusetts Residents: You are advised of your right to obtain a police report in connection with this incident.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.