

Stephens & Smith Construction Provides Notice of Data Security Incident

Stephens & Smith Construction (“Stephens & Smith”) provides notice of an incident that may affect the security of some information relating to certain Stephens & Smith vendors and employees. Stephens & Smith takes the confidentiality, privacy and security of information in its care seriously. Importantly, at this time, Stephens & Smith has not received any reports of actual or attempted misuse of the information involved.

What Happened? On January 29, 2021, Stephens & Smith discovered suspicious activity involving an employee email account. Stephens & Smith immediately secured its network and began investigating the activity to determine the scope of the incident and potential unauthorized access in the Stephens & Smith network. On March 3, 2021, Stephens & Smith determined that an unknown, unauthorized actor gained access to an employee email account beginning on or about January 12, 2021. Stephens & Smith then conducted a thorough and time-consuming review of the contents of the email account to determine what information may have been involved and to whom the information relates. This effort concluded on or about April 20, 2021.

While the investigation did not confirm that any information in the account was accessed or removed from the environment, the review determined that personal information was contained in the account during the incident. Therefore, Stephens & Smith is providing notice to all individuals associated with sensitive information in the affected account out of an abundance of caution.

What Information Was Involved? Stephens & Smith determined that the types of information in the impacted account may vary by individual and include one or more of the following: name, address, driver’s license number, and/or Social Security number.

What Stephens & Smith is Doing in Response? Upon discovering the event, Stephens & Smith moved quickly to investigate and respond to the incident, assess the security of its systems, and notify potentially affected individuals. Stephens & Smith is also working to implement additional safeguards and training to its employees. Stephens & Smith is providing access to credit monitoring services, through IDX, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Stephens & Smith is providing impacted individuals with 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 credit card company and/or bank. Stephens & Smith 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.

What Potentially Affected Individuals Can Do? Individuals who believe they may be impacted by this incident can call the dedicated confidential assistance line detailed below or find out more about how to protect against potential identity theft and fraud in the below section *Steps You Can Take to Better Protect Your Information*.

For More Information. If you believe you may have been impacted by this incident and have questions, please call Stephens & Smith’s dedicated assistance line at (800) 939-4170 between the hours of 8am – 8pm CT.

STEPS YOU CAN TAKE TO BETTER PROTECT YOUR INFORMATION

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide 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, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, 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/credit-help
888-298-0045	1-888-397-3742	833-395-6938
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade

Stephens & Smith Construction – Substitute/Website Notice

Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.