

Notice of Security Event

Professional Personnel Service, Inc., and its affiliated companies d/b/a Luttrell Staffing Group (“Luttrell Staffing”) is providing notice of an event that may impact the security of information related to current and former employees and associates. While there is no evidence of any attempted or actual misuse of this information, Luttrell Staffing is providing individuals potentially impacted by this event with information about the event, its response, and the steps these individuals may take to further protect their information against identity theft and fraud, should they feel it necessary to do so.

What Happened? On June 14, 2021, Luttrell Staffing became aware that certain files on its computer system were encrypted with malware by an unknown actor. Luttrell Staffing promptly took steps to secure the impacted systems and its network and launched an investigation to determine the nature and scope of the event. The investigation determined that an unauthorized actor gained access to certain Luttrell Staffing systems between June 10, 2021 and June 23, 2021. As a result, the unauthorized actor may have had access to certain files within these systems and certain current and former employee and associate information may have been accessed or acquired by the unauthorized actor.

What Information Was Involved? Although the investigation was able to determine that certain Luttrell Staffing systems were accessed, it was unable to confirm what specific information was actually accessed. Therefore, Luttrell Staffing began a comprehensive review of the impacted files out of an abundance of caution to determine what information was present at the time of the incident. Luttrell Staffing is notifying individuals now because on December 27, 2021, this review determined that certain information related to current and may have been impacted. This information includes names, dates of birth, Social Security number, government-issued identification number, financial account information, credit or debit card information, biometric information and medical and health insurance information.

What Luttrell Staffing is Doing. The privacy and security of information is among Luttrell Staffing’s highest priorities and we take this incident very seriously. Luttrell Staffing is reviewing its security policies and procedures, as well as working with cybersecurity specialists, to reduce the risk of this happening in the future and implemented additional measures and security tools to further protect information in its systems. Luttrell Staffing is also working to provide additional training to employees regarding data privacy and security. Luttrell Staffing is also offering complimentary credit monitoring services to affected individuals and reported this incident to federal law enforcement.

For More Information. If there are additional questions, or individuals believe they may be impacted by this event, please call Luttrell Staffing’s dedicated assistance line at (855) 568-2038. Individuals may also write to Luttrell Staffing at 1040 Tidewater Court, Kingsport, TN 37660.

What Affected Individuals Can Do. Luttrell Staffing encourages potentially impacted individuals to remain vigilant against incidents of identity theft and fraud by reviewing their account statements and monitoring their free credit reports for suspicious activity. Additionally, 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. In order for a consumer to order their free credit report, they can 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 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 a consumer is the victim of identity theft, the consumer is entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should a consumer wish to place a fraud alert, they may 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 the consumer’s name without their 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 security freeze, consumers 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 a consumer wish to place a fraud alert or credit freeze, they may 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

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, 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. 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 consumer’s 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, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and www.oag.state.md.us. Luttrell Staffing is located at 1040 Tidewater Court, Kingsport, TN 37660.

For 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 bureaus 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 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. We encourage you to 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.

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, you have the right to obtain any police report filed in regard to this incident.