



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

FEB 07 2022

CONSUMER PROTECTION

Gregory Lederman
Office: (267) 930-4637
Fax: (267) 930-4771
Email: glederman@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 1, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Professional Personnel Services, and its related entities, d/b/a Luttrell Staffing Group (“Luttrell Staffing”), located at 1040 Tidewater Court, Kingsport, TN 37660, and are writing to notify your Office of an incident that may affect the security of information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Luttrell Staffing does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

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. While the investigation into the full scope of the incident is ongoing, the investigation recently determined that an unauthorized actor gained access to certain Luttrell Staffing systems between June 1, 2021 and June 18, 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. Luttrell Staffing then undertook a comprehensive review of the potentially impacted systems to determine what data was present at the time of the incident and to whom the information belonged. On December 27, 2021, this review was completed and determined the information that could have been subject to unauthorized access includes name and Social Security number.

Notice to New Hampshire Residents

On or about September 7, 2021, Luttrell Staffing began notifying potentially affected individuals while the investigation and review was ongoing. On or about February 1, 2022, Luttrell Staffing provided written notice of this incident to affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. Luttrell Staffing also posted notice of this event on its website and provided notice to prominent media outlets in New Hampshire. A copy of Luttrell Staffing's website and media notices are attached here as *Exhibit B*.

Other Steps Taken and To Be Taken

Upon discovering the event, Luttrell Staffing moved quickly to investigate and respond to the incident, assess the security of Luttrell Staffing systems, and notify potentially affected individuals. Luttrell Staffing is also working to implement additional safeguards and training to its employees. Luttrell Staffing is providing access to complimentary credit monitoring services for twelve (12) months through Kroll, to individuals whose personal information was potentially affected by this incident.

Additionally, Luttrell Staffing is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4637.

Very truly yours,



Gregory Lederman of
MULLEN COUGHLIN LLC

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Notice of Data Breach - CA residents only)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Professional Personnel Service, Inc., and its affiliated companies, d/b/a Luttrell Staffing Group (“Luttrell Staffing”) is writing to inform you of an event that may impact some of your information. While there is no evidence of any attempted or actual misuse of your information, we are providing you with information about this event, our response, and the steps you may take to further protect your information against identity theft and fraud, should you 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. We are notifying you now because on or about December 27, 2021, this review determined that certain information related to you may have been impacted. This information includes your <<b2b_text_2(name, data elements)>>.

What We Are Doing. The privacy and security of your information is among our 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 our systems. Luttrell Staffing is also working to provide additional training to employees regarding data privacy and security.

While we do not have any indications that fraud or identity theft has occurred as a result of this incident, we are offering twelve (12) months of complementary identity monitoring through Kroll as an added precaution. We also reported this incident to federal law enforcement and are notifying state regulators, as required.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity. Additional information and resources are included in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also activate the complementary identity monitoring available to you at no cost. Activation instructions are enclosed in this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-855-568-2038 Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. You may also write to Luttrell Staffing at 1040 Tidewater Court, Kingsport, TN 37660.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Mary Wagner

Mary Wagner
Chief Operating Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring

Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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 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, 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 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 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.

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 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. There is 1 Rhode Island residents impacted by this incident

EXHIBIT B

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.

**PROFESSIONAL PERSONNEL SERVICE, INC. PROVIDES
NOTICE OF DATA SECURITY EVENT**

Kingsport, TN - February 1, 2022 - 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 or about 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/or 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 1-855-568-2038, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Individuals may also write to Luttrell Staffing at 1040 Tidewater Court, Kingsport, TN 37660 or visit Luttrell Staffing’s website at www.luttrellstaffing.com.

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.