Morgan Lewis

Kristin M. Hadgis
Partner
215.963.5563
kristin.hadgis@morganlewis.com

VIA US MAIL

February 3, 2022

State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Security Incident of UKG as Vendor to PUMA North America, Inc.*

Dear Office of the Attorney General:

This Firm represents PUMA North America, Inc. ("PUMA"), and we are writing to notify you regarding the nature and circumstances of a recent data security incident involving UKG Inc. ("UKG" or "Kronos"), one of PUMA's human resources vendors. As you may know, UKG has announced that it experienced a ransomware attack on its systems. UKG discovered the ransomware attack on or around December 11, 2021, and provided notice to PUMA on January 10, 2022, after discovering that the ransomware attack resulted in the unauthorized disclosure of personal information owned by PUMA.

On December 11, 2021, UKG began experiencing service interruptions in certain of its cloud-based solutions. Immediately upon discovering that UKG was experiencing a potential security incident, UKG took steps to secure the affected environment. Shortly thereafter, UKG determined that UKG was the victim of a ransomware attack. While UKG's investigation of this matter is ongoing, UKG has determined that a malicious actor or actors accessed the cloud-based environment earlier in 2021, stole data from that environment and encrypted the environment. Since the attack was discovered, UKG has been conducting a comprehensive review of the impacted environment to determine whether any individual's personal information was subject to unauthorized access or acquisition. On January 7, 2022, UKG determined that certain files containing personal information relating to PUMA personnel and other individuals were removed from UKG's systems in connection with the security incident. UKG notified PUMA of this determination in the afternoon on January 10, 2022, and shortly thereafter provided the impacted files to PUMA for analysis.

Based on a comprehensive review of the impacted files, PUMA has ascertained that the personal information of 270 New Hampshire residents was impacted. The impacted information varies by individual resident but may include first name, last name, address, email address, social security or tax ID number, gender, marital status, pay information, employment status, employee identification number and/or position code.

UKG informed PUMA that upon discovering the incident, it immediately took steps to reduce the risk to customers and the data in its systems. UKG is working with leading cybersecurity experts and has notified law enforcement. To help prevent similar incidents from happening in the future, UKG informed PUMA that it has implemented and is continuing to implement additional procedures to further strengthen the security of its IT system environments, including expanding the scanning and monitoring program of these environments.

Protecting the privacy and security of personal information is a chief priority of PUMA. PUMA's contracts with UKG require UKG to keep all personal information relating to PUMA confidential and to have all necessary security procedures in place to minimize data security incidents, and PUMA will continue to take steps to ensure that data held by UKG on PUMA's behalf is adequately secured. At this time, PUMA has no evidence that any personal information has been used inappropriately. Nevertheless, PUMA, through UKG, will offer all affected individuals complementary credit monitoring services, identity restoration service, identity theft insurance through Experian's® IdentityWorksSM for a period of 24 months.

Further information about what PUMA has done and what it is recommending to the individuals in question can be found in the enclosed notification that will be sent to the impacted New Hampshire residents via U.S. mail on February 3, 2022.

If you have any questions, please do not hesitate to contact me.

Regards,

Kristin M. Hadgis

Kristin M. Hadgis

Enclosures

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 3, 2022

H4870-L03-0000003 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L03 EMPLOYEE
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample:

UKG Inc., and its affiliates and subsidiaries (collectively, "UKG", "Kronos" or "we"), is a workforce and human resource management services company that provides services to PUMA North America, Inc. ("PUMA"). We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, this letter is to inform you that we were recently the victim of a ransomware attack that involved some of your personal information, which was provided to us in connection with the services we provide to PUMA. This letter explains the incident, the measures we have taken in response and the steps you can take.

What Happened? On December 11, 2021, we began experiencing service interruptions in some of our cloud-based systems. Immediately upon discovering that we were experiencing a potential security incident, we took steps to secure the affected environment. Shortly thereafter, we determined that we were the victim of a ransomware attack. While our investigation of this matter is ongoing, we have determined that a malicious actor or actors accessed the cloud-based environment earlier in 2021, stole data from that environment and encrypted the environment. Since the attack was discovered, Kronos has been conducting a comprehensive review of the impacted environment to determine whether any individual's personal information was subject to unauthorized access or acquisition. On January 7, 2022, Kronos confirmed that some of your personal information was among the stolen data. We notified PUMA of this incident on January 10, 2022.

What Information Was Involved? The personal information involved included your [Extra2].

What We Are Doing? Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we immediately took steps to reduce the risk to customers and the data in our systems. We are working with leading cybersecurity experts and have notified the authorities. To help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures to further strengthen the security of our IT system environments, including expanding the scanning and monitoring program of these environments.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information. At this time, we have no evidence that any personal information has been used inappropriately. However, as a measure of added security and to help protect your identity, we are offering a complimentary 24-month membership to Experian's® IdentityWorks℠. This product provides you with services including credit monitoring, identify restoration, and identity theft insurance. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Extra3]
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 256-3157** by **April 30, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and noncredit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 256-3157**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at **(833) 256-3157**, Monday through Friday between 9:00 a.m. and 11:00 p.m. and Saturday through Sunday between 11:00 a.m. and 8:00 p.m. Eastern Time, excluding some major U.S. holidays.

Sincerely,

Liz McCarron
SVP, Chief Legal Officer

0000003

H4870-L03

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state. You may have the right to place and lift a security freeze on your credit report at no charge. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for District of Columbia and Massachusetts Residents): State law gives you the right to place a security freeze on your consumer reports free of charge. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above. You have the right to place and lift a security freeze on your credit report at no charge.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a resident of the District of Columbia, you can contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, www.oag.dc.gov, 1-202-727-3400 or the FTC to obtain information about steps you can take to avoid identity theft.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. You can contact the Office of the Attorney General or the FTC to obtain information about steps you can take to avoid identity theft.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, 1-914-834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and to the FTC. You can contact the Oregon Department of Justice, Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392.

If you are a Rhode Island resident, you have the right to obtain a police report. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov/, 1-401-274-4400 or file a police report by contacting 1-401-444-1000.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. To place a security freeze on your credit report, please contact the three major credit reporting companies as indicated above. Fees may be required to be paid to the credit reporting agencies for placing a security freeze on your credit report.

In order to request a security freeze, you may need to provide the following information: full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; a copy of a police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if applicable; and any fee(s).

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 3, 2022

H4870-L04-0000004 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 EMP MINOR DEPENDENTS
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Dear Sample A. Sample (as Parent or Legal Guardian of [Extra1]):

UKG Inc., and its affiliates and subsidiaries (collectively, "UKG", "Kronos" or "we"), is a workforce and human resource management services company that provides services to PUMA North America, Inc. ("PUMA"). We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, this letter is to inform you that we were recently the victim of a ransomware attack that involved some of your dependent's personal information, which was provided to us in connection with the services we provide to PUMA. This letter explains the incident, the measures we have taken in response and the steps you can take.

What Happened? On December 11, 2021, we began experiencing service interruptions in some of our cloud-based systems. Immediately upon discovering that we were experiencing a potential security incident, we took steps to secure the affected environment. Shortly thereafter, we determined that we were the victim of a ransomware attack. While our investigation of this matter is ongoing, we have determined that a malicious actor or actors accessed the cloud-based environment earlier in 2021, stole data from that environment and encrypted the environment. Since the attack was discovered, Kronos has been conducting a comprehensive review of the impacted environment to determine whether any individual's personal information was subject to unauthorized access or acquisition. On January 7, 2022, Kronos confirmed that some of your dependent's personal information was among the stolen data. We notified PUMA of this incident on January 10, 2022.

What Information Was Involved? The personal information involved included your dependent's [Extra2].

What We Are Doing? Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we immediately took steps to reduce the risk to customers and the data in our systems. We are working with leading cybersecurity experts and have notified the authorities. To help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures to further strengthen the security of our IT system environments, including expanding the scanning and monitoring program of these environments.

What You Can Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor your dependent's free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your dependent's information. At this time, we have no evidence that any personal information has been used inappropriately. However, as a measure of added security and to help protect your dependent's identity, we are offering a complimentary 24-month membership to Experian's® IdentityWorks℠. This product provides your dependent with services including credit monitoring, identify restoration, and identity theft insurance. To activate your dependent's membership and start monitoring your dependent's personal information please follow the steps below:

- Ensure that you **enroll by**: **April 30, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Extra3]
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **(833) 256-3157** by **April 30, 2022**. Be prepared to provide engagement number **ENGAGE#** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Social Security Number Trace**: Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and noncredit related fraud.
- **Experian IdentityWorks ExtendCARE™:** Your dependent receives the same high-level of Identity Restoration support even after your dependent's Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your dependent's personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **(833) 256-3157**. If, after discussing the situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your dependent's credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your dependent's identity to its proper condition).

Please note that this Identity Restoration support is available to your dependent for 24 months from the date of this letter and does not require any action on your or your dependent's part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

---

[1] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For More Information. We regret that this incident occurred and any concern it may cause you or your dependent. If you have additional questions, please call our dedicated, toll-free call center at **(833) 256-3157,** Monday through Friday between 9:00 a.m. and 11:00 p.m. and Saturday through Sunday between 11:00 a.m. and 8:00 p.m. Eastern Time, excluding some major U.S. holidays.

Sincerely,

Liz McCarron
SVP, Chief Legal Officer

0000004

H4870-L04

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling 1-877-322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com 1-800-525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com 1-800-680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state. You may have the right to place and lift a security freeze on your credit report at no charge. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for District of Columbia and Massachusetts Residents): State law gives you the right to place a security freeze on your consumer reports free of charge. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above. You have the right to place and lift a security freeze on your credit report at no charge.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent).

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office about for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a resident of the District of Columbia, you can contact the Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, www.oag.dc.gov, 1-202-727-3400 or the FTC to obtain information about steps you can take to avoid identity theft.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023. You can contact the Office of the Attorney General or the FTC to obtain information about steps you can take to avoid identity theft.

If you are a Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, 1-914-834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and to the FTC. You can contact the Oregon Department of Justice, Office of the Attorney General, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392.

If you are a Rhode Island resident, you have the right to obtain a police report. You can also contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov/, 1-401-274-4400 or file a police report by contacting 1-401-444-1000.

You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. To place a security freeze on your credit report, please contact the three major credit reporting companies as indicated above. Fees may be required to be paid to the credit reporting agencies for placing a security freeze on your credit report.

In order to request a security freeze, you may need to provide the following information: full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; a copy of a police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if applicable; and any fee(s).