

March 26, 2021

Via Mail

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

Norton Rose Fulbright Canada LLP
1 Place Ville Marie
Suite 2500
Montréal, Quebec
H3B 1R1 Canada

RECEIVED

MAR 29 2021

Julie Himo
Partner
Direct line 514 971 2497
julie.himo@nortonrosefulbright.com

CONSUMER PROTECTION

Tel +1 514 847 6017
nortonrosefulbright.com

Re: *Legal Notice of Information Security Incident*

Dear Sirs or Madams:

We write on behalf of our client, Premier Tech Limited ("**Premier Tech**"), to notify you of a security incident which resulted in the unauthorized access and exfiltration of the personal information of 3 New Hampshire residents, including 1 team member and 2 dependents of a team member.

On January 25, 2021, Premier Tech discovered that it was the victim of a cybersecurity attack by an unauthorized third party by which the malicious actor deployed ransomware to encrypt Premier Tech's technology infrastructure and to exfiltrate data.

Upon detection of the attack, Premier Tech engaged a cyber forensic firm to conduct a comprehensive investigation to determine how the security incident occurred, the scope of such incident and to assist it with remediation efforts.

On February 11, 2021, Premier Tech discovered that the unauthorized third party may have gained access to and may have exfiltrated the personal information of Premier Tech's team members residing in the United States, and immediately undertook an additional investigation to determine the scope of the information affected. Based on the investigation of our internal specialists and outside experts, the following personal information of team members may have been compromised: name, address, gender, date of birth, salary, bank routing and account numbers, bank account names and social security numbers. The following information of dependents of a team member may have been compromised in the incident: name, relationship to the team member, date of birth and social security number.

From the investigation, we have determined that the unauthorized third party had access to Premier Tech's systems between January 13, 2021 and January 25, 2021.

Premier Tech has also conducted a thorough review of the potentially affected records and continues to review existing policies and procedures designed to try to prevent a similar occurrence from happening again.

Office of the Attorney General
March 26, 2021
Page 2

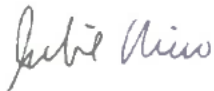
 NORTON ROSE FULBRIGHT

In addition, to help protect the identity of impacted individuals, we are offering a complimentary 2 year membership of Equifax ID Patrol. This product provides superior identity detection and resolution of identity theft. For minors we are offering a complimentary 2 year membership of Equifax Child Identity Monitoring.

All potentially affected individuals will be notified of the incident on March 26, 2021. A copy of the notification letter is enclosed.

If you have any questions or need further information regarding this incident, please contact me (514) 971 2497 or julie.himo@nortonrosefulbright.com.

Very truly yours,



Julie Himo

Enclosure



1, avenue Premier
Campus Premier Tech
Rivière-du-Loup QC G5R 6C1

March 26, 2021

000004

Re: Notice of Privacy Incident

We are writing in regard to a cybersecurity incident at Premier Tech Ltd., concerning information held by itself and its subsidiaries including: Premier Tech Inc., Premier Horticulture Inc., and Premier Tech Prairie Inc. (collectively the “**Premier Tech**”). As a team member of Premier Tech, this incident may have impacted your personal information. We wish to advise you of the steps we are taking to continue to protect your personal information and steps that you can take to help protect your personal information. Your privacy is of the utmost importance to us and we sincerely regret any concern this incident may cause you.

What Happened

On January 25, 2021, we discovered that Premier Tech was the victim of a cybersecurity incident by an unauthorized third party, where the unauthorized third party encrypted Premier Tech’s technology infrastructure and copied and removed some data. Premier Tech immediately undertook an investigation into the source and scope of the breach. On February 11, 2021, Premier Tech discovered that the unauthorized third party may have gained access to and may have exfiltrated certain personal information of certain US Premier Tech’s team members. We immediately undertook an additional investigation to determine the scope of the information affected.

What Information Was Involved

Based on the investigation of our internal specialists and outside experts, the following personal information of certain US team members contained in our database may have been compromised: full name, address, gender, date of birth, social security number, bank routing and account number, salary, hire date, termination date and dependent information.

It is important to note that there is no evidence confirming that all the personal information identified above was compromised or misused. However, as we take the security of our team members and former team members’ personal information seriously, out of an abundance of caution we wanted to notify you of this incident.



What We Are Doing

Upon detection of the incident, Premier Tech engaged a cyber forensic firm to conduct a comprehensive investigation to determine how the security incident occurred, the scope of such incident and to assist with remediation efforts.

Additionally, Premier Tech is providing you with complimentary identity theft and credit monitoring solutions from Equifax free of charge for 24 months. Through this, you will be able to receive regular alerts to notify you if there are significant changes on your credit report.

These services provide you with alerts when changes occur to your Experian, TransUnion and Equifax credit file. This notification is sent to you the same day that the change or update takes place with the bureau.

Your unique activation code for your credit monitoring subscription is [REDACTED]

The activation code will expire on **July 31, 2021**.

To activate your subscription, visit **www.myservices.equifax.com/patrol**

In order to protect against fraudulent access to credit report information, you will be subject to a verification and authentication process. You will need to provide personal information such as date of birth, address and phone number to be successfully authenticated.

Please note that the service requires an internet connection and email account and may not be available to minors under the age of 18.

What You Can Do

We ask that you remain vigilant about any emails, text messages or phone calls asking you to provide sensitive information or click on links or attachments, even if they appear to come from Premier Tech, or an individual that you know or trust. It is not unusual for hackers to use information obtained during a breach to design targeted phishing campaigns.

Please review the "Information About Identity Theft Protection Guide" reference, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

If you have any further questions or concerns, please contact our dedicated call centre at **866-349-3175**

Regards,



Yvan Pelletier
Vice-président principal développement organisationnel
Senior Vice-President Organizational Development
Premier Tech

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
1-800-525-6285 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	1-800-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) social security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: 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. You may submit a declaration of removal to remove information placed in your credit report as a result of being a



victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.



1, avenue Premier
Campus Premier Tech
Rivière-du-Loup QC G5R 6C1

March 26, 2021

000002

Re: Notice of Privacy Incident

We are writing in regard to a cybersecurity incident at Premier Tech Ltd., concerning information held by itself and its subsidiaries including: Premier Tech Inc., Premier Horticulture Inc., and Premier Tech Prairie Inc. (collectively the "**Premier Tech**"). As a dependent of a Premier Tech team member, this incident may have impacted your personal information. We wish to advise you of the steps we are taking to continue to protect your personal information and steps that you can take to help protect your personal information. Your privacy is of the utmost importance to us and we sincerely regret any concern this incident may cause you.

What Happened

On January 25, 2021, we discovered that Premier Tech was the victim of a cybersecurity incident by an unauthorized third party, where the unauthorized third party encrypted Premier Tech's technology infrastructure and copied and removed some data. Premier Tech immediately undertook an investigation into the source and scope of the breach. On February 11, 2021, Premier Tech discovered that the unauthorized third party may have gained access to and may have exfiltrated certain personal information of dependents of certain US Premier Tech's team members. We immediately undertook an additional investigation to determine the scope of the information affected.

What Information Was Involved

Based on the investigation of our internal specialists and outside experts, the following personal information of certain US team members' dependents contained in our database may have been compromised: name, relationship to the team member, date of birth, and social security number.

It is important to note that there is no evidence confirming that all the personal information listed above was compromised or misused. However, as we take the security of our team members dependents' personal information seriously, out of an abundance of caution we wanted to notify you of this incident.



What We Are Doing

Upon detection of the incident, Premier Tech engaged a cyber forensic firm to conduct a comprehensive investigation to determine how the security incident occurred, the scope of such incident and to assist with remediation efforts.

Additionally, Premier Tech is providing you with complimentary identity theft and credit monitoring solutions from Equifax free of charge for 24 months. Through this, you will be able to receive regular alerts to notify you if there are significant changes on your credit report.

These services provide you with alerts when changes occur to your Experian, TransUnion and Equifax credit file. This notification is sent to you the same day that the change or update takes place with the bureau.

Your unique activation code for your credit monitoring subscription is [REDACTED]
The activation code will expire on **July 31, 2021**.

To activate your subscription, visit **www.myservices.equifax.com/patrol**

In order to protect against fraudulent access to credit report information, you will be subject to a verification and authentication process. You will need to provide personal information such as date of birth, address and phone number to be successfully authenticated.

Please note that the service requires an internet connection and email account and may not be available to minors under the age of 18.

What You Can Do

We ask that you remain vigilant about any emails, text messages or phone calls asking you to provide sensitive information or click on links or attachments, even if they appear to come from Premier Tech, or an individual that you know or trust. It is not unusual for hackers to use information obtained during a breach to design targeted phishing campaigns.

Please review the "Information About Identity Theft Protection Guide" reference, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

If you have any further questions or concerns, please contact our dedicated call centre at **866-349-3175**

Regards,



Yvan Pelletier
Vice-président principal développement organisationnel
Senior Vice-President Organizational Development
Premier Tech

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
1-800-525-6285 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	1-800-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) social security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: 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. You may submit a declaration of removal to remove information placed in your credit report as a result of being a

victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.



1, avenue Premier
Campus Premier Tech
Rivière-du-Loup QC G5R 6C1

March 26, 2021

000003

Re: Notice of Privacy Incident

We are writing in regard to a cybersecurity incident at Premier Tech Ltd., concerning information held by itself and its subsidiaries including: Premier Tech Inc., Premier Horticulture Inc., and Premier Tech Prairie Inc. (collectively the "**Premier Tech**"). As a dependent of a Premier Tech team member, this incident may have impacted your child's personal information. We wish to advise you of the steps we are taking to continue to protect your child's personal information and steps that you can take to help protect the personal information. Your child's privacy is of the utmost importance to us and we sincerely regret any concern this incident may cause you.

What Happened

On January 25, 2021, we discovered that Premier Tech was the victim of a cybersecurity incident by an unauthorized third party, where the unauthorized third party encrypted Premier Tech's technology infrastructure and copied and removed some data. Premier Tech immediately undertook an investigation into the source and scope of the breach. On February 11, 2021, Premier Tech discovered that the unauthorized third party may have gained access to and may have exfiltrated the personal information of dependents of certain US Premier Tech's team members. We immediately undertook an additional investigation to determine the scope of the information affected.

What Information Was Involved

Based on the investigation of our internal specialists and outside experts, the following personal information of certain US team members' dependents contained in our database may have been compromised: name, relationship to the team member, date of birth, and social security number.

It is important to note that there is no evidence confirming that all the personal information identified above was compromised or misused. However, as we take the security of our team members dependents' personal information seriously, out of an abundance of caution we wanted to notify you of this incident.

What We Are Doing

Upon detection of the incident, Premier Tech engaged a cyber forensic firm to conduct a comprehensive investigation to determine how the security incident occurred, the scope of such incident and to assist with remediation efforts.



Additionally, to protect your child, Premier Tech is providing you with complimentary child identity monitoring from Equifax free of charge for 24 months. This service provides you with alerts when there are any instances involving your child's social security number or Equifax credit file.

If no social security number match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the child's name and immediately "lock" the Equifax credit file. This will prevent access to the child's Equifax credit file in the future. If Equifax receives a request for your child's Equifax credit report, you will receive an email alert.

If an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file.

The child's Equifax credit file will be locked for 24 months from date of activation. After that time, the child's Equifax credit file will be deleted from our credit database, if it contains no credit data.

Your unique activation code for your child identity monitoring subscription is [REDACTED]
The activation code will expire on **July 31, 2021**.

To activate your subscription, visit **www.myservices.equifax.com/efx1_brminor** and follow the steps below:

1. Register: Parent/Guardian, you must complete the form with your information, then click "Continue".
2. Create Account: Enter your email address and create a password. Check the box to accept the Terms of Use and click "Continue".
3. Verify ID: Answer the security questions to verify your identity and click "Submit Order".
4. Order Confirmation: Click "View My Product" to access the product features.
5. Enroll Child: Click the orange "Enroll Child" button and enter your child's information.
6. Confirm Guardianship: Check the box confirming you are the child's parent or guardian and click "Submit" to complete enrollment.

In order to protect against fraudulent access to credit report information, you will be subject to a verification and authentication process. You will need to provide personal information such as date of birth, address and phone number to be successfully authenticated.

Please note that the service requires an internet connection.

What You Can Do

We ask that you remain vigilant about any emails, text messages or phone calls asking you to provide sensitive information or click on links or attachments, even if they appear to come from Premier Tech, or an individual that you know or trust. It is not unusual for hackers to use information obtained during a breach to design targeted phishing campaigns.

Please review the "Information About Identity Theft Protection Guide" reference, enclosed here, which describes additional steps you may take to help protect your child, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your child's credit file.

For More Information

If you have any further questions or concerns, please contact our dedicated call centre at **866-349-3175**

Regards,



Yvan Pelletier
Vice-président principal développement organisationnel
Senior Vice-President Organizational Development
Premier Tech

Information About Identity Theft Protection Guide

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
1-800-525-6285 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	1-800-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

The following information reflects recommendations from the Federal Trade Commission regarding identity theft protection.

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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. Pursuant to the Economic Growth, Regulatory Relief, and Consumer Protection Act, you may place a fraud alert on your file free of charge.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) social security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: 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. You may submit a declaration of removal to remove information placed in your credit report as a result of being a

victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Federal Trade Commission 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 immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.