MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

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

August 7, 2020

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 Behavioral Health Network, Inc. ("BHN") located at 417 Liberty Street, Springfield, MA 01104, and are writing to notify your office of an incident that may affect the security of some personal information relating to one hundred fifty-two (152) 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, BHN 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 May 28, 2020, certain BHN systems became infected with a virus that prohibited access to its files. Upon discovery, BHN immediately commenced an investigation, which included working with third-party IT and forensic investigators, to determine the full nature and scope of the incident and to secure the BHN network. Through this investigation, BHN determined that an unauthorized actor had placed malware within the BHN environment that disrupted the operation of certain BHN systems. On or about July 17, 2020, BHN's investigation further determined that the unauthorized actor had gained access to certain BHN systems between May 26, 2020 and May 28, 2020. As a result, the unauthorized actor may have had access to certain files within these systems. While the investigation was able to determine these BHN systems were accessed, it was unable to determine whether any specific file containing sensitive information was actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, BHN is notifying all current and former individuals served and employees of this incident because the following types of information were

present in the affected systems: name, address, date of birth, Social Security number, medical/diagnosis/treatment information, and/or health insurance claim information.

Notice to New Hampshire Residents

On or about July 27, 2020, BHN began providing notice of this incident to affected individuals, which includes one hundred fifty-two (152) New Hampshire residents. Written notice is being provided beginning on August 7, 2020 in substantially the same form as the letter attached here as ***Exhibit A***. BHN also posted notice of this incident on its website. A copy of BHN's website notice is attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

Upon discovering the event, BHN moved quickly to investigate and respond to the incident, assess the security of BHN systems, and notify potentially affected individuals. BHN is also working to review existing policies and procedures, to implement additional safeguards, and to provide additional training to its employees.

While the investigation was unable to determine whether any specific file containing sensitive information was actually accessed or acquired by the unauthorized actor, BHN, in an abundance of caution, is providing access to twelve months of credit monitoring and identity restoration services, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, BHN is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising 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 their Explanation of Benefits, account statements, and 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) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/ara

EXHIBIT A

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

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

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

Behavioral Health Network, Inc. ("BHN") writes to inform you of a recent incident that may affect some of your information. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with an overview of the incident, our response, and steps you may take to better protect yourself, should you feel it necessary to do so.

What Happened? The cybercrime industry is an ever growing and changing threat to organizations of all sizes and industries. Like Facebook, Twitter, and countless other organizations, BHN is not immune from these types of incidents. On May 28, 2020, certain BHN systems became infected with a virus that prohibited access to our files. Upon discovery, BHN immediately commenced an investigation, which included working with third-party IT and forensic investigators, to determine the full nature and scope of the incident and to secure our network. Through this investigation, we determined that an unauthorized actor had placed malware within our environment that disrupted the operation of certain BHN systems. On or about July 17, 2020, BHN's investigation further determined that the unauthorized actor had gained access to certain BHN systems between May 26, 2020 and May 28, 2020. As a result, the unauthorized actor may have had access to certain files within these systems.

What Information Was Involved? While the investigation was able to determine these BHN systems were accessed, it was unable to determine whether any specific file containing sensitive information was actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, BHN is notifying you of this incident because you are a <<b2b_text_1(ClientIdentifier)>> and the following types of information related to you were present in the affected systems: <<b2b_text_2(ImpactedData)>>. To date, BHN has not received any reports of actual or attempted misuse of your information.

What Are We Doing? The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we discovered this incident, we immediately launched an investigation and took steps to secure our systems and determine what personal data was at risk. As part of our ongoing commitment to the security of information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We will be notifying state and federal regulators, as required.

As an added precaution, we are also offering you complimentary access to twelve (12) months of credit and identity monitoring services through Kroll. We encourage you to activate these services, as we are not able to act on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What Can You Do. We encourage you to review the enclosed *Steps You Can Take To Help Protect Your Information* for additional steps you may take and information on what you can do to better protect against the possibility of identity theft and fraud, should you feel it is appropriate to do so. You may also activate the free credit and identity monitoring services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-844-930-2836 between the hours of 8:00am and 5:30pm Central Time, Monday through Friday, excluding major U.S. holidays. You may also write to BHN at 417 Liberty Street, Springfield, MA 01104.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Steven Winn, Ph.D.
President and CEO
Behavioral Health Network, Inc.

Steps You Can Take to Help Protect Your Information

Activate Credit and Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. 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.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **November 3, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your Explanation of Benefits and account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT(1-877-438-4338); 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 Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

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 agencies 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 276999001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XX Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

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 will 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.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-844-930-2836 between the hours of 8:00am and 5:30pm Central Time, Monday through Friday, excluding major U.S. holidays. You may also write to BHN at 417 Liberty Street, Springfield, MA 01104.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Steven Winn, Ph.D.
President and CEO
Behavioral Health Network, Inc.

Steps You Can Take to Help Protect Your Minor's Information

Activate Minor Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration at no cost to you for one year. 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.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your Minor Identity Monitoring services.

You have until ***November 3, 2020*** *to activate your Minor Identity Monitoring services.*

Membership Number: <<Member ID>>

Additional information describing your minor's services is included with this letter.

Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your minor's Explanation of Benefits and account statements, and to monitor his or her credit reports for suspicious activity, if he or she has credit files. While minors under the age of eighteen (18) typically do not have credit files, the following information relates to protecting one's credit once established:

Under U.S. law, adults are entitled to one free credit report annually from each of the three major credit bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

Adults have the right to place a "security freeze" on their credit report, which will prohibit a consumer reporting agency from releasing information in their credit report without their express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in consumer's name without their consent. However, you should be aware that using a security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your minor's full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Your minor's Social Security number;
3. Your minor's date of birth;
4. If your minor has moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If your minor is a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, adults 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect your minor by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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 Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

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 agencies 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 276999001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Rhode Island residents, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XX Rhode Island residents impacted by this incident.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF MINOR IDENTITY MONITORING SERVICES

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

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your minor's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

Fraud Consultation

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

Identity Theft Restoration

An experienced Kroll licensed investigator will work on your behalf to resolve issues related to identity theft. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator will be able to dig deep to uncover all aspects 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.

EXHIBIT B

NOTICE OF DATA PRIVACY INCIDENT

Behavioral Health Network, Inc. ("BHN") is providing notice of a recent incident that may affect the security of information for current and former individuals served by BHN. The confidentiality, privacy, and security of information in BHN's care is one of its highest priorities and BHN takes this incident very seriously. To date, BHN has not received any reports of actual or attempted misuse of your information.

What Happened? The cybercrime industry is an ever growing and changing threat to organizations of all sizes and industries. Like Facebook, Twitter, and countless other organizations, BHN is not immune from these types of incidents. On May 28, 2020, certain BHN systems became infected with a virus that prohibited access to its files. Upon discovery, BHN immediately commenced an investigation, which included working with third-party IT and forensic investigators, to determine the full nature and scope of the incident and to secure the BHN network. Through this investigation, BHN determined that an unauthorized actor had placed malware within the BHN environment that disrupted the operation of certain BHN systems. On or about July 17, 2020, BHN's investigation further determined that the unauthorized actor had gained access to certain BHN systems between May 26, 2020 and May 28, 2020. As a result, the unauthorized actor may have had access to certain files within these systems.

What Information Was Involved? While the investigation was able to determine these BHN systems were accessed, it was unable to determine whether any specific file containing sensitive information was actually accessed or acquired by the unauthorized actor. Therefore, in an abundance of caution, BHN is notifying all current and former individuals served of this incident because the following types of information were present in the affected systems: name, address, date of birth, Social Security number, medical/diagnosis/treatment information, and/or health insurance claim information.

What Are We Doing? Upon discovering this incident, BHN immediately launched an investigation and took steps to secure its systems and determine what personal data was at risk. BHN is individually notifying the potentially affected individuals and as an added precaution, providing individuals with access to complimentary credit monitoring and identity protection services. As part of BHN's ongoing commitment to the security of information in its care, BHN is working to review existing policies and procedures, to implement additional safeguards, and to provide additional training to BHN employees on data privacy and security. BHN will also be notifying state and federal regulators, as required.

For More Information. You may have questions about this incident that are not addressed in this letter. If you have additional questions and are impacted by this incident, please call BHN's dedicated assistance line at 844-930-2836 between the hours of 8:00am and 5:30pm Central Time, Monday through Friday, excluding major U.S. holidays. You may also write to BHN at 417 Liberty Street, Springfield, MA 01104.

What Can You Do. BHN sincerely regrets any inconvenience this incident may have caused individuals BHN has served in relation to this matter. BHN encourages you to remain vigilant against incidents of identity theft and fraud, to review your Explanation of Benefits and account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); 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.