BRIAN MIDDLEBROOK
BMIDDLEBROOK@GRSM.COM

GORDON&REES
SCULLY MANSUKHANI
YOUR 50 STATE PARTNER™

ATTORNEYS AT LAW
1 BATTERY PARK PLAZA, 28TH FLOOR
NEW YORK, NY 10004
WWW.GRSM.COM

July 27, 2019

VIA ELECTRONIC MAIL (SECURITYBREACH@ATG.WA.GOV)
Bob Ferguson, Attorney General
Washington State Office of the Attorney General
1125 Washington Street SE
P.O. Box 40100
Olympia, WA 98504-0100

Re: Notification of Data Security Incident
Our File No: 1186678

Dear Attorney General Ferguson:

Our client, Community Psychiatric Clinic ("CPC") provides an array of accredited outpatient mental health treatment and counseling services throughout Seattle and Kings County. CPC understands the importance of protecting the personal information and protected health information provided by its clients and employees and is making this notification to your Office in accordance with applicable law following a recent data security incident.

On or about March 12, 2019, CPC became aware of a potential data security incident involving unauthorized access to one of its employees' Microsoft Office365 ("O365") email accounts. CPC immediately changed all passwords associated with the O365 account, and restored the employee's hard drive, thereby terminating all potentially unauthorized access on March 12, 2019. CPC also implemented additional security measures on this employee's O365 account to prevent any similar incidents from occurring in the future. Lastly, CPC undertook an internal investigation which did not identify any signs of data exfiltration.

On or about May 8, 2019, CPC became aware of a separate potential data security incident involving unauthorized access to another employee's O365 account when a malicious actor attempted to induce CPC to engage in a fraudulent wire transfer of funds. As a result of CPC's immediate efforts to investigate and remediate this event, all funds were recovered. CPC also immediately changed all passwords associated with the employee's O365 account, thereby terminating all potentially unauthorized access on May 8, 2019, and implemented additional security measures on the account to prevent any similar incidents from occurring in the future.

As a result of these events and in an abundance of caution, CPC undertook a comprehensive external forensic investigation of its entire O365 environment to determine the nature of the data security incidents and confirm that all potential unauthorized access had been terminated.

The external forensic investigation concluded that the O365 accounts referenced above, as well as two additional employees' O365 accounts, were potentially compromised. CPC immediately undertook efforts to cease any potential unauthorized access on the two additional identified accounts by changing passwords and implementing additional security measures, thereby terminating all potential unauthorized access on May 29, 2019.

All potential unauthorized access for each of the impacted mailboxes was through Outlook Web Access, significantly reducing the likelihood of large scale data exfiltration. This was confirmed by the external forensic investigation, which did not identify any signs of data exfiltration. The forensic investigation also did not identify any access to CPC's servers or workspaces beyond the access to the four O365 accounts via Outlook Web Access.

In continuing its thorough investigation, CPC also undertook a comprehensive manual review process to identify the specific individuals with personal information and/or protected health information contained in the impacted mailboxes, if any. The forensic investigation and manual review process were completed on July 21, 2019.

Nonetheless, CPC has begun providing notification to all potentially impacted clients and employees *via* written and substitute notice beginning on July 27, 2019 in an abundance of caution, including approximately 6,600 Washington residents.

A sample copy of the notification letter is attached. As noted in the attachment, CPC has included in the notification an offer to provide twelve months of one-bureau credit monitoring services to the affected Indiana residents. CPC has also provided notification of this data security incident to the Department of Health and Human Services/Office of Civil Rights in accordance with HIPAA.

CPC is continuing to work closely with leading security experts to identity and implement measures to further strengthen the security of its system to help prevent this from happening in the future.

Best regards,

GORDON REES SCULLY MANSUKHANI, LLP

/s/ Brian Middlebrook

Brian Middlebrook, Esq.

Enclosures

COMMUNITY PSYCHIATRIC CLINIC
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>><<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

July 26, 2019

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Community Psychiatric Clinic ("CPC") provides an array of accredited outpatient mental health treatment and counseling services throughout Seattle and Kings County. CPC understands the importance of protecting your personal information and protected health information. We are writing to inform you that CPC recently identified and addressed a security incident that may have involved your personal information and/or protected health information. This notice describes the incident, outlines the measures that CPC has taken in response, and advises you on steps you can take to further protect your information.

What Happened?

On or about March 12, 2019, CPC became aware of a potential data security incident involving unauthorized access to one of its employees' Microsoft Office365 ("O365") email accounts. CPC immediately changed all passwords associated with the O365 account, and restored the employee's hard drive, thereby terminating all potentially unauthorized access on March 12, 2019. CPC also implemented additional security measures on this employee's O365 account to prevent any similar incidents from occurring in the future. Lastly, CPC undertook an internal investigation which did not identify any signs of data exfiltration.

On or about May 8, 2019, CPC became aware of a separate potential data security incident involving unauthorized access to another employee's O365 account when a malicious actor attempted to induce CPC to engage in a fraudulent wire transfer of funds. As a result of CPC's immediate efforts to investigate and remediate this event, all funds were recovered. CPC also immediately changed all passwords associated with the employee's O365 account, thereby terminating all potentially unauthorized access on May 8, 2019, and implemented additional security measures on the account to prevent any similar incidents from occurring in the future.

As a result of these events and in an abundance of caution, CPC undertook a comprehensive external forensic investigation of its entire O365 environment to determine the nature of the data security incidents and confirm that all potential unauthorized access had been terminated.

The external forensic investigation concluded that the O365 accounts referenced above, as well as two additional employees' O365 accounts, were potentially compromised. CPC immediately undertook efforts to cease any potential unauthorized access on the two additional identified accounts by changing passwords and implementing additional security measures, thereby terminating all potential unauthorized access on May 29, 2019.

All potential unauthorized access for each of the impacted mailboxes was through Outlook Web Access, significantly reducing the likelihood of large scale data exfiltration. This was confirmed by the external forensic investigation, which did not identify any signs of data exfiltration. The forensic investigation also did not identify any access to CPC's servers or workspaces beyond the access to the four O365 accounts via Outlook Web Access.

In continuing its thorough investigation, CPC also undertook a comprehensive manual review process to identify the specific individuals with personal information and/or protected health information contained in the impacted mailboxes, if any. The forensic investigation and manual review process were completed on July 21, 2019.

What Information Was Involved?

Ultimately, the data security incidents described above may have resulted in unauthorized access to personal information and/or protected health information, including names, dates of birth, Social Security numbers, diagnosis information, treatment information and claims/financial information. CPC is providing this notification to you because, through its comprehensive forensic investigation and manual review process, your personal information and/or protected health information was identified as being located in one of the impacted mailboxes. Please note that it is entirely possible that your personal information and/or protected health information may not have been compromised as a result of the incident. Nonetheless, we are providing you with this notification in an abundance of caution.

What We Are Doing

As stated above, upon learning of a potential data security incident for each of the impacted mailboxes, CPC immediately undertook efforts to eliminate any potential unauthorized access by changing all passwords associated with the accounts and implementing additional security measures on the accounts to prevent any similar incidents from occurring in the future. CPC is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Additionally, we are offering you a free 12-month membership to EquiFax Credit Watch credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product also includes various features such as identity theft insurance with no deductible, subject to policy limitations and exclusions. EquiFax Credit Watch is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and EquiFax Credit Watch, including instructions on how to activate your complimentary 12-month membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<ENROLLMENT DATE>>.***

What You Can Do

We are aware of how important your personal information and protected health information is to you. To protect yourself from potential harm associated with this incident, we encourage you to closely monitor all mail or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also ask that you report any such activity, or any suspicious contact whatsoever, to CPC, as well as to law enforcement if warranted.

Under the Health Insurance Portability and Accountability Act, we note that protected health information is defined as individually identifiable information transmitted or maintained in electronic media or any other form or medium, including demographic information collected from an individual, and relates to the past, present, or future physical or mental health conditions, provision of health care, or payment for health care to an individual.

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies.

In order to request a security freeze, you may 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.); and
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.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of ordering a copy of your credit report:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of placing a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Other Important Information

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Hawaii, Michigan, Missouri, New Mexico, North Carolina, Virginia, Vermont, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Maryland and West Virginia: It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected incidents of identity theft to local law enforcement or the Attorney General.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois and North Carolina: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630
www.illinoisattorneygeneral.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

For residents of New Mexico: Pursuant to the Fair Credit Reporting Act, you have 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 violators. 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 Avenue NW, Washington, DC 20580.

For residents of Rhode Island: We believe that this incident may have affected _0_ Rhode Island residents.

For More Information

CPC understands the importance of protecting your personal information, and deeply regret any concern this may have caused to you. CPC remains committed to protecting your personal information and personal health information. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 877-804-6420** Monday through Friday from 9am to 9pm ET.

In the event that the call in center is unable to assist with your questions, we invite you to contact CPC directly at (206) 461-3614.

Sincerely,

Douglas Crandall
Chief Executive Officer, Community Psychiatric Clinic

Enter your Activation Code: <*INSERT ACTIVATION CODE*>

Product Information

Equifax® Credit Watch™ Gold provides you with the following key features:

- Equifax® credit file monitoring with alerts to key changes to your Equifax Credit Report
- Automatic Fraud Alerts[1] With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit
- Wireless alerts (available online only) Data charges may apply.
- Access to your Equifax® credit report
- Up to $25,000 Identity Theft Insurance[2]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instruction

To sign up online for online delivery go to www.myservices.equifax.com/gold

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

To sign up for US Mail delivery, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.

2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.

3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your Equifax credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.

4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

1. The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

2. Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions and exclusions of coverage. Coverage may not be available in all jurisdictions.

COMMUNITY PSYCHIATRIC CLINIC
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Name 1>><<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

July 26, 2019

NOTICE OF DATA BREACH

Dear <<Name 1>>:

Community Psychiatric Clinic ("CPC") provides an array of accredited outpatient mental health treatment and counseling services throughout Seattle and Kings County. CPC understands the importance of protecting your personal information and protected health information. We are writing to inform you that CPC recently identified and addressed a security incident that may have involved your personal information and/or protected health information. This notice describes the incident, outlines the measures that CPC has taken in response, and advises you on steps you can take to further protect your information.

What Happened?

On or about March 12, 2019, CPC became aware of a potential data security incident involving unauthorized access to one of its employees' Microsoft Office365 ("O365") email accounts. CPC immediately changed all passwords associated with the O365 account, and restored the employee's hard drive, thereby terminating all potentially unauthorized access on March 12, 2019. CPC also implemented additional security measures on this employee's O365 account to prevent any similar incidents from occurring in the future. Lastly, CPC undertook an internal investigation which did not identify any signs of data exfiltration.

On or about May 8, 2019, CPC became aware of a separate potential data security incident involving unauthorized access to another employee's O365 account when a malicious actor attempted to induce CPC to engage in a fraudulent wire transfer of funds. As a result of CPC's immediate efforts to investigate and remediate this event, all funds were recovered. CPC also immediately changed all passwords associated with the employee's O365 account, thereby terminating all potentially unauthorized access on May 8, 2019, and implemented additional security measures on the account to prevent any similar incidents from occurring in the future.

As a result of these events and in an abundance of caution, CPC undertook a comprehensive external forensic investigation of its entire O365 environment to determine the nature of the data security incidents and confirm that all potential unauthorized access had been terminated.

The external forensic investigation concluded that the O365 accounts referenced above, as well as two additional employees' O365 accounts, were potentially compromised. CPC immediately undertook efforts to cease any potential unauthorized access on the two additional identified accounts by changing passwords and implementing additional security measures, thereby terminating all potential unauthorized access on May 29, 2019.

All potential unauthorized access for each of the impacted mailboxes was through Outlook Web Access, significantly reducing the likelihood of large scale data exfiltration. This was confirmed by the external forensic investigation, which did not identify any signs of data exfiltration. The forensic investigation also did not identify any access to CPC's servers or workspaces beyond the access to the four O365 accounts via Outlook Web Access.

In continuing its thorough investigation, CPC also undertook a comprehensive manual review process to identify the specific individuals with personal information and/or protected health information contained in the impacted mailboxes, if any. The forensic investigation and manual review process were completed on July 21, 2019.

What Information Was Involved?

Ultimately, the data security incidents described above may have resulted in unauthorized access to personal information and/or protected health information, including names, dates of birth, Social Security numbers, diagnosis information, treatment information and claims/financial information. CPC is providing this notification to you because, through its comprehensive forensic investigation and manual review process, your personal information and/or protected health information was identified as being located in one of the impacted mailboxes. Please note that it is entirely possible that your personal information and/or protected health information may not have been compromised as a result of the incident. Nonetheless, we are providing you with this notification in an abundance of caution.

What We Are Doing

As stated above, upon learning of a potential data security incident for each of the impacted mailboxes, CPC immediately undertook efforts to eliminate any potential unauthorized access by changing all passwords associated with the accounts and implementing additional security measures on the accounts to prevent any similar incidents from occurring in the future. CPC is continuing to work closely with leading security experts to identify and implement measures to further strengthen the security of their systems to help prevent this from happening in the future.

Additionally, we are offering you a free 12-month membership to EquiFax Credit Watch credit monitoring service. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This product also includes various features such as identity theft insurance with no deductible, subject to policy limitations and exclusions. EquiFax Credit Watch is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft protection and EquiFax Credit Watch, including instructions on how to activate your complimentary 12-month membership, please see the additional information attached to this letter. ***To take advantage of this offer, you must enroll by <<ENROLLMENT DATE>>.***

What You Can Do

We are aware of how important your personal information and protected health information is to you. To protect yourself from potential harm associated with this incident, we encourage you to closely monitor all mail or other contact from individuals not known to you personally, and to avoid answering questions or providing additional information to such unknown individuals. We also ask that you report any such activity, or any suspicious contact whatsoever, to CPC, as well as to law enforcement if warranted.

Under the Health Insurance Portability and Accountability Act, we note that protected health information is defined as individually identifiable information transmitted or maintained in electronic media or any other form or medium, including demographic information collected from an individual, and relates to the past, present, or future physical or mental health conditions, provision of health care, or payment for health care to an individual.

We remind you to remain vigilant for incidents of fraud or identity theft by reviewing account statements and credit reports for unauthorized activity. Residents of the United States are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

You may want to consider placing a fraud alert on your credit report. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. A fraud alert does not impact your ability to get a loan or credit, but rather alerts a business that your personal information may have been compromised and requires the business to verify your identity before issuing you credit. Although this may cause some delay if you are applying for credit, it may protect against someone else obtaining credit in your name. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies. The agency that you contacted must notify the other two agencies.

Additionally, you have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, 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 security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. However, unlike a fraud alert, you must separately place a security freeze on your credit file at each of the three national credit reporting agencies.

In order to request a security freeze, you may 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.); and
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.

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of ordering a copy of your credit report:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Below are the toll-free numbers and addresses for the three largest credit reporting agencies for purposes of placing a security freeze on your credit file:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

Other Important Information

Below is the toll-free number, address and website address for the Federal Trade Commission, which you may contact to obtain further information on how to protect yourself from identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For residents of Hawaii, Michigan, Missouri, New Mexico, North Carolina, Virginia, Vermont, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Maryland and West Virginia: It is required by state law to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report using the contact information listed above.

For residents of Iowa: State law advises you to report any suspected incidents of identity theft to local law enforcement or the Attorney General.

For residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois and North Carolina: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General
Consumer Protection
150 South Main Street
Providence, RI 02903
1-401-274-4400
www.riag.ri.gov

Office of the Illinois Attorney General
Identity Theft Hotline
100 W Randolph St, Fl. 12
Chicago, IL 60601
1-866-999-5630
www.illinoisattorneygeneral.gov

North Carolina Office of the Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Rhode Island and West Virginia: You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed above.

For residents of New Mexico: Pursuant to the Fair Credit Reporting Act, you have 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 violators. 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 Avenue NW, Washington, DC 20580.

For residents of Rhode Island: We believe that this incident may have affected _0_ Rhode Island residents.

For More Information

CPC understands the importance of protecting your personal information, and deeply regret any concern this may have caused to you. CPC remains committed to protecting your personal information and personal health information. **Should you have any questions and would like further information regarding the information contained in this letter, please do not hesitate to contact 877-804-6420** Monday through Friday from 9am to 9pm ET.

. In the event that the call in center is unable to assist with your questions, we invite you to contact CPC directly at (206) 461-3614.

Sincerely,

Douglas Crandall
Chief Executive Officer, Community Psychiatric Clinic

Enter your Activation Code: <*INSERT ACTIVATION CODE*>

Product Information

Equifax Child Identity Monitoring will scan the Equifax credit database for any instances of the minor's social security number and look for a copy of the minor's Equifax credit file.

- If no SSN match is found and no Equifax credit file exists, Equifax will create an Equifax credit file in the minor's name and immediately "lock" the Equifax credit file. This will prevent access to the minor's Equifax credit file in the future. If Equifax receives a request for your minor's Equifax credit report, you will receive an email alert.
- If there is a match and an Equifax credit file exists, Equifax will immediately "lock" the file and alert you to activity against the file, such as an attempt to open a new line of credit.
- The minor's Equifax credit file will be locked for 12 months from date of activation. After that time, the minor's Equifax credit file will be deleted from our credit database if it contains no credit data.

Enrollment Instructions

To enroll in Equifax Child Identity Monitoring go to http://myservices.equifax.com/efx1_brminor and follow the instructions below:

1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with **YOUR** contact information first (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept the Terms of Use and click the "Continue" button.

4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

6. Click the orange button "Enroll Child" to enter your child's information (child's name, Date of Birth and Social Security Number). Note: if you enter the child's SSN incorrectly, you will need to remove the minor by going to your Member Center and clicking on "My Account" to remove the minor from the account. You may then re-enroll the minor with the correct SSN.

7. Check the box confirming you are the child's parent or guardian.

8. Click "Submit" to enroll your child.