



77 Court Street, Bangor, ME 04401

April 25<sup>th</sup>, 2017

Client Name  
Address  
City, State, Zip

Re: **Behavioral Health Center (“BHC”)  
Notice of Unauthorized Access to Confidential Personal Health Information**

Dear Client:

**Please read this letter in its entirety.** You are receiving this letter because either you or your minor child have been a client of Behavioral Health Center (“BHC”).

We take the confidentiality, integrity and security of our client’s personal data very seriously. Unfortunately, we recently learned that despite our secure systems and processes maintained to protect that data, an unauthorized hacker gained illegal access to BHC’s computer system and files containing client records. When we became aware that this may have occurred, we took immediate steps to investigate. We have confirmed that the unauthorized access occurred on March 14, 2017. We also learned that your personal information was included in the files that were hacked. The accessed information includes the fact that you are or were a client, notes regarding the services provided and related information, your address, date of birth, Social Security number and phone number.

**BHC is taking steps to address this situation.**

Behavioral Health Center is providing you with access to ***Triple Bureau Credit Monitoring\**** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. These services will be provided by **CyberScout**, a company that specializes in identity theft education and resolution.

**Here is how to enroll for the free services:**

To enroll in **Credit Monitoring\*** services at no charge, please log on to [https://www.myidmanager.com/promo\\_code.html](https://www.myidmanager.com/promo_code.html) and follow the instructions provided. When prompted please provide the following unique code to receive services:

**NOTE THAT YOU MUST ENROLL PRIOR TO JULY 28, 2017 TO RECEIVE THESE FREE SERVICES.**

For guidance with the CyberScout services, or to obtain additional information about these services, **please call the CyberScout help line at 1-800-405-6108** and supply the fraud specialist with your unique code.

**Here are things you can do on your own to address this situation:**

If you choose not to use credit monitoring service outlined above, **we strongly urge you to do the following:**

**A. Place a fraud alert on your credit file. To do this you will need to contact one of the three major credit agencies directly. *Fraud alerts last for 90 days.***

<b>Experian (1-888-397-3742)</b> P.O. Box 4500 Allen, TX 75013 www.experian.com	<b>Equifax (1-800-525-6285)</b> P.O. Box 740241 Atlanta, GA 30374 www.equifax.com	<b>TransUnion (1-800-680-7289)</b> P.O. Box 2000 Chester, PA 19016 www.transunion.com
--	--	--

**B. Obtain and review your credit report.**

You can get your free credit reports from [annualcreditreport.com](http://annualcreditreport.com). Check the report for any accounts or inquiries you don't recognize. You can order a free report from each of the three credit reporting companies once a year.

***Be sure to promptly report any suspicious activity to CyberScout.***

**C. Consider "Freezing" your credit report.**

With certain specific exceptions, a security freeze prohibits a credit reporting agency from releasing your credit report or any information from it without your express authorization. This means that lenders will not be able to see your credit file and will likely not issue credit. You will still be able to get credit for yourself and allow potential employers to run a background check.

The freeze goes into effect five (5) business days after the credit reporting agency has received notification. After 10 business days from receiving your request to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a

safe place. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name. A security freeze is free to identity theft victims who have a police report, investigative report or a complaint to a law enforcement agency concerning identity theft.

**D. Be wary of solicitors.** Don't believe anyone who calls and says you'll be arrested unless you pay for taxes owed or for other debt — even if they have part or all of your Social Security number, or they say they're from the IRS.

**E. Get additional information regarding steps to take to guard against identity theft or fraud.** You can look on the Maine Attorney General's website at [www.maine.gov/ag/privacy/index.shtml](http://www.maine.gov/ag/privacy/index.shtml) and at the Federal Trade Commission's website at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft). You can also call the Federal Trade Commission's Identity Theft Hotline at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**There are additional steps for you to take if this situation involves your minor child:**

For your minor child, there are additional steps and precautions that can be taken to help manually monitor and protect their information. BHC is making available services that will provide you with special assistance to deal with the exposure of this information, as credit monitoring tools are not available for minor children due to the fact that they should not have a credit file before age 18. This includes assistance with placing a Protected Consumer Security Freeze with the credit bureaus to provide proactive protection. Fees will apply depending on the state in which the minor resides.

To take advantage of the CyberScout services, or to obtain additional information about these services, **please call the CyberScout help line at 1-800-405-6108** and supply the fraud specialist with your child's unique code.

**Dependent:                      Code:**

**If you choose not to use these services, we are recommending that you ensure that no credit file exists in the name of your minor child by contacting each of the three major credit agencies at the phone numbers listed above.**

Please know that Behavioral Health Center acted immediately upon discovery of the potential unauthorized access to the system, to retain information technology experts to investigate whether such access had occurred, the cause, and the nature and extent of the breach. Systems were promptly shut down, remote access was disabled, and upon discovery of the source of the access, the file was disabled to prevent further internet access. We are working with the same IT and forensics experts to implement heightened security measures, to minimize if not entirely remove the risk of any future unauthorized access to the BHC systems

We understand that this incident will be concerning for you, especially given the potential inconvenience as well as future risk. We sincerely regret that this situation has occurred and offer our apologies as we continue to work to remedy and address the incident. For example:

- We have contacted the Federal Bureau of Investigation, to report the incident and to explore whether the hacker can be identified, and whether the stolen information can be retrieved;
- We are continuing our own internal forensics investigation, and the use of third party IT consultants, to evaluate and implement measures to prevent any such future occurrence;
- We are updating our internal operational, technology, and security systems to improve internal monitoring of potential threats to our system.

BHC will be doing everything within our means to facilitate protecting you and your data going forward.

Sincerely,

William Donahue