



COGNITIVE BEHAVIOR THERAPY CENTER

Notice of Third Party Data Breach

October 14, 2026

To Our Valued Patients:

The purpose of this letter is to notify you of a recent data breach our third party billing company, Express Billing Systems, experienced that may have involved some of your personal health information (PHI). We want to provide you with details regarding this incident, Express Billing Systems' response, and our response.

What Happened:

On August 24, 2026, Express Billing Systems became aware of a data breach incident via unauthorized access to their computer systems. The unknown entity had access to their system and encrypted their computer system. A ransom was demanded but was not paid. Upon discovering the breach, Express Billing Systems immediately disabled any access and worked with forensic investigators to rebuild the system. Some data with PHI was taken by the unknown entity. Additionally, the unknown entity has contacted some patients and clients in an attempt to extort money.

What Information Was Involved?

The compromised information includes PHI such as name, address, phone number, social security number (depending on insurance carrier) and, in some cases, information about services rendered and diagnosis.

What We Are Doing:

Express Billing Systems: Per communication we have received from Express Billing Systems, they are continuing to work diligently to further strengthen the security of their systems to the highest possible level.

Cognitive Behavior Therapy Center: We are also working to

**Your partners
in mental health.**

860 Greenbrier Circle
Suite #208
Chesapeake, VA 23320

(757) 410-0700
hello@mycbtcenter.com
www.mycbtcenter.com

continually strengthen and adapt our security systems to the ever evolving world of cybersecurity and cybercrime. We are instituting regular training designed to increase our administrative staff and clinicians' knowledge of cybersecurity, increasing their ability to recognize potential phishing attacks, and maintaining security. Additionally, all staff and clinicians are required to utilize 2-factor authentication in an effort to further increase security and reduce future risk for cyberattacks.

What You Can Do:

Attached to this letter is information and steps that you can take to protect your information and prevent fraudulent use of your credit and other financial resources.

Please, do not hesitate to call our office (757.410.0700) or Express Billing Systems (757.410.8954) if you have any questions and/or concerns.

Thank you,

A handwritten signature in black ink that reads "Brittany L. Montes, Psy.D." The signature is written in a cursive, flowing style.

Brittany L. Montes, Psy.D.
Licensed Clinical Psychologist
President, Co-Owner
VA License #: 0810005191, IN License #: 2004378A, APIT License #: 11541

Recommended Steps to Help Protect Your Information

- 1. Review your credit reports.** We recommend that you remain vigilant by regularly reviewing account statements and credit reports. Federal law entitles individuals to one free credit report from each of the three major credit reporting companies every 12 months. To obtain your annual free copy of your credit report, go to www.annualcreditreport.com or call 1.877.322.8228. You may wish to stagger your requests so you receive a free report every four months.

You should know that you have the right to file a police report if you ever experience identity theft. Please note that in order to file a criminal or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can also report suspected incidents of identity theft to local law enforcement or to the Attorney General.

- 2. Place Fraud Alerts.** The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts and/or change your existing accounts. To place an alert, contact any one of the three major credit bureaus. Once one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. The alert may be renewed after one year.

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you do not recognize as these can be signs of identity theft. If your personal information has been misused, visit the FTC's site at identitytheft.gov to report the identity theft and find recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit report periodically so you can spot problems and address them quickly.

- **Equifax**
 - equifax.com/personal/credit-report-services
 - 1.800.685.1111
- **Experian**
 - experian.com/help
 - 1.888.397.3742
- **TransUnion**

- transunion.com/credit-help
- 1.888.909.8872

- 3. Security Freeze.** A credit freeze means potential creditors cannot obtain your credit report. This makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus (listed above). A freeze will remain in effect until you ask the credit bureau(s) to temporarily lift it or to remove it. There is no cost to freeze and/or unfreeze your credit files. However, please keep in mind that you will be unable to open new accounts or borrow money in your name while the freeze is in place (you will either need to temporarily lift or fully remove the freeze in order to pursue new accounts).
- 4. Additional Information:** Additional information regarding steps you can take to avoid identity theft can be found at identitytheft.gov/databreach. Finally, the FTC encourages those who discover their information has been misused to file a complaint with them.