COVID-19 AND OTHER VIRUSES

STEPS BFG IS TAKING TO ENSURE SAFETY

Updated: March 17, 2020

We have sent several updates on COVID-19 and actions that our clients and contacts should consider taking in the midst of this pandemic, and we will continue to do so. Now we'd like to describe policies that we've had in place at BFG for many years along with some enhancements in an effort give you some reassurance of how we are seeking to protect our staff and clients while we continue to provide support to our clients and their employees.

Office Schedule

Our office will remain open and available for service until further notice. While we're available for in person meetings, out of respect for everyone's need for safety during this time, we will be targeting remote meetings via web conferencing or by telephone to eliminate the need for in-person meetings in most cases. We are watching the CDC reports and recommendations and will be taking a day-by-day approach to decision making about whether and/or when we may need to close our office. We will keep you informed of that.

Health Policies

In order to minimize the risk of spreading illnesses and viruses, such as the flu and COVID-19, we are following the policies below:

1. We are now encouraging remote meetings as an option to all clients, though our office is open for in-person meetings if preferred.
2. We are recommending to clients who are high risk or who have high risk persons living in their home to either meet via phone or postpone meeting if possible.
3. We have a long-standing policy of insisting employees who are sick to stay home. We have reinforced this to include showing symptoms of an illness as well as if they feel they have been exposed to COVID-19.
4. We have been reducing the usage of handouts at meetings over the last several years. We will now only be providing meeting materials and handouts electronically.
5. We are refraining from initiating shaking hands temporarily and are maintaining "social distancing." Each associate has made a commitment to do the same when they are away from the office.
6. We are avoiding serving lunch or drinks in glasses in the office and have recently begun using only disposable plates, cups, utensils internally.
7. We are providing hand sanitizer in all areas of the office.
8. We are regularly sanitizing commonly-touched surfaces in our office and our office conference rooms following meetings.
9. Building management has assured us that they also taking extra precautions in the restrooms and public areas of the building as well.

Working Remotely

We have taken steps for contingency plans in the event that it becomes recommended that our office closes. We have always maintained a supply of computers for remote usage. Recently, we invested in an expanded line up of laptop computers in order that each of our associates will be able to work remotely. These computers we will be used exclusively for work. They are each being outfitted with our secure Virtual Private Network (VPN) so as to be able to maintain the same level of security we have in our current office system.

If and when we were to close our office, our associates will be able to communicate with one another using chat systems, phone forwarding, email and our client databases. We have a developed a regular schedule for internal conferencing to help us with status reports on client work. Our daily work schedules would remain the same, and our commitment to you would not change.

Confidentiality

When working remotely, our associates will be following the same confidentiality protocols as they do at our office. These are covered during initial employee orientation and then we reinforce and train on these regularly. Some of the more key functions include:

- All employees are required to undergo an FBI fingerprint background check.
- All employees sign Confidentiality and Code of Ethics Agreements, which are strictly enforced.
- All employees are required to attend initial and ongoing Compliance training.
- Compliance reminders are regularly shared with all Business Financial Group (BFG) associates.
- All office computers, laptops and flash drives are encrypted and password protected in the event they are lost or stolen.
- Wireless connections are secured and encrypted with software designed specifically to protect data at the highest levels including financial securities transactions.
- All BFG-related work will be conducted through access to the BFG Network through the secure VPN connection.
- No work will be conducted using a computer outside the VPN system.
- No paper files will be taken away from our main office where all confidential files are stored and locked daily.
- Each associate will be required to maintain a designated work place in their home where no other person should have access. Any necessary phone communication will take place behind closed doors.
- Each associate understands that no client information may be shared with any other person outside of BFG personnel. As has always been the case, sensitive information is stored on separate drives with secured access and limited to BFG associates with need-to-know rights.
- Each associate has been trained on the use of passwords and the need for the highest level of strength. Our President and Compliance Officer, Lynn Weirich, is the only person who has access to all passwords in an encrypted password vault.
- Email access via a mobile or any similar device requires Compliance Officer permission and is installed only after Commonwealth Financial Network has encrypted the device and the associate has installed software that will immediately and completely wipe all

data from the device, rendering it useless and inaccessible in the event it is lost or stolen.

IT Controls
Commonwealth Financial Network is a registered broker/dealer and investment adviser that provides Business Financial Group with integrated technology, practice management, investment research, transition support, planning resources and the following data protection services:

- Infrastructure implementation and management.
- Server OS patch management.
- Managed Intrusion Protection System.
- Managed Firewall and VPN.
- Managed Antivirus and Spyware software.
- Encryption for Mobile Devices.
- Managed Exchange server.
- Managed file server.

CRSA is an information technology managed service provider that provides Business Financial Group with Level 3 local IT support, 24/7 managed services and the following data protection services:

- Managed onsite data backups.
- Managed offsite data backups that are AES 256-bit encrypted and SOX and HIPAA compliant.
- Server OS patch management.
- Managed hardware.
- Image-based backups that occur hourly to a Backup and Disaster Recovery (BDR) server in the BFG server room.
- BDR server backups are able to do file recoveries or bare-metal restores to different hardware.
- Image backups on the BDR server are able to be virtualized and spun up as Virtual Machines in the event of an emergency.
- The BDR server backups are encrypted and sent offsite to a CRSA cloud backup provider.
- Data from BDR backups can be accessed by BFG from the CRSA office.
- We have in place a written documented and regularly tested disaster recovery plan to ensure business continuity.

Payroll and Disbursements
CyberPay is a cloud-based application that provides BFG with an interface to process payroll, the tools necessary to streamline payroll processing and the following data protection services:

- All data transferred between CyberPay, CyberPay Online (CPO), and the end client is protected by SSL 2048-bit SHA-2 encryption.
- Data transferred between CyberPay and CPO is protected by multifactor authentication, username, password, and secondary authentication via text or email.
- The entire CPO Phoenix Platform, including the ESS (Employee Self-Serve) portal, is hosted on the Microsoft Azure Cloud Platform in the United States. See attached SOC 3 Report.
- The Microsoft Azure Cloud Platform provides the CPO Platform with managed OS/Hardware updates, and 24/7 support.

- All BFG and End Client data stored on the CPO Platform is backed up every week using a managed backup solution.
- The Microsoft Azure Cloud Platform backs up the CPO Phoenix Platform at the database level in real time.
- All Automated Clearing House (ACH) banking transactions are processed by Kotapay, which is SSAE 18 certified and carries a $50 million dollar crime bond to protect BFG and our clients.

Closing Thoughts

We know that each of you is dealing with this same situation and that you each have different dynamics you are facing. If there is anything we can do to help you, please let us know. Obviously, none of us wishes to be in the situation, but it is our belief that we will come through this together and be better and stronger in spite of it.

We will continue to keep you updated as new information comes out including expanding our Q&A format.

For More Information

We will continue to monitor this situation and release updates. For more information or assistance, please contact our team at **210–495–8474**, toll-free at **1–888–757–2104**, or **Info@BFGonline.com**.

BUSINESS FINANCIAL GROUP

BusinessFinancialGroup.com

210-495-8474 / 1-888-757-2104

Business Financial Group provides corporate services, including human resources consulting, compliance and administration support, payroll and employee benefit program development and maintenance. We also provide group retirement and personal financial planning services.