PRIVATE CLIENT SERVICES™
MEMBER FINRA, SIPC
A Registered Investment Advisor

Compliance Alert – 2024-03

To: All PCS Registered Representatives, Support Staff, Supervisory

Date: Personnel October 7, 2024

Re: **Branch Office Security Policy Guidelines**

The security and protection of customer information cannot be overstated in today's environment. It is not only cyber-attacks that threaten our customer information, but also the manner in which we protect customer information in our daily routines and office security features and controls. Private Client Services has recently reviewed the control guidelines and policies in place for our branch locations and is implementing the following policies to assist our representatives with securing and protecting client information:

Branch Office Access:

Each representative is assigned to a branch location, whether that office is an OSJ, Registered Branch, or Non-Registered Branch Location. Each of these locations must have safeguards in place to secure the location and information contained therein.

Every branch location is expected to have one of the following safeguards in place:

1. A receptionist in place to greet visitors when entering the office location
2. A locked entry door that requires someone within the branch location to allow visitors to enter.

Best practice: When visitors meet at a branch office, they should be identified and recorded:

- Any person entering a branch location should be verified by showing identification at the time of entry.
- The name and time of arrival be entered on a visitor log that is maintained by the branch location.

Corporate headquarters located at
2225 Lexington Road • Louisville, KY 40206
(502) 451 0600

PRIVATE CLIENT SERVICES™

Branch Office Client Data Management:

Branch office physical client files should be maintained in locked file cabinets or a locked storage room at all times.

If client records are maintained in electronic format, the storage drives used to maintain records should be password protected and best practice is to use multi-factor authentication to access the records. Only authorized personnel should be granted access to the client data records.

Visitor Electronic Internet Access:

Many branch offices want to be able to provide visitors/clients with internet access when visiting their branch locations. Internet access should only be provided via a guest Wi-Fi login that is separate and distinct from the branch network access. The guest Wi-Fi should be limited to internet access only.

Under no circumstances should a visitor be permitted to plug a computer into an open office LAN port or connection, or to use the branch network Wi-Fi login. If your office has any open LAN ports they should be disabled from the branch network unless the location with the port is occupied by an approved branch representative or support personnel.

Secure Printing:

Many branch offices utilize shared printers. When printing documents that contain client PII (Personal Identifiable Information), the person printing the document(s) should either use a printer connected locally to their computer or have a print code installed for a shared printer that requires the individual enter the code to activate the print job while at the printer. Never leave a document on a shared printer.

Clean Desk Policy:

Branch offices must be aware of the information left on a desk or conference room table/workspace within the office. If someone with malicious intent visits your office, and client information is left unattended, you are creating an opportunity for that information to be stolen. Office locations have building maintenance people, cleaning people, and many others who may visit the office throughout the day and after hours. Any document with client information, whether applications, notes, or any other document, must be secured before leaving your office or workstation.