Brown ADVISORY
Thoughtful Investing.

Protecting Clients: Information Security at Brown Advisory

From investment research to account administration to client reporting, technology has revolutionized our ability to deliver the performance, advice and service that you need. Unfortunately, we have all seen the evidence in recent years of the security and privacy risks that come along with greater digital connectivity.

Every day, our clients talk to us about the stories they see regarding security-related incidents in the news. We know you worry, and we share your concern—your privacy and confidentiality is of paramount importance to us, and we are constantly at work throughout our organization to ensure the security of your identity and financial data.

Confidentiality is about more than technology

Perhaps the most important promise we make to you is our commitment to safeguard the information you have shared with us in confidence. This promise transcends information technology, and impacts many other aspects of our business. Conversations about clients are discreet, take place behind closed doors, and only involve colleagues directly relevant to a given client situation. Sensitive documents—from digital files to old-fashioned paper statements—are kept in secure areas. Other examples include:

- **Physical access restrictions.** We restrict access to your sensitive information. This information is generally kept behind an actual or virtual locked door, and only those who need to see that data have access.
- **Security audits.** We regularly test our own security systems with periodic audits, to make sure our safeguards are working and to ensure compliance with our own policies and procedures.
- **Redundancy.** For certain tasks, we maintain dual control procedures and segregation of duties—what this means is that multiple individuals must authorize certain sensitive activities.
- **Annual training.** Every year, every single Brown Advisory staff member must undergo training on information security and identity theft issues. We also periodically test the awareness of our staff with "drills" such as mock phishing emails sent to employees by our IT department.

Specifically related to information security, we have an extensive set of risk controls in place. While we cannot disclose the details of the tools and technologies that we use, we are constantly reviewing and evaluating these, and making adjustments as security risks evolve.

- **Security Operations Center (SOC).** Our SOC has broad responsibilities to continually assess and monitor our security measures. The SOC deploys firewalls and other protective layers to safeguard our network, and utilizes a variety of other defensive tools and measures.
- **Third-Party Risk Assessments.** Every year we coordinate external third-party assessments of our information security program. This includes network penetration tests, firewall analysis, policy reviews, and other activities. We use the results and findings from these assessments to help us further strengthen our defenses.

- **Secure transmissions / data loss prevention.** When we transmit communications outside of our network, we have tools that automatically scan our communications, identify emails with sensitive information, and automatically encrypt that information so that it is sent to you safely and securely.
- **Firewalls.** We protect our networks and the sensitive client files within those networks, behind robust firewall systems that are kept up to date.
- **Entitlements.** Our systems provide role-based to access information, which means that individuals can only access data that they are specifically entitled to. Our systems also require those individuals to authenticate their identities to gain that access. These controls help to prevent external actors from obtaining sensitive information through fraudulent means.
- **Systems Monitoring.** Our networks and servers are monitored constantly, to detect cyber-attacks on our critical systems. On real-time basis, our safeguards detect and alert to any cyber-attacks that are directed at Brown Advisory. We closely monitor and respond to these alerts.
- **Systems Management.** We use antivirus software and consult with third-party IT vendors to obtain and install patches that resolve software vulnerabilities. We also have comprehensive backup procedures so that we can restore our data in the event of a system failure. The backups preserve the security, confidentiality and integrity of client information.

A final note: Technology will continue to evolve, but our relationship with you will always be one of the best tools we have to guard you from identity theft or other security breaches. Our relationship with you is personal, which means that even though we use technology, our understanding of your needs allows us to best serve you according to your preferences. We will always endeavor to maintain a close personal connection with you, so that we fully understand your current priorities—and hopefully detect any actions or requests that appear to stray from those priorities.

Please don't hesitate to reach out to your Brown Advisory team if you have additional questions you would like to discuss.