Information Security Brief

CAPTRUST Financial Advisors has prepared this Brief to review the information security strategies currently in place. CAPTRUST is committed to securing all data, with special emphasis on protecting customer information. CAPTRUST's review of information security considered, among other things, the following areas:

POLICIES

CAPTRUST has implemented internal policies to stipulate how employees should handle and care for corporate and client sensitive data. Policies outline strategies for, but is not limited to, access control, password requirements and management, network security and email security. In addition, policies cover acceptable use of the firm's technology in an effort to mitigate potential malicious activity as a direct or indirect result of employee actions.

DATA SECURITY STRATEGY

Access to the CAPTRUST internal LAN is limited to CAPTRUST-owned and approved devices so that we can control what happens on our network. Client data is restricted via access control to only those employees requiring access to service the accounts.

Application and database servers reside on VLANs which are segmented from the rest of the network; physical and remote access to all servers and network equipment is restricted to senior IT staff. Our CRM database and client files are housed on SAN storage which employs self-encrypting solid state drives using AES- 256 encryption algorithm. Client portal access is secured over HTTPS using RSA 2048 encryption.

Our email infrastructure employs Transport Layer Security (TLS) as the preferred method of delivery which creates a secure communication tunnel between our mail server and the recipient's. This secures the message in transit. When sending sensitive data in an email (including attachments), our users employ message encryption technology to ensure the message and contents are secured end to end.

Corporate laptops and desktops are protected by enterprise class anti-virus / anti- malware software and laptops are further protected with full disk hard drive encryption software.

DATA RECOVERY STRATEGY

Our current disaster recovery plan involves performing point-in-time snapshots of all critical data which is stored on-premise for fast recovery. All snapshots are mirrored to an off-premise location daily to ensure recovery should our main site become incapacitated. Test restores are performed and verified periodically throughout the year and have been successful. For redundancy and failover capabilities we have virtualized all mission critical applications and maintain a fully redundant server and storage environment. All data is stored on industry leading SAN storage both on-premise and off-premise.

NETWORK SECURITY

Industry leading firewalls are implemented at the firm's network perimeter as well as at SOHO office locations for VPN tunnel access. Both ingress and egress filtering is employed on the corporate perimeter firewall to restrict inbound access and limit outbound access. Firewall configs are regularly reviewed and internal tests are performed periodically to check for potential security holes. Web content filtering is employed at the Internet egress point to protect against Internet borne malware.

Servers are patched and updated monthly. Critical security updates are applied immediately to protect against vulnerabilities. Annual vulnerability audits are conducted by a third party firm with the findings reviewed and addressed by CAPTRUST staff.

4208 Six Forks Road, Suite 1700, Raleigh, NC 27609
captrust.com | 800.216.0645

CAPTRUST

CAPTRUST COMPLIANCE SUMMARY OF CYBER & INFORMATION SECURITY PROGRAM(S)

INFORMATION TECHNOLOGY	COMPLIANCE	INSURANCE BONDING	AUDIT
CYBER & INFORMATION SECURITY PROGRAM(S)			
Information Security Policy	Privacy & Confidentiality	Errors & Omissions (E&O) and Directors & Officers (D&O) coverage	Independent Financial Audit (annual)
Information Security Incident Response	Anti-money Laundering & Customer Identification	Fidelity (ERISA 3(38) & Crime) Bonding Surety (Signature Medallion Guarantee)	Independent Anti-money laundering (AML) audit (annual)
Information Security Standards	Identity Theft Protection	Cyber-Security insurance	Independent custodial audit and review of Internal Control Procedures (annual)
IT Disaster Recovery Plan	Business Continuity Plan (BCP)	General/umbrella	Compliance team branch audits (periodic)

At CAPTRUST, we are committed to service beyond expectation and we value the confidence our clients place in us.

CAPTRUST has a full-time staff of compliance professionals who supervise the ongoing investment advisory activity of CAPTRUST and its associated persons. Supervision of investment or securities related activity includes (but is not limited to) supervision of all securities transactions, approval of communications with the public (including any advertising, marketing material, correspondence, as well as surveillance of email), recordkeeping, registrations and licensing. CAPTRUST's Chief Compliance Officer and key member of the Compliance Team meet regularly with CAPTRUST's Chief Technology Officer and key members of the IT Department to coordinate CAPTRUST's Information Security Program(s).

CAPTRUST Financial Advisors (also known as CapFinancial Partners, LLC) is an investment adviser registered under the Investment Advisers of 1940 ("40 Act"). Under 40 Act Rules 204-2(b) & 206(4)-2, we are subject to independent audit requirements pertaining to internal control procedures around the processing of client funds & securities and a "surprise" audit under the Custody Rule. Each year, Form ADV E is filed electronically with the US Securities & Exchange Commission by the independent Public Company Accounting Oversight Board (PCAOB) accounting firm of Batchelor, Tillery, and Roberts, PA.

Our annual independent anti-money laundering ("AML") audit is conducted by the compliance consulting firm, Securities Compliance Management, Inc.

Although we are not required by regulation to file a Service Organization Control Report 1 (SOC 1) or SSAE 16, formerly known as SAS 70 Report on Controls, we do undergo several independent and internal audits (summarized in the table above) each year.

Under Rule 17a5 of the Securities Exchange Act, our affiliate, CapFinancial Securities, LLC, is the subject of an annual independent audit of its financial statements, which is filed with the SEC and FINRA within 60 days of the fiscal year end (12/31).

Additional details regarding firewalls, multifactor authentication, access controls, physical security to the facility, DLP, real-time detection and related policies for your review:

We maintain an effective information security program modeled after NIST 800-53 guidelines. These policies are summarized in the enclosed Information Security Brief.

CAPTRUST's policies and procedures are designed to protect clients' Non-Public Information (NPI) and Personally Identifiable Information (PII) from improper disclosure as follows:

- Pursuant to our Privacy Policy, private Client information is accessible to employees on a "need to know" basis. Only those persons who are engaged in client service have access to Client records.
  - Our anti-money laundering and customer identification policies and procedures require employees to exhibit great care and discernment in the handling of private (personal) information of Clients. Employees are trained on these policies annually.
  - CAPTRUST's Information Security Policy outlines the requirements of all personnel and contractors. It is signed upon hire and annually thereafter. CAPTRUST's Information Technology Standards defines technical standards that the Information Technology team must meet for technology assets.
  - The Incident Response Plan addresses how the Firm prepares for and responds to significant threats or disruptions. There are four incident response sub-plans that collectively define how the Firm constitutes its Critical Incident Response Team (CIRT) and handles Information Technology, Information Security, and Facility or Personnel incidents.
  - The Business Continuity Plan (BCP) addresses how the Firm prepares for and addresses significant events that might impact the ability to provide services to clients. The SEC and FINRA require that we publish a formal BCP and that it be tested annually, subject to audit and review.

    Our current BCP for system failures involves either delegated responsibility for SaaS applications as validated by SOC Audit, or replicated servers between data centers using advanced replication technology. This failover process typically completes in under 2 minutes (RTO) with data loss limited to 5-10 seconds (RPO). We also can restore servers from snapshot backups as necessary.

    In the event of a site disaster, we have a dedicated DR suite workspace at TierPoint in Raleigh that can house 16 people with capability to expand to 48. The DR suite is serviced by the data center's generators, fuel resupply arrangements, and is capable of withstanding a direct hit by 150 mph winds.

TECHNOLOGY

- **Data Centers:** CAPTRUST operates three data centers – within headquarters, within TierPoint's Raleigh co-location facility and within Microsoft Azure U.S. East (Boydton, VA). All data centers have battery backup (UPS), advanced cooling, generator backup, and multiple independent Internet connections. All data is stored on encrypted storage and backed-up to a separate data center or zone (for Azure). No data is housed outside of the United States and Canada
- **Network:** CAPTRUST's network is protected by Firewalls (Cisco ASA & CloudGenix) with ingress, egress filtering and intrusion protection. Cisco ISE is used to authorize switch port access and controls wireless access to corporate devices. All LANs are configured with multiple VLANs to segregate access and allowable protocols. Guest Wi-Fi is segregated from the corporate Wi-Fi traffic and is offered only to Clients or guests who appear in person at our offices for a limited duration of time with a unique ID.

  A cloud-based SIEM collects logs from all perimeter devices, servers, and endpoints (key authentication and resource access traffic). 24-months of log data is retained with 9-months being actively processed for additional detection of APTs.

- **Servers:** All servers are virtualized with VMWare (only domain controllers and one of two phone systems are standalone). All servers use Crowdstrike. ACLs protect servers from unauthorized traffic and prevent servers from accessing the Internet unless necessary. Portal applications appropriately hash and salt passwords using modern, core .NET functionality. All endpoints are Windows Server 2012 or newer, patched regularly (21-day rotating schedule), and validated with Tenable / Nessus.
- **Endpoints:** All identity is managed via Okta Federated Identity Manager which allows for Single-Sign On (SSO) and SAML with all external applications. All endpoints are Windows 10, patched regularly (21-day rotating schedule), and validated with Tenable / Nessus. All endpoint drives are encrypted with Bitlocker with AES-256, validated and monitored by Crowdstrike which also provides anti-virus protection. No USB devices are allowed other than FIPS-compliant Apricorn USB drives which require an 8 digit PIN to access and erase after multiple failure attempts. All endpoints access the Internet via ZScaler Internet Access proxy which blocks poisoned DNS attacks, decrypts SSL traffic, blocks advanced threats, and provides for employee supervision. ZScaler Private Access is being used for VPN access. Public-facing websites use EV-SSL certificates.
- **Email:** All email filtered through Mimecast before being delivered to Office 365 where it scanned a second time. All URLs within email are rewritten to prevent direct execution of links. A proxy examines all rewritten URL links for reputation and malware before allowing the end-user to hyperlink. All email is sent via TLS by default and can be required on a Client-by-Client basis if so desired. Email containing sensitive information will be sent via the Mimecast Secure Message Gateway where it requires a browser and credentials to access. Every email is archived for a minimum of six years within GlobalRelay (per the Investment Advisers Act of 1940 and the Securities Exchange Act of 1934).
- An annual security assessment and penetration test of CAPTRUST's network and servers is performed by an external party.

COMPLIANCE

Compliance audits all email (inbound and outbound) using algorithms to detect complaints and suspicious activity in addition to random audits of a sample of all email. Compliance scans personal drives on a rolling basis to detect any misuse of private client information.

Questions about our Cyber-Information Technology Program(s) may be directed to Jon Meyer, our Chief Technology Officer, at (919)870-6822, ext 10407 or by email at jon.meyer@captrust.com, or Nick Brezinski, Senior Manager | Information Security at (919)870- 6822, ext 10308 or by email at nick.brenzinski@captrust.com or our Chief Compliance Officer, Denise Buchanan, may be reached at (919)870-6822, ext 10267 or by email at compliance@captrust.com.