RMB Capital is committed to protecting its employees, investors, clients and data from nefarious acts and threats posed by cyber criminals, malicious individuals/entities, and hackers. During this time of global uncertainty, we are writing to provide an overview of our security and business continuity practices.

Cybersecurity Program

RMB maintains a formal cybersecurity program structured around the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and works diligently to keep your financial information secure. We believe it is the responsibility of everyone at the firm to contribute to the efforts of safeguarding critical data and assets and that this is not achieved through a single solution or action, but rather requires a combination of processes, tools, and awareness. To that end, some of the measures taken to enhance RMB's security stance include:

- Conducting mandatory cybersecurity training and testing for all employees on a semi-annual basis. The training program covers all relevant topics in the cybersecurity space and is designed to reduce human-related security incidents by educating employees to recognize present day cyber-attacks. **Education is considered paramount in preventing cybersecurity threats**.
- Implementing an Artificial Intelligence/Machine Learning-based tool that is based on the principles of the human immune system to ward off cyber threats. The solution is self-learning, detecting novel threats without using prior assumptions of what "malicious" activity looks like and is constantly monitoring our users, networks, communications and certain cloud applications for anomalous activities.
- Forming an Incident Response Team (IRT) that assesses and responds to cyber threats, ensuring that they are addressed by the appropriate parties and documented/reported as necessary.
- Enforcing TLS encryption with key partners and service providers for all email communications. The firm has a secure messaging platform and document vault in place for exchanging any sensitive data with clients when enforcing TLS encryption over email is not possible.
- Use of multi-factor authentication and 256-bit encryption for remote connectivity and access to cloud applications including email, forced password resets and least privileged access to systems/data.
- Conducting weekly exterior vulnerability scans and leveraging our managed service provider to also monitor our network.

- Patching servers, workstations, and software monthly using a centralized patch management process. Critical and high severity patches are applied as soon as possible.
- Endpoint protection product installed on all company-issued workstations/laptops; all laptop hard drives encrypted to prevent accidental data loss.

Business Continuity Plan

RMB's Business Continuity Plan (BCP) ensures that RMB can continue to meet its fiduciary obligations in the event of an unplanned business disruption, including the loss of critical services (e.g., computing services), loss of office or facility access, or physical facility catastrophe.

- RMB's primary technology production environment, located in Chicago, is replicated to an off-site, SSAE-16 Type 2 and SOC 3 certified co-location data center every 2-3 hours. This includes systems used for trading and portfolio accounting.
- Email and other core systems such as Enfusion (Trading) and Salesforce (CRM) are cloud-based and inherently provide robust business continuity and disaster recovery capabilities.
- All employees have secured and encrypted remote access capability into the core RMB infrastructure and services.
- Tests of RMB's BCP are conducted annually. Additionally, infrastructure tests of the disaster recovery environment are conducted at least quarterly to ensure uptime and operational viability.

Should you have any questions, please contact your RMB representative. We look forward to continuing to serve you and appreciate the opportunity to do so. Thank you.