HOW WE KEEP YOU SAFE

SignatureFD utilizes a multi-layered, multi-tiered Cybersecurity plan comprised of controls and policies that include, but not limited to:

- **Multi-Factor Authentication(MFA)**: An electronic authentication method in which a computer user is granted access to a website or application only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something only the user knows), possession (something only the user has), and inherence (something only the user is). MFA protects the user from an unknown person trying to access their data such as personal ID details or financial assets.

- **Data Loss Prevention (DLP)**: The practice of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.

- **Identity and Access Management**: An essential part of overall IT security that manages digital identities and user access to data, systems, and resources within an organization. IAM security includes the policies, programs, and technologies that reduce identity-related access risks within a business. IAM programs enable organizations to mitigate risks, improve compliance, and increase efficiencies across the enterprise.

- **Secure Email / Email Encryption (TLS)**: A protocol that encrypts and delivers mail securely, for both inbound and outbound mail traffic. It helps prevent eavesdropping between mail servers – keeping your messages private while they're moving between email providers.

- **Employee Cyber Education**: We make sure that our employees know and adhere to our security policies. We require periodic training for all personnel, and those who work directly with customers receive extra training on the latest methods used by criminals to perpetrate identity theft.

- **Security in our offices**: We vigilantly monitor all work areas to prevent theft or unauthorized use of your sensitive information. In addition, authorized personnel can only enter work areas through use of a security badge or PIN.

- **Managed Detection and Response (MDR)**: A cyber solution we leverage to effectively detect, respond, and recover from cyberattacks. Solution includes 24x7 security monitoring with broad visibility into our environment, threat hunting, incident response and remediation, and strategic guidance by skilled security experts to enhance our security and compliance posture.