This Agreement is made and entered into effective ___4/30/20___ ("Effective Date") by and between Fogarty Service ("Supplier") and _____Neric_____ ("Client")

Data Security and Privacy

A. **Security Plan.** Supplier shall adhere to a coherent, complete set of information security policies, standards, and practices as requested and outlined by Client in SOWs or agreements, which shall be in conformity with this agreement and legal, regulatory and industry standard best practices Including but not limited to: authentication and authenticator protection, network monitoring and protection, data encryption, intrusion detection and countermeasures, system and network monitoring, security testing, and incident response. Supplier's information security policies, standards, and practices shall include provisions for the periodic assessment of the same.

B. General Requirements.

(1) Supplier agrees to comply with all of Client's security and risk management requirements as requested and outlined by Client in SOWs or agreements, in relation to the security of Clients computing environment, including any subsequently agreed to security plan or information processing requirements that may be embodied in the applicable Statement of Work or in a separately executed information security plan, explained In greater detail in subsection 2, below. Supplier agrees and understands that security and risk management requirements may be changed by Client from time-to-time, and Supplier agrees to abide by Client's then-current security requirements. Supplier further agrees to fully cooperate with Client's reasonable requests for additional information pertaining to Supplier's security environment.

(2) Supplier shall treat Client information and systems as strictly confidential and shall assure the confidentiality and maintain the accuracy and integrity of Client information and systems in a manner consistent with Supplier's defined Information security policies, standards, and practices.

(3) Supplier will submit to periodic assessment of Supplier's security policies, standards, and practices by Client, make reasonable efforts to resolve deficiencies noted as a result of these assessments in a manner commensurate to the risk those deficiencies represent, and notify Client of any material changes to its security policies, standards, and practices.

(4) Supplier will promptly notify Client of any Supplier financial distress, catastrophic events and significant incidents, including but not limited to; information and data loss breaches (even If Client data or Information is not involved), service or system Interruptions, compliance lapses, enforcement actions, or other regulatory actions.

C. **Security Breach.** If supplier experiences an actual security breach or suspects that a security breach has occurred in violation of Supplier's security obligations under this Agreement and the security breach either compromises or could compromise Client's data or confidential information, Including customer or consumer data (e.g., physical trespass on a secure facility, computing systems Intrusion/hacking, loss/theft of a PC (laptop or desktop), loss/theft of printed materials, etc.) (collectively, a "Security breach"), Supplier will immediately notify Client relationship manager and security personnel of such Security breach, and will immediately coordinate with Client's security personnel to investigate and remedy the Security Breach, as directed by such Client's security personnel. Except as may be strictly required by applicable law, supplier agrees that It will not inform any third party of any such Security Breach. Without Client's prior written consent: however, if such disclosure is required by applicable law, Supplier agrees to work with Client at no additional cost to Client regarding the content of such disclosure so as to minimize any potential adverse Impact upon Client and its clients and customers,

D. **Data safeguards.** Supplier, for itself and all Supplier Personnel, shall establish and maintain safeguards against the destruction, loss, alteration of or unauthorized access, to Client data in the possession of Supplier Personnel as requested and outlined by Client in SOWs and agreements. Supplier will implement Client-requested changes to such safeguards on the schedule mutually agreed upon by the Parties. In the event Supplier Personnel Intend to Implement a change to Supplier's data safeguards, Supplier shall notify Client, and upon Client's Written approval, Supplier will Implement such change. Supplier Personnel will retain all information obtained or created In the course of performance under this Agreement in accordance with the longer of the records retention guidelines of Client that may be communicated to Supplier from time to time, or as is required by law