APPENDIX: CLEAR Data Privacy & Security

Exhibit F – Data Privacy & Security

This Exhibit F is agreed to by Partner into pursuant to a certain Service Agreement dated October 5, 2020 between Spreedly, Inc. (referred to in this Exhibit F as "Partner") and Secure Identity, LLC (referred to in this Exhibit F as "CLEAR").

Definitions. For purposes of This Appendix, the following definitions shall apply:

"Breach" means an unauthorized acquisition, destruction, modification, use, or disclosure of, or access to, CLEAR Data.

"**Cardholder Data**" (CHD) - (i) with respect to a payment card, the account holder's name, account number, service code, card validation code/value, PIN or PIN block, valid to and from dates and full track data (magnetic stripe data); and (ii) information relating to a payment card transaction that is identifiable with a specific account.

"**CLEAR Data**" means Personally Identifiable Information and any information regarding the business or business activities of CLEAR or CLEAR Entities (as defined below) that is not available to the general public, or Personally Identifiable Information. For the avoidance of doubt, to the extent the designation of any data or information as CLEAR Data, in This Appendix conflicts with any definition of confidential information within the body of the Agreement, to the fullest extent possible, such conflict shall be interpreted as This Appendix imposing additional or supplemental responsibilities and obligations in connection with such information and not as creating a conflict therewith. To the extent any such conflict cannot be resolved in accordance with the preceding sentence; in accordance with its terms This Appendix shall take precedence and control over any conflict.

"**CLEAR Entities**" means, collectively, Secure Identity, LLC and any entity controlled by, controlling or under common control of Secure Identity, LLC, where control means, having the power, directly or indirectly, to direct or cause the direction of the management and policies of the entity, whether through ownership of securities, contract or otherwise. Alclear Holdings, LLC and all companies in which Alclear Holdings, LLC directly or indirectly owns a majority interest, commonly called "subsidiaries" of Alclear Holdings, LLC, including but not limited to Alclear, LLC, Secure Identity, LLC, NoQue, LLC, Alclarity, LLC, and Alclear PC, LLC.

"**Data Protection Requirements**" means, collectively, all national, state and local laws or regulations relating to the protection of information that identifies or can be used to identify an individual that apply in the jurisdictions in which CLEAR Entities do business and that apply with respect to Partner's handling of CLEAR Data (including, without limitation, the California Consumer Privacy Act) and any self-regulatory programs to which the CLEAR Entities subscribe, relating to the protection of data that identifies or can be used to identify an individual that apply with respect to Partner's handling of CLEAR Data.

"**PCI Requirements Standards**" means the security standards for the protection of payment card data with which the payment card companies require merchants to comply, including, but not limited to, the Payment Card Industry Data Security Standards currently in effect and as may be updated from time to time.

"Personally Identifiable Information" (PII) - any information that identifies or can be used to identify an individual, or that is recorded in any form about an identified or identifiable individual. Personally Identifiable Information may relate to any individual, including, but not limited to, any employee, former employee, service provider, former service provider, customer, prospective customer, former customer, business associates, or former business associates of the CLEAR Entities. Personally Identifiable Information includes, without limitation, names, addresses, telephone numbers, fax numbers, e-mail addresses, data and place of birth, driver's license number, images of driver's licenses, Internet Protocol ("IP") address, passport number, credit card information, frequent flyer and other membership reward program information and affiliations with companies or associations, and information about transactions with CLEAR Entities.

"Security Incident" means an event (or chain of events) that compromises the confidentiality, integrity, or availability of CLEAR's or Partner's data or systems or violates Partner's IT security policies or standards or the requirements of the Agreement.

1. Data Use and Restrictions

1.1. Partner represents and warrants: (i) it will at all times comply with and treat CLEAR Data in accordance with the requirements of this Appendix and the Data Protection Requirements; (ii) it will not use CLEAR Data for its own purposes or for the purpose of any affiliate or third party, except as otherwise permitted under this Appendix; (iii) it will not use CLEAR Data to market its services or those of an affiliate or third party; and (iv) it will not sell or rent CLEAR Data to its affiliates or third parties.

1.2. Partner will hold CLEAR Data in strict confidence and will not, except as may be permitted pursuant to This Appendix, disclose CLEAR Data to any third party, firm or enterprise (including, without limitation, Partner's affiliates) or use (directly or indirectly) any CLEAR Data for any purpose other than as specifically directed by CLEAR in writing and in accordance with the Data Protection Requirements.

1.3. Before providing CLEAR Data to any third party, including, without limitation, Partner's affiliates or a potential subcontractor or service provider, Partner must obtain written approval for such disclosure from an officer of CLEAR. If Partner is permitted to disclose CLEAR Data to such third party, such disclosure must be limited to the minimum CLEAR Data necessary for the third party to fulfill its obligations to Partner. Partner agrees that if CLEAR consents to Partner's disclosure of CLEAR Data to such third party, prior to making such disclosure Partner will enter into a written agreement with the third party that includes obligations that are at least as broad in scope and restrictive as those under This Appendix. Nonetheless, Partner shall remain at all times accountable and responsible for all actions by such third parties with respect to the disclosed CLEAR Data.

1.4. Partner may not physically transfer CLEAR Data to, or allow access to Personally Identifiable Information by, its employees or personnel, including, without limitation, any third party, firm or enterprise (including, without limitation, Partner's affiliates) in any location outside the United States without first receiving CLEAR's prior written consent.

1.5. At no time shall Partner acquire any ownership, license, rights, title or other interest in or to CLEAR Data, all of which shall, as between CLEAR and Partner, be and remain the proprietary and confidential information of CLEAR.

1.6. In the event that Partner is unable to comply with the obligations stated in this Appendix, Partner shall promptly notify CLEAR, and CLEAR shall then be entitled (at its option) to suspend the transfer of CLEAR Data, require Partner to cease using relevant CLEAR Data, request Partner immediately delete the data and upon request certify that such data has been deleted, and/or immediately terminate the Agreement.

2. Legal Disclosures; Requests for Information

2.1. If Partner is requested or required by law to disclose any CLEAR Data to a third party, Partner shall immediately notify CLEAR of any such anticipated disclosure (except to the extent otherwise required by applicable law) and shall not disclose CLEAR Data to the third party without providing CLEAR notice at least forty-eight (48) hours following such request or demand, so that CLEAR may, at its own expense, exercise such rights as it may have under law to prevent or limit such disclosure. Notwithstanding the foregoing, Partner shall exercise commercially reasonable efforts to prevent and limit any such disclosure to only such CLEAR Data as Partner's legal counsel has determined is required to be produced and to otherwise preserve the confidentiality of CLEAR Data, including, without limitation, by cooperating with CLEAR to obtain an appropriate protective order or other reliable assurance that confidential treatment will be accorded to CLEAR Data.

2.2. Partner shall notify CLEAR promptly in writing (and in any event within five (5) days of receipt) of any communication received from an individual relating to his or her request to access, modify or correct Personally Identifiable Information relating to the individual, and Partner shall comply with all reasonable instructions of CLEAR before responding to such communications.

2.3. Upon notice to Partner, Partner shall promptly assist and support CLEAR in the event of an investigation by any regulator, including without limitation a data protection regulator or similar authority, if and to the extent that such investigation relates to CLEAR Data handled by Partner. Such assistance and support shall be at CLEAR's sole expense, except where such investigation was required due to Partner's acts or omissions, in which case such assistance and support shall be at Partner's sole expense.

2.4. Partner shall comply with CLEAR's written instructions to preserve CLEAR Data in connection with any investigations, lawsuits or other disputes in which any CLEAR Entities may be involved.

3. **Partner Information Security Obligations**. Partner shall designate a management level employee as Partner's primary security manager, responsible for managing, coordinating, and periodically reviewing the performance of Partner's information security obligations set forth in this section.

Name of Primary Security Manager

Email:

Phone:

3.1. **Security Management.** Partner maintains an information security program that:

3.1.1. is managed by a senior employee responsible for overseeing and implementing the program;

3.1.2. is appropriate to the nature, size, and complexity of Partner's business operations;

3.1.3. includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of CLEAR Data;

3.1.4. includes a risk assessment framework to identify and assess internal and external risks to the confidentiality, integrity, and availability of electronic, paper, and other records containing CLEAR Data;

3.1.5.is reviewed at least annually or whenever there is a material change in Partner's business practices that may reasonably affect the security or integrity of CLEAR Data.

3.1.6.Partner may not alter its information security program in such a way that will weaken or compromise the confidentiality, integrity, and availability of CLEAR Data.

3.2.**Personnel Security.** Partner will maintain personnel security policies and procedures whereby Partner:

3.2.1. will engage a reputable, commercially recognized background check or investigative entity to conduct background checks in compliance with applicable laws.

3.2.1.1. The background check will include a federal and county criminal conviction check in the counties of residence in the previous seven (7) years for felony and misdemeanor convictions, pending charges, and outstanding warrants, employment in the last seven (7) years, the highest degree of education, and global blacklists.

3.2.2. will maintain a security process to conduct appropriate due diligence prior to engaging subcontractors.

3.2.3. will ensure that all employees have the reasonable skill and experience suitable for employment and placement in a position of trust and trained with respect to Partner's security policies and procedures.

3.3.**Physical Security.** Where Partner processes CLEAR Data outside of CLEAR's environment, Partner shall restrict access to, control, and monitor all physical areas ("Secure Areas") and maintain appropriate physical security controls on a 24-hours-per-day, 7-days-per-week basis ("24/7"). Further, Partner revokes any physical access to Secure Areas promptly after the cessation of the need to access buildings and system(s).

3.3.1. Partner maintains a documented access authorization and logging process. The authorization and logging process will include at minimum:

3.3.1.1. reports detailing all access to Secure Areas, including the identities and dates and times of access;

3.3.1.2. video surveillance equipment to monitor and record activity at all Secure Areas entry and exit points on a 24/7 basis to the extent permitted by applicable laws and regulations.

3.3.2. To the extent Partner is operating a data center, Partner complies with physical security controls in alignment with industry standards such as ISO 27001 and SSAE / SOC, or some other similar standard.

3.4.Logical Security.

3.4.1. **Access Control.** Partner employs access control mechanisms that are intended to:

3.4.1.1. prevent unauthorized access to CLEAR Data;

3.4.1.2. limit access to users who have a business need to know;

3.4.1.3. follow the principle of least privilege, allowing access to only the information and resources that are necessary;

3.4.1.4. detect, log, and report access to the system and network, and attempts to breach security of the system or network;

3.4.1.5. ensure Partner users have an individual account that authenticates that individual's access to CLEAR Data;

3.4.1.6. prevent sharing of accounts;

3.4.1.7. ensure passwords are configured in accordance with industry standards and best practices;

3.4.1.8. maintain a process to review access controls on a minimum annual basis for all Partner systems that transmit, process, or store CLEAR Data;

3.4.1.9. require multi-factor authentication for remote access to all networks storing or transmitting CLEAR Data; and,

3.4.1.10. revokes access to systems and applications that contain or process CLEAR Data promptly after the cessation of the need to access the system(s) or application(s).

3.4.2. **Integrations and Access Control.** If Partner connects to the computing systems or networks of any CLEAR Entities, Partner:

3.4.2.1. will not access, and will not permit any other person or entity to access, the computing systems or networks of the CLEAR Entities without CLEAR's prior written authorization;

3.4.2.2. will ensure connectivity to the computing systems and networks of CLEAR Entities and all attempts at same shall be only through CLEAR's security gateways/firewalls; and,

3.4.2.3. shall inform CLEAR in writing of the identity of any Partner personnel who have access to the systems or networks of CLEAR Entities. Partner may change employees and personnel who have access to the systems or networks of CLEAR Entities, provided Partner gives prior written notice and receives written approval for any such change.

3.4.3. **Network Security.** Partner:

3.4.3.1. deploys firewall technology in the operation of the Partner's sites. Traffic between CLEAR and Partner will be protected and authenticated by industry standard cryptographic technologies.

3.4.3.2. deploys an intrusion detection system to generate, monitor, and respond to alerts which could indicate potential compromise of the network and/or host.

3.4.3.3. implements network segmentation between the corporate enterprise network and hosting environment for CLEAR Data, and applies separation between environments dedicated to development, testing/staging, and production.

3.4.3.4. ensures that all external connections to Partner's networks and applications must be individually identified, documented, and risk-assessed.

3.4.3.5. ensures that remote access is secured, controlled, and monitored and is restricted to only authorized individuals, and user activity must be logged and subject to review.

3.4.3.6. restricts remote access to Partner systems to only authorized individuals and uses encryption standards such as NIST or secure methods and tools (SSL, VPN, SSH) if transmitting or storing CLEAR Data. Remote access authentication must also be performed using multiple factors.

3.4.3.7. protects its email systems by a combination of policy, training, and email-based controls to prevent loss of data in error.

3.4.3.8. subjects all wireless access to its systems to authorization, authentication, and encryption protocols; and only from locations approved by Partner.

3.4.3.9. implements a mobile policy for Mobile Device Management or Bring Your Own Device for remote access by user owned devices, which includes restrictions or prohibited use of accessing CLEAR Data over the network.

3.4.4. **Encryption.** Partner:

3.4.4.1. utilizes industry standard encryption algorithms and key strengths to encrypt all CLEAR Data in electronic form while (a) in transit over all public wired networks (e.g., Internet) and all wireless networks; (b) stored on laptops or storage media; (c) where technically feasible, on portable devices; and, (d) stored on any device that is transported outside of the physical of logical controls of Partner.

3.4.4.2. safeguards the security and confidentiality of all encryption keys associated with encrypted CLEAR Data.

3.4.5. **Malicious Code Protection.** Partner:

3.4.5.1. runs the current version of industry standard anti-virus / anti-malware software with the most recent updates and virus definitions available on workstations and servers.

3.4.5.2. configures such equipment, and has supporting policies, to prohibit users from disabling anti-virus/anti-malware software, altering security configurations, or disabling other protective measures put in place to protect CLEAR Data.

3.4.5.3. configures anti-virus/anti-malware software to run real-time scanning of machines and a full system scan on regularly scheduled intervals.

3.4.5.4. scans incoming and outgoing content for malicious code on all gateways to public networks, including, but not limited to, email and proxy servers.

3.4.6. **Data Loss Prevention.** Partner employs data leakage tools to detect any unauthorized transfers of CLEAR Data within Partner's systems, and any unauthorized external transfers of CLEAR Data.

3.5. **Software Development and Maintenance.** Partner:

3.5.1. carries out development activities in accordance with a documented system development methodology.

3.5.1.1. If Partner is developing code specifically for CLEAR, Partner must share such development methodology upon request.

3.5.1.2. Partner ensures that system build activities (including coding and package customization) are carried out in accordance with industry best practices and performed by individuals with the relevant skills and provided with the appropriate tools.

3.5.2. does not use CLEAR Data within test environments without CLEAR's prior written approval and agreement regarding the controls to be implemented for such use.

3.5.3. applies Security by Design principles throughout the software development lifecycle, at the design and architecture level, by conducting security design review and threat modeling, using the documented methodology.

3.5.4. conducts development activities in specialized development environments that are isolated from live environments and protected against disclosure of information.

3.5.5. employs a documented change management program which includes logically or physically separate environments from production for all development and testing.

3.5.6. develops and implements a patch management plan for its systems.

3.6. **Vulnerability Management and Security Assessments.** Partner runs external network vulnerability scans at least quarterly and after any material change in the network configuration. Partner performs external network vulnerability scans at least quarterly and internal host-based vulnerability scans daily. Vulnerabilities identified and rated as critical risk are remediated or mitigated promptly after discovery. In addition:

3.6.1. For all Internet-facing applications that collect, transmit or display CLEAR Data, Partner conducts an application security assessment review to identify common security vulnerabilities as identified by industry-recognized organizations (e.g., OWASP Top 10 Vulnerabilities; CWE/SANS Top 25 vulnerabilities) annually or for all major releases, whichever occurs first. The scope of the security assessment will primarily focus on application security, including, but not limited to, a penetration test of the application, as well as a code review.

3.6.2. For all mobile applications that collect, transmit or display CLEAR Data, Partner conducts an application security assessment review to identify and remediate industry-recognized vulnerabilities specific to mobile applications.

3.6.3. Partner utilizes a qualified third party to conduct the application security assessments. Partner may conduct the security assessment review directly, following industry standard best practices.

3.7. **Storage, Handling and Disposal.** Partner:

3.7.1. physically or logically separates and segregates CLEAR Data from its other customers' data;

3.7.2. utilizes industry standard encryption algorithms and key strengths to encrypt all CLEAR Data in electronic form while at rest in Partner's systems;

3.7.3. stores all backup and archival media containing CLEAR Data in secure, environmentally-controlled storage areas;

3.7.4. disposes of CLEAR Data in a method that renders the data unrecoverable, to the extent reasonably possible, in accordance with industry practices for wiping of electronic media (e.g. NIST SP 800-88);

3.7.5. destroys any equipment containing CLEAR Data that is damaged or non-functional.

3.8. **Logging and Monitoring.** Partner shall:

3.8.1. monitor and maintain logs of all key events such as those that

3.8.1.1. have the potential to impact the confidentiality, integrity and availability of CLEAR Data; and,

3.8.1.2. may assist in identifying or investigating material incidents and/or breaches of access rights occurring in relation to CLEAR's Data.

3.8.2. retain logs for a period of at least twelve (12) months or as reasonably requested by CLEAR.

3.8.3. protect logs against unauthorized change (including, amending or deleting a log).

3.8.4. provide logs to CLEAR upon written request.

3.9. **Business Continuity and Disaster Recovery**. Partner develops, implements, and maintains a business continuity management program that ensures the continuity of services under this agreement in the event of an outage, force majeure event, or other event that may impact ongoing operations. To that end, Partner completes a minimum level of business impact analysis, crisis management, business continuity, and disaster recovery planning:

3.9.1. Business Impact Analysis includes, but is not limited to, a systematic review of business functions and their associated processes that identifies dependencies, evaluates potential impact from disruptions; defines recovery time objectives, and improves process understanding improvement, performed annually.

3.9.2. Crisis Management Plan includes, but is not limited to, elements such as event management, plan and team activation, event and communication process documentation, exercised at least annually.

3.9.3. Business Continuity Plan includes, but is not limited to, elements such location work-arounds, application work-arounds, vendor work-arounds, and staffing work-arounds, exercised at minimum annually.

3.9.4. Disaster Recovery Plan includes, but is not limited to, infrastructure, technology, and system(s) details, recovery activities, and identifies the people/teams required for such recovery, exercised at least annually.

4. Audit Rights

4.1. Partner shall establish and maintain complete and accurate books, notices, and accounting and administrative records necessary to document the proper handling of CLEAR Data under this Agreement, including without limitation accounts of all transactions involving CLEAR Data, and shall retain such records pursuant to applicable law. Upon CLEAR's written request, not more than one time in any twelve (12) month period, to confirm Provider's compliance with this Agreement, as well as any applicable laws, regulations, and industry standards, Provider grants CLEAR or, upon CLEAR's election, a third party on CLEAR's behalf, permission to perform an assessment, audit, examination, or review of all controls in Provider's physical and/or technical environment in relation to all CLEAR Data being handled and/or services being provided to CLEAR pursuant to this Agreement. Provider shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that processes, stores, or transports CLEAR Data pursuant to this Agreement. Any external costs incurred by CLEAR for a third party for such assessment shall be fully paid by CLEAR.

4.2. In addition, at least once annually upon CLEAR's written request, Provider shall:

4.2.1. provide CLEAR with the results of any audit by or on behalf of Provider performed that assesses the effectiveness of Provider's information security program as relevant to the security and confidentiality of CLEAR Data shared during the course of this Agreement, including without limitation Service Organization Controls ("SOC") reports, ISO 27001/2 certifications, or industry-specific certifications or attestations;

4.2.2. complete CLEAR's information security questionnaire, which shall include responses to any questions regarding Partner's controls for any part of the Services performed by a third party by or on behalf of Partner; and

4.2.3. make available an appropriately senior representative of Partner's information security team to meet with CLEAR's information security team to discuss any questions or concerns CLEAR may have regarding Partner's information security program.

4.3. Partner agrees to make available to CLEAR, upon request, the summary report of the most recent penetration test.

5. Security Incidents and Breaches.

5.1. Partner shall have an incident response policy and procedures that outline roles and responsibilities for promptly responding and investigating Security Incidents and Breaches, and proper communication and reporting. Partner shall notify CLEAR in writing, at trust@clearme.com, or by phone at (512) 967-0949, of known Security Incidents or Breaches within forty-eight (48) hours of discovery. The incident report must provide the following incident details: (i) Partner's assessment of the impact and immediate risk arising from such Security Incident or Breach; and (ii) any corrective measures taken or to be taken by Partner, and next steps. Partner shall provide status updates to CLEAR regarding the investigation and resolution of the Security Incident or Breach and prevention of future Security Incidents or Breaches.

5.2. In the event of a Breach caused by Partner's material breach of its obligations under this Exhibit F, Partner further agrees (i) to provide reasonable assistance and cooperation requested by CLEAR and/or CLEAR's designated representatives, in the furtherance of any correction, remediation, or investigation of any such Breach and/or the mitigation of any damage, and (ii) to reimburse CLEAR for the reasonable, documented out-pocket expenses actually incurred by CLEAR and/or CLEAR's designated representatives to send notifications required by applicable law to individuals impacted by the Breach, and/or the provision of any credit reporting service that CLEAR is legally required to provide to such individuals. Unless required by law, Partner shall not notify any individual or any third party other than law enforcement of any potential Breach involving CLEAR Data without first consulting with, and obtaining the permission of, CLEAR. In addition, within 30 days of identifying or being informed of a Breach, Partner shall develop and execute a plan that reduces the likelihood of a recurrence of such Breach.

5.3. Partner agrees that CLEAR may at its discretion immediately terminate the Agreement without penalty if a Breach occurs and such Breach was caused solely by Spreedly's material breach of its obligations under this Exhibit F. Partner agrees that CLEAR, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of the provisions of this Appendix without the necessity of posting any bond or other security.

6. Return or Destruction of Data. Except to perform Termination Support if and as outlined in the Agreement, upon termination or expiration of the Agreement for any reason or upon CLEAR's request, Partner shall immediately cease handling CLEAR Data or portion of CLEAR Data specified by CLEAR, and shall:

6.1.1. return in a manner and format reasonably requested by CLEAR, or, if specifically directed by CLEAR, shall destroy in a manner required by Section ___, any or all such CLEAR Data in Partner's possession, power or control, in whatever form, including without limitation all copies, fragments, excerpts, and any materials containing CLEAR Data, whether or not such CLEAR Data has been intermingled with Partner's own information or materials.

6.1.2. permanently remove, upon CLEAR's instruction to destroy or return CLEAR Data, all copies of CLEAR Data from Partner's, its agents', subcontractors' and third parties' systems, records, archives and backups;

6.1.3. cease all subsequent use of such CLEAR Data by Partner, its agents, subcontractors and third parties; and,

6.1.4. certify to CLEAR, upon request, by an officer of Partner that all forms of the requested CLEAR Data have been destroyed by Partner.

7. Additional Obligations

7.1. **PCI Compliance.** If Partner has access to Cardholder Data, Partner:

7.1.1. shall ensure that its information security program addresses the requirements of the PCI Standards;

7.1.2. shall maintain a complete audit trail of all transactions and activities associated with Cardholder Data;

7.1.3. shall not store card validation codes/values, complete magnetic stripe data or PINs and PIN blocks;.

7.1.4. represents and warrants that it shall maintain certification of its compliance with the PCI Standards and that it shall undergo independent, third-party quarterly system vulnerability scans;.

7.1.5. shall provide, at the request of CLEAR, current certification of compliance with the PCI Standards, by an authority recognized by the payment card industry for that purpose. If during the term of the Agreement, Partner undergoes, or has reason to believe that it will undergo, an adverse change in its certification or compliance status with the PCI Standards and/or other material payment card industry standards, it will promptly notify CLEAR of such circumstances;. and

7.1.6. represents and warrants that it shall not take any actions that will compromise CLEAR's ability to comply with the PCI Standards.

7.2. [reserved]

7.3. Data Protection Requirements. As needed to comply with Data Protection Requirements, or to the extent required by any changes in such Data Protection Requirements or the enactment of new applicable laws, the Parties agree to work cooperatively and in good faith to amend this Appendix in a mutually agreeable and timely manner in an effort to comply with any such Data Protection Requirements. If the Parties cannot so agree, or if Partner cannot comply with the new or additional requirements, CLEAR may terminate this Agreement upon written notice to Partner.

7.4. Third Party Beneficiaries. The parties agree that, to the extent such entity is not a party to the Agreement, each of the CLEAR Entities are intended third-party beneficiaries of the data protection and security provisions of this Agreement and such provisions are intended to inure to the benefit of the CLEAR Entities. Without limiting the foregoing, the CLEAR Entities will be entitled to enforce all data protection and security provisions of this Agreement as if each was a signatory to this Agreement.

7.5. Interconnection Security Agreement. If Partner is performing services for CLEAR in furtherance of a CLEAR government contract, such as TSA PreCheck™, then Partner shall work with CLEAR to document and execute an Interconnection Security Agreement ("**ISA**") that documents the connections between CLEAR and Partner's respective systems.

APPENDIX: CLEAR Data Privacy & Security