1. Introduction

This Information Security and Data Protection Statement ("**Statement**") summarizes FIS' information security policies, procedures and standards ("**FIS' Information Security Practices**") and forms an integral part of the Agreement which incorporates it by reference. The Statement sets out obligations of FIS with respect to information security and data protection in relation to the Agreement. To the extent of any conflict or inconsistency between the provisions of this Statement and any provision of the Agreement, the provisions of this Statement shall prevail and take precedence over such conflicting or inconsistent provisions.

FIS' Information Security Practices are compliant with Industry Standards Organization ISO 27001:2013 and are designed to protect the security, confidentiality and integrity of Client's Confidential Information processed or stored on FIS' systems. FIS' Information Security Practices are made available to Client under the Vendor Management Resource Center on the Client Portal or upon request. FIS will provide access instructions for the Client Portal to Client upon request.

2. Organizational Practices

FIS' Information Security Department is responsible for developing and implementing FIS' Information Security Practices. FIS maintains safeguards designed to prevent the compromise or unauthorized disclosure of Client's Confidential Information and Personal Data, including loss, corruption, destruction or mis-transmission of Client's Confidential Information and Personal Data.

FIS maintains FIS' Information Security Practices designed to comply with (1) all applicable laws relating to the privacy, confidentiality and security of Client's Confidential Information or Personal Data to the extent applicable to FIS as a third-party service provider; (2) the requirements set forth in this Statement; and (3) all applicable provisions of FIS' related policies including but not limited to FIS' Information Security Policy. Client may review additional information concerning FIS' Information Security Practices in the Client Portal.

FIS' internal and external auditors regularly review FIS' Information Security Practices. FIS performs security assessment reviews to determine whether identified vulnerabilities, in particular as related to web and network environments have been remediated. Security assessment reviews include: diagnostic reviews of devices, internal and external penetration testing, assessments of applications that can access sensitive data and assessments of FIS' Information Security Practices.

FIS updates FIS' Information Security Practices from time to time in response to evolving information security threats. Such updates shall provide at least an equivalent or increased level of security compared to what is described in this Statement, and FIS will provide Client with a summary of any updates upon request.

FIS will implement commercially reasonable administrative, technical, and physical safeguards designed to: (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security or integrity of Personal Data; and (iii) protect against unauthorized access to or use of Personal Data. FIS will review and test such safeguards on no less than an annual basis.

3. Security Controls

3.1. Access Control to Facilities

3.1.1. FIS Facility Restrictions

Access to FIS facilities is restricted using controls such as camera coverage and badge access. Badges and keys are only distributed in accordance with documented organizational procedures. Visitors are screened prior to admittance, are provided a visitor badge, and in sensitive areas require an escort in accordance with FIS'

Information Security Policy. Alarm systems are in place to notify appropriate individuals of potential threats. FIS regularly tests its emergency procedure protocols.

Physical security measures implemented at FIS offices are designed to protect employees, visitors, and assets. Physical security consists of a combination of physical barriers, electronic access and monitoring systems, Security Officers and procedures for controlling access to buildings and sensitive or restricted areas. Security is staffed 24 hours a day, seven days a week, at FIS data center facilities. Secure shred bins are provided for the proper disposal of hard copy documentation and other small media thorough-out the campus.

An access control system utilizing individual badge identification, doors protected by an electronic badge reader or locked with limited access to the physical key, closed circuit camera monitoring, and onsite physical security guards stationed in strategic locations are utilized to provide facility physical security and protection. Physical access to FIS buildings, office spaces and certain secured areas within the facility are controlled by an electronic access control system. The system provides for real-time monitoring of all electronic badge accesses across the monitored facility, requires physical security officer acknowledgement of system identified error codes or issues, and is tied to centralized servers communicating the exact date and time stamp for each entry (utilizing network time protocol). Automated database backups are performed daily and are replicated on the secondary server.

For data centers, FIS maintains automatic early-warning sensors (e.g., fire, water, temperature and humidity), independent air conditioning systems and fire suppression systems. Mission-critical hardware is protected by an emergency power supply system with batteries and backup generators. Hazardous or combustible materials are kept at a safe distance from information assets.

3.2. Logical Controls and Security

FIS has a dedicated group that is responsible for overseeing operational security, network security, host and server security, applications and system development, patch and vulnerability management, authentication and remote passwords, encryption, passwords and monitoring systems (collectively, "**Logical Controls and Security**"). FIS has documented protocols for all Logical Controls and Security including the following:

3.2.1. Operational Security

3.2.1.1. Employees

FIS performs (at the time of hire) a background check, as described herein, for each FIS employee that is performing any services under the Agreement. Currently, the background check in the United States of America consists of, at a minimum, verification of the highest level of education completed, verification of employment (as allowed by applicable law), social security number trace and validation, and a check of U.S. Government Specially Designated National (OFAC) and other export denial lists. Background checks outside of the United States consist of similar reviews to the extent allowed by local laws of each country. In addition, to the extent permitted by law, the background check may include a 9-panel drug test and criminal record search. FIS complies with all applicable laws related to the background check, including required notices and applicable consents. FIS assigns all employees mandatory security awareness training on an annual basis. FIS requires all employees with access to sensitive information to follow a clean desk and clear screen standard such that the information is controlled and/or protected at all times. FIS will not assign any employee to perform services for Client if his/her background check findings do not meet the standards established by FIS. FIS has formal disciplinary procedures in place to address policy violations. A terminated employee's access to FIS facilities and Client Confidential Information and Personal Data is suspended upon termination.

3.2.1.2. Network Security

FIS employs a defensive model when building networks (including firewalls) in a multi-tiered approach and uses separate layers of presentation, business logic and data when considered necessary. Connection between networks is limited to those ports and services required for FIS to support, secure, monitor and perform the services under the Agreement.

FIS uses Network Intrusion Detection and/or Prevention Systems to monitor threats to the FIS environment. FIS monitors these threats 24x7x365/366.

FIS may from time to time in its reasonable discretion block attempted access to FIS services from technology of individuals, entities, or governments FIS reasonably believes may pose a threat to FIS services, systems or clients (such technology, "Suspicious Technology"). Due to the unknown timing of cyber threats, FIS may not be able to provide Client prior notice of blocking the Suspicious Technology, and it may impact the availability of FIS services. If Client is adversely affected, FIS will make reasonable efforts to resolve any impacts to Client as long as FIS can reasonably prevent any ongoing threats to FIS services, systems and clients.

3.2.1.3. Host and Server Security

FIS hardens its operating systems in accordance with industry security standards and procedures. For example, FIS ensures all default passwords are changed, unneeded functionality is disabled or removed, FIS adheres to the concept of "least-privileged" access, file permissions do not include world writeable ability, administrative or "root" access is limited to the console only, and only those network ports that are necessary to provide the services are opened. For database installations, FIS uses security at a table and row level, based upon the placement of a system and its role in the environment. FIS requires that anti-virus and anti-spyware software is enabled on its operating systems when they are available and supported by commercially available anti-virus solutions.

Access to FIS' operating systems is limited to those individuals required to support the system. FIS has implemented appropriate change management processes. Servers and workstations are enabled with auto-locking (password-protected) screensavers that activate after a period of inactivity. Installation of personal software is not allowed.

3.2.1.4. Applications and Systems Development

FIS uses System Development Lifecycle (SDLC) and system change procedures, which include requirements for code review and secure coding practices. Development and testing environments are segregated and firewalled from FIS' production environment. Version control software is utilized for the management and deployment of code through appropriate support groups.

3.2.1.5. Electronic Mail

FIS scans incoming emails and attachments prior to allowing them into the FIS environment. FIS also uses industry leading software to control what files are allowed or blocked as attachments to protect against malicious executable files being delivered and/or opened.

3.2.1.6. Patch and Vulnerability Management

FIS analyzes, tests, reviews and subsequently installs software updates on FIS systems and security patches as soon as reasonably possible after release. Critical security updates are promptly installed after testing is completed. FIS performs vulnerability scans, including scans on application and internal/external network infrastructure. Ethical hacking/penetration tests are performed by FIS on a periodic basis. FIS reviews, prioritizes and remediates known vulnerabilities based on identified risk factors.

a. Penetration Tests. FIS will conduct a penetration test and security evaluation, which will include tests to detect vulnerabilities listed in the SANS Top-20 or OWASP or its successor current at the time of the penetration test and security evaluation. Upon written request from Client, FIS will provide a high level summary of the penetration test and security evaluation to the Client. Personnel performing the penetration test shall be independent of the controls being tested and shall not report to the individuals who make the funding decisions for any noted vulnerabilities that require remediation.

b. Dynamic Application Scanning. FIS will conduct dynamic application scanning, which will include detecting vulnerabilities listed in the SANS Top 20 or OWASP or its successor current at the time of the dynamic application scan. FIS will provide a summary of the dynamic application scan to Client upon request. The scan shall be performed using an industry standard tool and shall occur no less than twice a year.

c. Static Application Security Testing. FIS will conduct static application security scanning, which will include detecting vulnerabilities listed in the SANS Top 20 or OWASP or its successor current at the time of the static application security scan. FIS will provide a summary of the static application security scan to Client upon request. The scan shall be performed using an industry standard tool.

d. Vulnerability Assessment. FIS maintains a vulnerability management program based on industry standard practices that frequently assesses all FIS computing devices and systems (including without limitation all such devices and systems used by FIS to provide any services under the Agreement) and all software provided by FIS under the Agreement to verify that the applicable security controls are sound, and that mitigates or eliminates vulnerabilities. As part of such program, (i) FIS uses an industry standard tool to perform all vulnerability scans or engage, at its expense, an unrelated security firm to perform the assessment; and (ii) routine network, database and software scans are scheduled on a periodic basis;

e. Vulnerability Assessment Findings. FIS shall provide to Client annually (or at such other more frequent intervals as requested by Client and mutually agreed upon by both parties) a summary which describes the results of the assessment. FIS follows a remediation timeframe policy based upon the CVSS scoring.

3.2.1.7. Authentication and Remote Access

3.2.1.7.1. Authentication.

The level of authentication required to access a particular FIS environment is based on the type of data protected within that environment. FIS permits only authorized persons to access any FIS systems in accordance with FIS' Information Security Policy. User authentications (i.e. user name and password) are bound to the respective user and may not be shared. The use of an emergency user account must be documented and logged. Remote access to FIS' systems requires the use of multi-factor authentication.

3.2.1.7.2. Passwords

FIS requires the use of complex passwords. User accounts are locked after a defined number of abortive or unsuccessful logon attempts. If a password is possibly disclosed, it shall be changed without undue delay. Using a documented procedure, FIS employs processes to minimize the risk of unauthorized or no longer needed user accounts in the systems and audits user accounts to determine that access that is no longer required is revoked.

3.2.1.7.3. Data Classification, Retention, and Controls

FIS' Information Security Policy addresses the confidentiality, integrity, security, availability, retention and disposal of Client's Confidential Information and any of Client's Personal Data. All FIS employees and vendors with access to sensitive information will comply with secure deletion standards in alignment with the latest NIST *Guidelines for Media Sanitization*. FIS will store Clients' Personal Data only for as long as necessary to achieve the purposes for which it was collected and in accordance with applicable laws.

3.2.1.7.4. Encryption

FIS has developed encryption key management policies and procedures in accordance with industry standards. FIS encrypts data at rest when and where FIS has implemented the ability to do so. Data is encrypted based on data classification policies and standards. FIS will use encryption key lengths that meet current NIST FIPS 140-

2 standards. FIS policies require that FIS shall not transmit any unencrypted Client Confidential Information and Personal Data over the internet. Specific algorithm and other minimum key lengths are specified within FIS' policy.

3.2.1.7.5. Monitoring Systems and Procedures / Logging

FIS uses a real-time event management system to monitor its networks (including wireless networks) and servers via system logs, intrusion detection/prevention systems, data loss prevention, file integrity monitoring and firewall logs on a 24-hour per day basis. FIS will perform reasonable logging, monitoring, or record keeping of user activity where legally permissible and in accordance with FIS' applicable information retention standards.

3.2.1.7.6. Notification

If FIS becomes aware of any breach of security leading to the accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to the Personal Data FIS processes for Client, FIS shall without undue delay notify Client thereof.

4. Business Continuity and Disaster Recovery / Availability

FIS has put in place disaster recovery plan(s), site recovery plan(s) and business continuity plan(s) designed to minimize the risks associated with a disaster affecting FIS' ability to provide the services under the Agreement. FIS' business continuity plans are based on a business impact analysis for recovery times and recovery points. FIS' business continuity management system meets the FFIEC business continuity guidelines and the PS-Prep / ISO 22301 business continuity international standards. FIS' recovery time objective (RTO) under such disaster recovery plan(s) is as set out in the Agreement or, if the Agreement is silent, as set forth in the business continuity management summary document made available to Client via the Client Portal or upon request. FIS will maintain adequate backup procedures in order to recover Client's Data to the point of the last available good backup, with a recovery point objective (RPO) as set out in the Agreement or, if the Agreement is silent, as set forth in the business continuity management summary document made available to Client via the Client Portal or upon request. FIS will test its recovery plans at least annually. FIS will provide a summary of the business continuity management and disaster recovery program in the FIS Client Portal or upon request. Disaster recovery exercise and site business continuity exercise results are provided in the form of an exercise bulletin, excluding any proprietary information, NPI, or Personal Data, via the Client Portal or upon request. Client is responsible for adopting a disaster recovery plan relating to disasters affecting Client's facilities and for securing business interruption insurance or other insurance necessary for Client's protection.

5. Vendor Management

FIS conducts a risk assessment for all third-party suppliers engaged in the provision of the services under the Agreement to validate compliance with FIS' standards. FIS will only allow such third-party suppliers to access or otherwise process Client's Confidential Data and Personal Data, where this is permissible under the respective agreement and applicable laws.

FIS maintains a list of all third-party suppliers with access to Client Personal Data on the Client Portal at the following: https://my.fisglobal.com (also available upon request).

6. Audit

6.1. Outsourcing and TSP Diligence Generally.

FIS will cooperate with Client to meet its responsibilities to perform due diligence and assess FIS as its third-party technology service provider. FIS will regularly make available audit reports and materials that address Client's vendor management and due diligence requirements. Specific information regarding the available materials is available under the Vendor Management Resource Center on the Client Portal or upon request.

6.2. Vendor Diligence and Audit Materials.

Through its Client Portal, Client will have continuous electronic access to audit reports, attestations, and other detailed information regarding FIS' internal systems testing and procedures, and FIS' information security and data protection controls. These audit materials and attestation evidence FIS' compliance with industry and regulatory standards and include recent independent audits (such as SSAE 18's), third party attestations and certifications (such as AT101's, ISO certifications, and PCI AOC's), and detailed information and testing results regarding physical, technical and administrative controls utilized by the service business lines within FIS and the security of Client's Confidential Information.

6.3. Information Security and Risk Management In-Depth Conferences.

Client may attend any or all of the FIS In-Depth Conferences, which are held each year and provide in-depth in-person discussions with FIS' senior executive team regarding FIS' information security and risk management processes and system testing results. The In-Depth Conferences provide Client with comprehensive vendor diligence information, including (i) a thorough, interactive review of FIS enterprise-wide security and system controls, and (ii) specific assessments of industry standards and best practices for financial technology information security and risk management.

6.4. SSAE 18 Audit

FIS shall cause an independent public accounting firm to perform the audits (generally SSAE 18) with respect to the services being provided under the Agreement which FIS has agreed to be in scope for such audits. FIS shall make available to Client a copy of the resulting independent audit report(s) relevant to the Agreement. FIS shall promptly address and resolve any mutually agreed upon deficiencies identified in such audit report(s).

7. Supplemental Contract Provisions

With respect to certain Personal Data being processed by FIS on behalf of Client under the Agreement, FIS will provide and agree to supplemental standard contract provisions relating to the processing and security of such Personal Data as specifically required by laws applicable to the processing of such Personal Data. By way of example, the Business Associate Addendum as required by the United States Health Insurance Portability and Accountability Act of 1996 ("**HIPAA**") and its implementing regulations in 45 CFR Parts 160 and 164 as amended from time to time, including by the Health Information Technology for Economic and Clinical Health Act ("**HITECH**") and/or the Data Protection Addendum as required by the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) or similar.

8. Defined Terms

As used in this Statement, the following terms shall have the following meanings:

"**Client Data**" is data stored in, or processed by, the Solution; provided that aggregated data that is: (i) not Personal Data; and (ii) not identifiable to Client, shall not be deemed Client Data nor Client's Confidential Information.

"**Client Portal**" is a self-service portal that offers a comprehensive and streamlined set of resources to effectively manage your relationship with FIS, including specific information and documentation about FIS and the Solution including FIS' Information Security Practices. The link to the Client Portal is as follows:
https://my.fisglobal.com/vendor-management

"**Confidential Information**" is all business or technical information disclosed by Client to FIS or by FIS to Client in connection with the Agreement. Confidential Information includes without limitation: (i) Client Data, information that is protected by applicable banking secrecy laws and the details of Client's computer operations; (ii) details of the FIS Solution; and (iii) the terms of this Statement and the Agreement, but not the fact that the Agreement has been signed, the identity of the parties hereto or the identity of the Solution. Confidential Information does not include information that: (aa) prior to the receipt thereof under the Agreement, had been developed independently by Client or FIS, or was lawfully known to Client or FIS, or had been lawfully received by Client or

FIS from other sources, provided such other source did not receive it due to a breach of an agreement; or (bb) is publicly known at or after the time either party first learns of such information, or generic information or knowledge which either party would have learned in the course of its work in the trade, business or industry; or (cc) subsequent to the receipt thereof under the Agreement: (1) is published by FIS or Client or is disclosed generally by Client or FIS to others without a restriction on its use and disclosure; or (2) has been lawfully obtained by Client or FIS or from other sources and which Client or FIS reasonably believes lawfully came to possess it.

"**Personal Data**" is any information relating to an identified or identifiable natural person.

"**Solution**" is the software and/or services being provided by FIS to Client under the terms of the Agreement.