This Model Data Access Agreement ("Agreement") is intended to serve as a resource to encourage the development of API relationships between financial institutions ("FIs") and third-party data providers ("Data Providers"). The terms set forth in this Agreement represent options for how FIs and Data Providers may wish to approach such relationships and may change based on the specific details of such relationships. Furthermore, the information contained in the Agreement should not to be misconstrued as legal advice or a recommendation regarding any of the legal issues or problems that may arise in such relationships. Nothing in this Agreement should be interpreted in any way as constituting the giving of legal advice, or the practice of law and users should consult their own attorney regarding their individual questions or needs.

TEMPLATE FOR U.S. ACCOUNTS]

DATA ACCESS AGREEMENT

The Data Access Agreement (the "**Agreement**") is entered into as of *[Fill in Effective Date]* (the "**Effective Date**") by and between *[Fill in Name of Financial Services Institution and Entity Type]* ("**FSE**") and *[Fill in Name of Data Access Platform Provider and Entity Type]* ("**Data Recipient**"). Each of FSE and Data Recipient is referred to as a "**Party**" and collectively as the "**Parties**." The Agreement consists of and incorporates in full the following documents, each as may be amended pursuant to the terms of the Agreement:

(1) this signature page,
(2) the General Terms attached hereto and
(3) the following Exhibits to the General Terms (the "**Exhibits**")

Exhibit #	Name
1.	Data Access Method; Approved Data Elements
2.	FSE Security Requirements
3.	Insurance
4.	List of Data Recipient Services as of Effective Date
5.	Reports
6.	Implementation Plan

IN WITNESS WHEREOF, and in consideration of the promises contained in the Agreement and other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, each Party agrees to the terms and conditions of the Agreement and has caused the Agreement to be executed by its duly authorized representatives as set forth below.

[FSE]	*[DATA RECIPIENT]*
By:	By:
Printed Name:	Printed Name:
Title:	Title:
Date:	Date:
Contacts for Notices:	Contacts for Notices:

DATA ACCESS AGREEMENT
GENERAL TERMS

These General Terms (the "**General Terms**") are an attachment to, are incorporated into and made part of the Data Access Agreement (also referred to as the Agreement), and apply to the data access and related activities described in the Agreement.

ARTICLE 1 PURPOSE AND STRUCTURE

1.1 Purpose.

(a) FSE is a financial services institution that holds, manages and maintains Accounts for Customers, and processes and generates Account Information relating to such Accounts, itself and through other FSE Entities.

(b) Customers may wish to access their data through a data access company (either directly or indirectly through a Data Recipient Client) that, as part of its service offering collects and accesses data from various sources so that such Customers are able to access, share (as permitted under the Agreement), view, and/or analyze their financial data, through a unified platform.

(c) Data Recipient is a data access company that has customers, or that has relationships with Data Recipient Clients that have customers, that also are customers of one or more FSE Entities, and who wish to have Account Information held by or through the FSE Entities accessible in connection with the Data Recipient Services.

(d) The Parties wish to enter into an arrangement hereunder whereby, upon and subject to the request and informed and explicit consent of a Designated Customer (as defined below), Data Recipient will be provided access through the Data Access Method to Account Information of such Designated Customer, in each instance solely in accordance with, subject to the terms of and for the purposes set forth in the Agreement. Under such arrangement, no Data Recipient Entity is or will be considered a vendor or supplier of FSE, and FSE is not receiving services from any Data Recipient Entity directly or on behalf of any Designated Customer. FSE is acting solely as an intermediary on behalf of Designated Customers to allow access to Account Information using the Data Access Method.

1.2 Interpretation. Unless the context requires otherwise, "including" (and its derivative forms) means "including but not limited to"; use of the singular includes the plural and vice versa; the word "or" will not be exclusive; and when calculating the period of time before which, within which or following which any act is to be done or step taken pursuant to the Agreement, the date that is the reference date in calculating such period will be excluded. Section headings are included for convenience or reference only and should not be used to construe or interpret the Agreement.

ARTICLE 2 DEFINITIONS

For the purposes of the Agreement, in addition to terms otherwise defined in the Agreement, the following terms have the meanings set forth below:

Access Token means access credentials authorized by a Designated Customer that permit Data Recipient to access Applicable Account Information on behalf of such Designated Customer.

Account means a United States depository, payment card, credit, mortgage, loan, brokerage, investment, or other United States financial account held, managed or maintained by an FSE Entity for a Customer.

Account Information means information relating to an Account of a Customer that is made available by an FSE Entity to a Customer. Account Information does not include Customer Account Credentials.

Affiliate means, as to any Person, any other Person that, directly or indirectly, Controls, is Controlled by or is under common Control with such Person.

Applicable Account Information means Account Information that is covered by the data elements set forth in **Exhibit 1** and made available by FSE to Data Recipient through the Data Access Method, subject to and in accordance with the request and consent of a Designated Customer and the terms of the Agreement.

Business Day means Monday through Friday, excluding days on which FSE is not open for business in the United States of America.

Computer Virus means (a) any software, code, program, or sub-program whose knowing or intended purpose is to damage or interfere with the operation of the computer system containing the code, program or sub-program, or to halt, disable or interfere with the operation of the software, code, program, or sub-program itself; (b) any device, method, or token that permits any Person to circumvent the normal security of the software or the system containing the code; or (c) any other parasitic program or programming code written intentionally to enter a computer program or network without the user's permission or knowledge, that damages or is intended to damage, modify, or disrupt the operation of software or hardware, including trojan horses, worms, logic bombs, time bombs, back doors, trap doors, spyware, malware or other code or components within software that have no documented purpose in the operation of the software.

Control means, with respect to any Person, the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such Person, whether through the ownership of voting securities (or other ownership interest), by contract or otherwise.

Customer means a Person with a consumer or business relationship with an FSE Entity.

Customer Account Credentials means the user name, online ID (or other user ID), passcode, password, challenge question and answer pairs, or other identity confirmation information (provided to or selected by a Designated Customer) that are necessary for Designated Customers to directly access their Account(s) and Account Information at or through the FSE Site(s).

Cyber Risk means risk of loss or vulnerability that could compromise (a) the systems or data of the FSE Entity (including the Data Access Method), (b) current, potential and former Customers (including Account Information and Customer Account Credentials relating to such Customers), (c) Personal Information) and/or (d) the systems, website or services of any Data Recipient Entity made available to or that host, store or transmit data relating to Designated Customers.

Data Access Method means the data distribution channel made available by FSE or an FSE Affiliate to provide Applicable Account Information to or on behalf of Data Recipient pursuant to the Agreement. The Data Access Method as of the Applicable Cutover Date is described in **Exhibit 1**, and may be changed by FSE upon notice to Data Recipient (which will be at least 60 days' notice unless FSE determines that a shorter period is appropriate to prevent a Major Risk or due to another legitimate business reason). Upon a change to the Data Access Method, Data Recipient will use the then-current Data Access Method and update its processes and integrations to adapt to the then-current Data Access Method.

Data Recipient Access Authentication means the authentication means assigned by Data Recipient to each of the Personnel of Data Recipient or a Data Recipient Subcontractor who will have access to the Data Access Method in order to access the Data Access Method.

Data Recipient Client means a third party developer or other service provider that obtains or has access to Account Information to display or use the Account Information in a Data Recipient Service.

Data Recipient Entities means Data Recipient, Data Recipient Clients and Data Recipient Subcontractors, and their Personnel.

Data Recipient Personnel means Personnel of any or all of the Data Recipient Entities.

Data Recipient Security Controls means those controls implemented by Data Recipient as part of its Information Security Program that address each of the FSE Security Requirements, and that Data Recipient requires each Data Recipient Client and Data Recipient Subcontractor to implement as applicable and in accordance with the Agreement.

Data Recipient Service means a customer-facing financial product or service provided by Data Recipient or any Data Recipient Client to a Designated Customer via a separate agreement with the Designated Customer and which, at the direction and with the informed and explicit consent of the Designated Customer, allows collection, sharing (as permitted under the Agreement) and display of the Account Information of such Designated Customer.

Data Recipient Subcontractor means a subcontractor or other third party service provider with a contractual relationship with Data Recipient to provide services to Data Recipient and that has access to or use of the Data Access Method or Account Information.

Data Recipient Terms means the privacy (including the Privacy Notice), disclosure, use and other terms that Data Recipient and/or a Data Recipient Client has with the Designated Customer regarding use of Account Information in a Data Recipient Service.

Delete and Destroy means delete and destroy all data (including metadata) and information by using any and all means to ensure that the data and information deletion is permanent and cannot be retrieved, in whole or in part, by any data or information retrieval tools or similar means. Any reference to Delete and Destroy will not require a Data Recipient Entity to delete or destroy data or information stored as required by Law or on secure back-up media not connected to a public network; provided, that, unless otherwise required by Law, any data or information stored on such media must be deleted and destroyed prior to the earlier to occur of [●] years from [●] or the date required in Data Recipient's record retention policy.

Designated Customer means a customer of an FSE Entity in the United States who also is a customer of Data Recipient and/or a Data Recipient Client and who has requested and consented to have his or her Account Information accessed through the Data Access Method in order to receive a Data Recipient Service.

*[**FSE Content** means certain materials provided by FSE to Data Recipient for Data Recipient's use hereunder, which include trademarks, service marks, images, illustrations, graphics, multimedia files and/or text generated in a form or media.]*[1]

FSE Entities means FSE and those Affiliates of FSE that FSE has designated as in scope for the purposes of the Agreement.

FSE Materials means (a) all materials that FSE provides to Data Recipient for Data Recipient's use for the sole purpose of using or accessing the Account Information, (b) and any and all data and information (i) relating to the FSE Entities or the products and business operations of the FSE or any personnel or providers of the FSE Entities, (ii) that is or includes Customer Account Credentials or (iii) relating to the performance or operations of the systems of any FSE Entities, including the Data Access Method or [(iv) FSE Content] and (c) any deliverables, interfaces, integrations, reports, data outputs, customizations, configurations and other materials created or developed in connection with or pursuant to the Agreement, whether by a Party jointly or alone.

FSE Security Requirements mean the privacy and security requirements as described in **Exhibit 2**, as may be updated in accordance with the Agreement.

[1] If FSE will require any marking / disclaimers in the Account Information, add applicable provisions to the Agreement.

FSE Site means a customer-facing access channel, including accessible through the internet or a mobile application, maintained by or on behalf of an FSE Entity at which Designated Customers may, upon successfully inputting their Customer Account Credentials, access their Accounts and perform certain transactions with respect to their Accounts.

FSE Systems means software, equipment and technology owned, licensed or provided by the FSE Entities.

Government Authority means any federal, state, municipal, local, territorial or other government department, regulatory authority, or judicial or administrative body, domestic, international or foreign that governs the Agreement and its performance.

Information Security Program means the documents that describe how Data Recipient will access and use the Data Access Method and how Data Recipient Entities may access and store FSE Materials, Account Information and Personal Information in a manner that complies with the confidentiality and information security requirements of the Agreement. Such information security program must describe the applicable network infrastructure and security procedures and controls that protect Confidential Information on a basis that meets or exceeds the FSE Security Requirements.

Intellectual Property Rights means all intellectual property rights throughout the world, including copyrights, patents, mask works, trademarks, service marks, trade secrets, inventions (whether or not patentable), know how, authors' rights, rights of attribution, and other proprietary rights and all applications and rights to apply for registration or protection of such rights.

Laws means applicable laws, statutes, ordinances, codes, rules, regulations, ethical standards, pronouncements that have the effect of law of any Government Authority, regulatory guidance and any court order.

Major Risk means actual or reasonably likely harm or damage to an FSE Entity or its customers, a Cyber Risk, or other material risk or a requirement of Law.

Person means an individual, corporation, partnership, limited liability company, association, trust, unincorporated organization, or other legal entity or organization, or a Government Authority.

Personal Information means any information relating to an identified or identifiable individual, and any other personal data to the extent protected by applicable Laws.

Personnel means employees, contractors, consultants or any other individuals employed or engaged by the applicable entity.

Privacy Notice means a notice provided to Designated Customers in connection with a Data Recipient Service that is a financial product or service in compliance with Privacy Regulations.

Privacy Regulations means all Laws regarding data protection and privacy and principles, guidelines and code issued by a competent data protection authority to which any FSE Entity or any Data Recipient Entity may be subject, including any amendments or successors thereto, by any country, state, or other jurisdiction.

Representative means an employee, contractor, officer, director or agent of an FSE Entity or a Data Recipient, as applicable.

Scraping means the process whereby a Person, including a Data Recipient Entity (but excluding an FSE Entity or the applicable Designated Customer), collects or obtains Account Information through the use of Customer Account Credentials, by any means other than through the Data Access Method.

Security Breach means: (a) any act or omission by any Data Recipient Entity that compromises or adversely affects the security, confidentiality and/or integrity of any FSE Site or FSE System, including the Data Access Method, or any Data Recipient Access System; (b) the actual or reasonably suspected theft, loss, or unauthorized disclosure, acquisition, destruction, alteration, processing, access to, or misuse of any FSE Materials, Account Information or Personal Information; or (c) any actual or reasonably suspected Cyber Risk. For clarity, the definition of Security Breach is not intended to include inconsequential incidents that occur on a daily basis, such as scans, pings, or other unsuccessful attempts to penetrate computer networks or servers.

ARTICLE 3 IMPLEMENTATION

3.1 Implementation Plan.

(a) The Parties have attached to the Agreement as **Exhibit 6** the plan and timeline for testing and implementing, the Data Access Method, and associated security controls, standards and processes, to allow Data Recipient to begin accessing Applicable Account Information through the Data Access Method for each Data Recipient Service in accordance with the Agreement (such plan and timeline, as may be updated upon agreement of the Parties, the "**Implementation Plan**").

(b) The Implementation Plan will include, for each Designated Customer who is enrolled in one or more Data Recipient Services, the date on which Data Recipient will cease use of Scraping as a means of accessing Account Information of such Designated Customer, and commence use of the Data Access Method (the "**Applicable Cutover Date**"). Without limiting the obligations of the Data Recipient Entities under the Agreement, unless otherwise set forth in the Implementation Plan, as of and after the Effective Date, Data Recipient will, and will cause all Data Recipient Entities to, implement and comply with the Information Security Program for all Account Information collected and/or accessed by the Data Recipient Entities as of and after the Effective Date, and comply with the terms of **Articles 5, 8, 12** and **13** and **Sections 3.4** and **6.3** through **6.6** with respect to all such Account Information.

(c) If there are material changes to the type or elements of the Account Information being accessed, subject to the terms of the Agreement, the Parties will develop an implementation plan to enable and implement additions and changes.

3.2 Performance. Data Recipient will be responsible for implementing and testing the Data Access Method for use by or on behalf of Data Recipient in accordance with the Agreement. Data Recipient will identify and resolve any problems that may impede or delay the timely completion of each task in each implementation plan that is its responsibility. FSE will use reasonable efforts to assist with the resolution of any problems that may impede or delay the timely completion of implementation.

3.3 Cessation of Scraping. A key objective of the Agreement is to cease the use of Scraping, and access to and use of Customer Account Credentials, by the Data Recipient Entities, and shift to a more secure and industry acceptable method of accessing Account Information. Accordingly, as of the Applicable Cutover Date, Data Recipient will ensure that all Data Recipient Entities to, as long as the Agreement is in effect:

(a) will not access, collect or request Customer Account Credentials;

(b) will cease use of, and not use, Scraping as a means of accessing any Account Information; and

(c) will use the Data Access Method as permitted under the Agreement as the sole means for accessing or collecting Account Information; provided, that, Data Recipient is at all times responsible for ensuring that all necessary and appropriate disclosures have been provided and all necessary and appropriate authorizations and informed and explicit consents have been obtained from the Designated Customer in accordance with **Article 5**.

3.4 Customer Account Credentials. If and while any Data Recipient Entity is in possession of Customer Account Credentials, including on any backup or archival systems, each Data Recipient Entity will maintain, store and transmit Customer Account Credentials using strong encryption consistent with industry best practices. As of the Applicable Cutover Date specified in the Implementation Plan and for as long as the Agreement is in effect, the Data Recipient Entities will no longer request, collect or access Customer Account Credentials, and will Delete and Destroy any and all Customer Account Credentials in its or their possession. Upon FSE's request, Data Recipient will attest to FSE that the foregoing is true, and that the Data Recipient Entities have Deleted and Destroyed all Customer Account Credentials.

ARTICLE 4 DATA ACCESS

4.1 Access Rights. Subject to the terms of the Agreement (including the suspension and termination provisions herein), FSE will permit Data Recipient, and Data Recipient agrees, to use and access the Data Access Method solely in order for Data Recipient to collect Applicable Account Information of Designated Customers as authorized by each respective Designated Customer in support of Data Recipient or Data Recipient Clients providing the Data Recipient Service(s) to that Designated Customer. Subject to **Article 3** above, for the purposes of providing Data Recipient Services, the Data Recipient Entities will not access or collect, or attempt to access or collect any Account Information through any FSE Sites or other websites or systems, and will only access or collect Account Information through the Data Access Method as permitted under the Agreement.

4.2 Data Recipient Services. A list of the approved Data Recipient Services as of the Effective Date is set forth in **Exhibit 4**. In the event Data Recipient wishes to (a) add a new Data Recipient Service to the scope of the Agreement or (b) for an existing Data Recipient Service, introduce or implement a new use case, material change (e.g., new functionality or new or change in market focus) or change that may have an adverse impact on the security controls or requirements of the Agreement or enhance the potential of a Major Risk (each, a "**Material Service Change**"), Data Recipient will notify FSE 30 days in advance of the planned implementation. For a change that is not a Material Service Change, Data Recipient will notify FSE of such change as soon as possible, but in any event within five days after implementation. All notices will include reasonable details regarding the applicable change or addition. All Material Service Changes must be approved by FSE in writing in advance of any implementation. Without limiting the foregoing, FSE reserves the right to not allow, or cease the allowance of, access to Account Information for a particular Data Recipient Service if FSE reasonably believes the service: (i) is illegal or could cause a FSE Entity to be in violation of any Law, (ii) does not have reasonable security controls in place or poses a Major Risk or (iii) could cause harm to FSE's reputation or contradicts FSE's business guidelines. Data Recipient will maintain an up-to-date list of Data Recipient Services that it will provide to FSE upon request.

4.3 Data Recipient Access and FSE Activities.

(a) Data Recipient will be responsible for managing and overseeing the assignment of Data Recipient Access Authentication for each Personnel of Data Recipient or a Data Recipient Subcontractor who will have access to the Data Access Method. For the avoidance of doubt, Data Recipient may not provide access to the Data Access Method to Data Recipient Clients and their Personnel. Data Recipient Access Authentication will be individual specific and only the individual who is assigned such Data Recipient Access Authentication may use such Data Recipient Access Authentication. Data Recipient will not permit any Data Recipient Access Authentication to be shared or used by any other individual other than the specific individual to whom Data Recipient Access Authentication is assigned. Data Recipient will be responsible for (i) all access to the Data Access Method by any Person using any Data Recipient Access Authentication, (ii) keeping Data Recipient Access Authentication secure and confidential and (iii) the loss or unauthorized access or use of Data Recipient Access Authentication and any resulting harm or damages. Data Recipient will maintain a log of all access to the Data Access Method by time and individual and, within 24 hours of FSE's request, provide to FSE or its Representative access to such log and the list of the names and contact information of all individuals with access to the Data Access Method during the time period specified by FSE.

(b) Data Recipient agrees that (i) FSE may monitor, record and review any access to the Data Access Method at any time and without notice to any Data Recipient Entity, (ii) the FSE Entities, and their Representatives, may, wherever they do business, store and otherwise process business contact information (BCI) of Data Recipient Personnel, for example, name, business telephone, address, email, and user ID for business dealings with them and (iii) the personnel and resources of the FSE Entities and their Representatives are located at sites of the FSE Entities and their Representatives worldwide, and FSE may use such personnel and resources to carry out its rights and obligations under the Agreement. Data Recipient consents to the foregoing, and Data Recipient will ensure that all Data Recipient Entities are advised of, and have consented to, all such activities. Data Recipient, on its own behalf and on behalf of all Data Recipient Entities waives any right or claims of privacy (express or implied) with respect to all such activities.

(c) Data Recipient acknowledges that FSE intends to, and that Data Recipient will ensure that all Data Recipient Entities to, cooperate fully with any Government Authorities, including law enforcement or judicial investigations, regarding any access to the Data Access Method or any FSE Materials or Account Information. This cooperation may include disclosure of the identities of, and the information transmitted or received by, Persons accessing the Data Access Method.

4.4 Data Recipient Systems. Data Recipient will be responsible for all systems (including software, hardware and connectivity) and tools that Data Recipient or any Data Recipient Subcontractor uses to access the Data Access Method or collect or access Account Information through the Data Access Method ("**Data Recipient Access Systems**"). Data Recipient will ensure that all Data Recipient Access Systems include up-to-date anti-virus and security software that meets best industry practices to prevent Computer Viruses from reaching the Data Access Method through Data Recipient Access Systems. Data Recipient and any Data Recipient Subcontractor will use all other best industry practices to prevent unauthorized access to the Data Access Method or Account Information. Data Recipient or any Data Recipient Subcontractor will use only those remote access methods approved in writing and in advance by FSE and ensure that any computer, system or device used by Personnel of Data Recipient and any Data Recipient Subcontractor to remotely access the Data Access Method will not simultaneously access the Internet or any other third party network while logged on to the Data Access Method.

4.5 Scope of Access.

(a) With respect to Account Information of a Designated Customer available through the Data Access Method, the Data Recipient Entities only will seek to access and/or retrieve Applicable Account Information that: (i) the Designated Customer has given the applicable Data Recipient Entity permission to access; and (ii) is related to the Designated Customer's Account that the Designated Customer has expressly identified as the Account for which the applicable Data Recipient Entity is permissioned to access data. At no time will any Data Recipient Entity seek to access or retain more information than is reasonably necessary to provide the Designated Customer with the Data Recipient Service that the Designated Customer has enrolled in, consistent with the informed and explicit consents provided by the Designated Customer. In the event that any Data Recipient Entity accesses or gathers Account Information from the Data Access Method other than Applicable Account Information that is reasonably necessary to provide the Data Recipient Service(s) that the Designated Customer has enrolled in consistent with the informed and explicit consents provided by the Designated Customer, then Data Recipient will promptly Delete and Destroy such Account Information and will ensure that any Data Recipient Entity that has received such Account Information will Delete and Destroy it.

(b) Pursuant to the terms of the Agreement and then only to the extent permitted by the applicable Designated Customer and by applicable Laws, Data Recipient may (i) use Applicable Account Information to provide such Designated Customer with any applicable Data Recipient Service(s) and (ii) share Applicable Account Information with a Data Recipient Subcontractor or Data Recipient Client solely in support of Data Recipient or the Data Recipient Client providing a Data Recipient Service. Data Recipient will require that all Data Recipient Subcontractors are subject to written agreements with Data Recipient with terms and obligations consistent with the terms and obligations of the Agreement. Data Recipient will be responsible for (1) the compliance by all Data Recipient Subcontractors with the terms of the Agreement to the same extent and in the same manner as Data Recipient and (2) any breach or noncompliance of the terms of the Agreement by a Data Recipient Subcontractor.

(c) Except for use to provide the Data Recipient Services as permitted in the Agreement or as permitted by a Designated Customer in accordance with applicable Laws, Data Recipient will not, and will ensure that Data Recipient Entities do not, sell, exploit or commercialize any Account Information or any information based on or derived from or combined with Account Information, including in any de-identified form.

(d) The Data Recipient Entities will only store and host as permitted under the Agreement FSE Materials and Account Information from locations within the continental United States. Any change to the location of the storage or hosting of FSE Materials or Account Information to outside of the continental United States must be approved in advance by FSE in writing. All access by Data Recipient (and Data Recipient Entities) of FSE Materials and Account Information must comply with all applicable Laws, including Privacy Regulations. Once Account Information is accessed by a Data Recipient Entity, Data Recipient is solely responsible, and no FSE Entity is responsible, for any use of such Account Information by a Data Recipient Entity or any other Person, including in violation of the Agreement.

(e) Without limiting FSE's other rights, Data Recipient agrees that the FSE Entities and their Representatives may display and create interactive tools for Customers that allow the Customers to view and manage consents and disclosures for data access platform companies, including consents and disclosures referencing and relating to Data Recipient and the Data Recipient Services ("**Customer Permission Portal**"). Data Recipient hereby agrees to allow the FSE Entities and their third parties to use the name and logo of Data

Recipient, Data Recipient Clients and the Data Recipient Services on the Customer Permission Portal for the purposes of managing consent and disclosures activity.

4.6 Data Elements.

(a) With respect to Account Information of a Designated Customer to be made available through the Data Access Method, only such Account Information that is within the data elements identified in **Exhibit 1** (referred to as Applicable Account Information) and meets technical standards supported by the Data Access Method will be made available.

(b) After the Effective Date, Data Recipient may request in writing to FSE that data elements relating to Accounts of Designated Customers that are not listed in **Exhibit 1** be made available to Data Recipient as part of the Account Information provided through the Data Access Method. Data Recipient will include a reasonably detailed description of the additional data elements. If FSE agrees to make the additional data available, the Parties will work together to establish an implementation timeline for implementing the availability of the additional data elements and finalize an amendment to the Agreement regarding such change. In no event will FSE be required to agree to any requests for additional data elements.

(c) Upon notice to Data Recipient (which will be at least 90 days' notice unless FSE determines that a shorter period is appropriate to prevent a Major Risk or due to another legitimate business reason), FSE may discontinue making a data element available to Data Recipient.

4.7 Frequency of Access by Data Recipient.[2]

4.8 Valid Access Tokens. Data Recipient agrees to use and continue to use Access Tokens to enable and track the provision of Account Information for each Data Recipient Service. Data Recipient will only collect and access Applicable Account Information for a Data Recipient Service for which there is a current and valid Access Token. For each Data Recipient Service, if a Designated Customer no longer authorizes use of his or her Account Information in connection with a Data Recipient Service, then Data Recipient will no longer use the Data Access Method to access Account Information associated with such Designated Customer attributable to such Data Recipient Service.

4.9 DISCLAIMERS. DATA RECIPIENT UNDERSTANDS AND AGREES THAT ALL USE AND ACCESS TO THE DATA ACCESS METHOD IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NON-INTERFERENCE AND NON-INFRINGEMENT. FURTHER, EACH FSE ENTITY EXPRESSLY DISCLAIMS ANY TYPE OF REPRESENTATION OR WARRANTY REGARDING THE AVAILABILITY OR RESPONSE TIME OF THE DATA ACCESS METHOD OR ACCOUNT INFORMATION OR THAT ACCESS TO THE DATA ACCESS METHOD OR ACCOUNT INFORMATION WILL BE UNINTERRUPTED OR ERROR-FREE; AND EXPRESSLY DISCLAIMS THE ACCURACY, COMPLETENESS, AND CURRENCY OF ACCOUNT INFORMATION. UNLESS EXPRESSLY PROVIDED OTHERWISE IN THE AGREEMENT, NEITHER THE FSE ENTITIES NOR ANY OF THEIR REPRESENTATIVES WILL BE LIABLE TO ANY DATA RECIPIENT ENTITY OR ANY OTHER PARTY FOR ANY LOSS OR INJURY ARISING OUT OF, OR CAUSED IN WHOLE OR IN PART BY, THE DATA ACCESS METHOD OR ACCOUNT INFORMATION OR THEIR ACTS OR OMISSIONS IN RELATION TO THE DATA ACCESS METHOD OR ACCOUNT INFORMATION.

4.10 Data Recipient Clients.[3]

(a) If a Data Recipient Client receives Account Information obtained by or on behalf of Data Recipient through the Data Access Method, then prior to such event, Data Recipient will require such Data Recipient Client to enter into an enforceable agreement that obligates such Data Recipient Client to comply in all material respects with the following sections of the Agreement in the same manner and subject to the same terms as Data Recipient: **Section 3.3(a)**; **Section 3.3(b)**; **Section 3.4** (*Customer Account Credentials*); **Section 4.5** (*Scope of Access*); **Section 4.9** (*Disclaimers*); **ARTICLE 5** (*Designated Customer Disclosure and Consent*); **Section 6.4** (*Retention of Records*); **Section 6.5** (*Audits*); **ARTICLE 8** (*Data Recipient Personnel*); **Section 9.2(b)**; **Section 9.3** (*Anti-Bribery; No Insider Trading*); **Section 11.3** (*Exit Rights*); **Section 11.4** (*Suspension Rights*); and **Section 15.2** (*Insurance*). The foregoing provisions will be deemed the "Required General Provisions."

(b) In addition to the requirements in **Section 4.10(a)**, for any Data Recipient Client that (i) has received Account Information, and (ii) is not an exempt financial institution that is subject to examination by a federal or state Government Authority for legal compliance with applicable Privacy Regulations and data security protections, Data Recipient will require such Data Recipient Client to comply in all material respects with the following sections of the Agreement in the same manner and subject to the same terms as Data Recipient: **Section 6.6** (*Security Reviews and Assessments*); **Section 7.1** (*Quality Assurance*); **Section 13.6** (*Control and Oversight*); **Section 13.7** (*Data Safeguards Generally*); and **Section 13.8** (*Breach of Security*) (except that notice under such **Section 13.8** will be provided to Data Recipient, not FSE). The foregoing provisions will be deemed the "Required Audit and Security Provisions." If Data Recipient Client is an exempt financial institution that is subject to examination by a federal or state Government Authority for legal compliance with applicable Privacy Regulations and data security protections, then Data Recipient Client will be required to comply with all Privacy Regulations and data security protections required by Governmental Authorities.

[2] Note: Include as applicable.

[3] [Note: Fundamental principle of the model contract is to require and enable standard flow down provisions. The sections identified have been selected for safety, security and soundness purposes.]

ARTICLE 5 DESIGNATED CUSTOMER DISCLOSURE AND CONSENT

5.1 Disclosures. Data Recipient and, to the extent applicable, Data Recipient Client, will provide clear and conspicuous disclosures to Designated Customers or prospective Designated Customers (which may be included in an applicable Privacy Notice) that comply with all applicable Laws and that describe how Account Information is collected, accessed, stored and used, including with respect to any derivatives, compilations or combinations of Account Information. These disclosures must: (a) describe the Account Information that will be accessed and/or collected; (b) be present in Data Recipient Terms that are valid and enforceable terms and conditions and that are formally accepted by each Designated Customer; (c) identify or disclose to each Designated Customer any and all categories of third parties to whom Account Information may be provided or whom may use, receive, store, or process Account Information; (d) include the right to terminate the Data Recipient Service at any time; and (e) inform Designated Customers that the Account Information does not represent an official record of the Designated Customer's Account. The Data Recipient Terms also must state that Data Recipient is acting independently and that no FSE Entity has any responsibility or liability with respect to the Data Recipient Services. If Data Recipient or Data Recipient Clients are required by applicable Privacy Regulations to provide a Privacy Notice to Designated Customers in connection with a Data Recipient Service, then Data Recipient will, or will require Data Recipient Clients to, comply with such Privacy Notice and Privacy Regulations, including all obligations to deliver Privacy Notices and restrictions on the sharing and reuse of Personal Information.

5.2 Customer Agreement. Data Recipient must ensure that there are valid and enforceable Data Recipient Terms formally accepted by each Designated Customer that govern Data Recipient or Data Recipient Clients providing the Data Recipient Service to that Designated Customer and that meet the requirements of **Section 5.1**. Data Recipient will, or will require Data Recipient Clients to, obtain and maintain all consents and approvals from the Designated Customers necessary for Data Recipient Entities to access and use the Account Information, as well as any derivatives, compilations or combinations of Account Information, with respect to the Data Recipient Services. Upon FSE's request, Data Recipient will provide copies of Data Recipient Terms for review by FSE.

5.3 Consent Database. Data Recipient will ensure that the party that obtains consents and/or provides disclosures described in this **Article 5** creates and maintains a record of when such consents and disclosures are provided to a Designated Customer and when the Designated Customer has formally accepted the Data Recipient Terms, and the scope and effective date (and, if applicable, expiration / termination dates) of the Data Recipient Terms and any consents. Upon request by FSE, Data Recipient will provide copies, or other evidence acceptable to FSE, of such consents and disclosures.

5.4 Process for Customer Permissions. Notwithstanding Data Recipient's obligations to obtain and maintain Customer consents and disclosures as set forth in the Agreement, the Data Recipient Entities understand and agree that FSE only will allow access to Account Information through the Data Access Method and for those Designated Customers who have authorized FSE to permit the Data Recipient Entities to access the Account Information.

5.5 Customer Issues and Complaints. Data Recipient will be responsible for managing any disputes or issues raised by a Designated Customer relating to the Data Recipient Services. FSE will have the right to engage with the Designated Customer directly regarding any issues and complaints relating to the access of Account Information, and will have the right to terminate access to any Account Information at any time to address a Designated Customer issue or complaint; provided, that, Data Recipient will remain solely responsible for any unauthorized access or use of Account Information once it is accessed or in the possession of any Data Recipient Entity and thereafter.

ARTICLE 6 GENERAL OBLIGATIONS

6.1 Data Recipient Access Systems. Data Recipient will procure, implement and maintain the Data Recipient Access Systems to access and use the Data Access Method. Data Recipient will ensure that all Data Recipient Access Systems are compatible and operate with the Data Access Method, including any updates and replacements thereto. Further, if FSE changes or plans to change its equipment, software or environment and such change requires a change to Data Recipient's equipment, software or environment, FSE will provide notice of such change to its equipment, software or environment at least 60 days' (unless FSE determines that a shorter period is appropriate to prevent a Major Risk or due to another legitimate business reason) prior to Data Recipient being required to implement changes to Data Recipient's equipment, software or environment. Data Recipient will make all changes, including any changes required to comply with Laws, at its own cost and expense. FSE will not be responsible for any integration and compatibility issues, and non-compliance with any Laws, including fines and related costs and expenses, associated with Data Recipient's use of the Data Access Method or access to any Account Information or the operation or functionality of the Data Recipient Access Systems.

6.2 Documentation. Data Recipient will provide to FSE reasonable documentation in printed and electronic formats to enable the FSE Entities to understand the scope of the Data Recipient Services and to facilitate access to the Data Access Method. FSE may use and reproduce for internal purposes all Documentation furnished by Data Recipient, including displaying the documentation on FSE's intranet or other internal electronic distribution system for use only by Representatives with a need to know for the purposes of the Agreement. On a periodic basis as agreed by the Parties, Data Recipient will provide FSE with the reports set forth in **Exhibit 5** in connection with the utilization of the Data Access Method and access to Account Information, and such other reports as agreed by the Parties.

6.3 Notice of Issues. If Data Recipient becomes aware of a situation where (a) it or any Data Recipient Subcontractor has failed to or its reasonably likely to fail to comply with its obligations under the Agreement or (b) a Data Recipient Client is in breach of or its reasonably likely to be in breach of a Required General Provision or Required Audit and Security Provision, as applicable, then Data Recipient will promptly inform FSE in writing of such situation.

6.4 Retention of Records. Data Recipient agrees to maintain complete and accurate books and records regarding the use of the Data Access Methods, access to Account Information by the Data Provider Entities and performance by the Data Provider Entities of the obligations under the Agreement ("**Applicable Records**"), including access activities and security logs, during the Term, and retain Applicable Records for a period of 7 years from creation unless a longer time is required by a Government Authority with jurisdiction over any of the Data Recipient Entities ("**Retention Period**"); provided, however, that in the event of any dispute arising with respect to the Agreement, the Retention Period lasts until the resolution of the dispute becomes final and non-appealable and all obligations of the Parties are fully satisfied. Applicable Records do not include internal financial statements of the Data Recipient Entities.

6.5 Audits. No more frequently than annually (unless more frequently as required by applicable Law or requested due to compliance or security concerns), the FSE Entities, their internal and external auditors, and their Representatives and Governmental Authorities ("**Auditors**") have the right, but not the obligation, during the Term and, if longer, the Retention Period, to audit, review and inspect Applicable Records, as well as the systems of the Data Recipient Entities relating to the obligations under the Agreement. Other than with respect to audits, reviews or inspections by regulators or in an emergency, FSE will provide Data Recipient reasonable notice of any audit, review or inspection. The Data Recipient Entities will reasonably cooperate in any such audit, review or inspection that FSE may undertake. During the Term and Retention Period, the Data Recipient Entities will:

(a) Make Applicable Records, as well as external audit opinions, external audit letters, external audit statements, and external audit reports relating to use of the Data Access Methods, access to Account Information and performance of its obligations under the Agreement, including access activities, available for inspection by Auditors, who will have the right to make copies on the applicable premises or by taking any of these materials to an offsite location for the sole purpose of copying.

(b) In connection with the audit, give Auditors reasonable access, during regular business hours unless a regulator requests differently or there is an emergency audit, to Data Recipient Personnel and the representatives, attorneys and accountants of the Data Recipient Entities.

(c) Provide, without charge, internet access, office space, furniture, telephone, print and other customary facility use in connection with performing any audit or review.

(d) Allow FSE and its Representatives to review documents evidencing that informed and explicit consents from Designated Customers have been properly obtained and are in place, and that proper disclosures have been provided, as described in **Section 5.3**. In addition to its other obligations, Data Recipient will be responsible for ensuring that the informed and explicit consents have been obtained from the Designated Customers to allow such review.

6.6 Security Reviews and Assessments.

(a) As part of the audit described in **Section 6.5**, Auditors may conduct on-site security reviews and assessments, vulnerability testing, and disaster recovery testing for any technology, including Data Recipient Access Systems, hosting, storing or processing Account Information or FSE Materials and otherwise audit the operations of the FSE Entities for compliance with the FSE Security Requirements. If vulnerabilities are identified, Data Recipient will: (i) promptly document and, within formally established timelines, implement a mutually agreed upon remediation plan; and (ii) upon FSE's request, provide FSE with the status of the implementation.

(b) At least annually, Data Recipient and each Data Recipient Client will for the scope approved by FSE (i) have a certified independent public accounting firm or another independent, certified, industry-recognized third party conduct a review and provide a full attestation and report under SOC 2 Type II (or a successor or replacement thereof) or, if a SOC 2 Type II attestation and report is not an available option, then a review and certification reasonably satisfactory to FSE to demonstrate compliance with systems and operational controls, in each case, including a review of all key systems and operational controls used in connection with any Account Information, Personal Information or FSE Materials; and (ii) conduct and provide a full report of an independent network and application penetration test. Data Recipient will provide all findings from these attestations, reviews, and tests to FSE upon receipt from the applicable third party. The Data Recipient Entities will implement the recommendations set forth in such attestations, reviews, reports, and any other reasonable recommendations made by FSE arising out of FSE's analysis of such reviews, and, upon FSE's request, provide FSE with the status of the implementation.

ARTICLE 7 QUALITY ASSURANCE AND GOVERNANCE

7.1 Quality Assurance. The Data Recipient Entities will develop quality assurance and internal controls, including implementing tools and methodologies, to ensure that Account Information and Personal Information is accessed in a secure manner consistent with industry best practices and in compliance with Laws, Designated Customer consents and the terms of the Agreement. Without limiting the foregoing, the Data Recipient Entities will:

(a) maintain a strong control environment in day-to-day operations in accordance with industry standards for any environments that host, access, process or store FSE Materials or Account Information and Personal Information;

(b) develop and execute a process to ensure that every six (6) months internal control self-assessments are performed with respect to any environments that host, access, process or store FSE Materials, Account Information or Personal Information and report the outcomes of such self-assessments to FSE; and

(c) maintain an internal audit function sufficient to monitor the processes and systems used by the Data Recipient Entities (e.g., perform audits, track control measures, communicate status to management, drive corrective action) and that supports audit requirements of the Agreement.

ARTICLE 8 DATA RECIPIENT PERSONNEL

8.1 Personnel. The Data Recipient Entities will assign Data Recipient Personnel with appropriate technical and professional skills to enable them to perform their duties, and meet the obligations, under the Agreement. Data Recipient will be responsible for payment of wages, salaries, overtime pay and other compensation due to any Data Recipient Entities (and each Data Recipient Entity is responsible for the payment of wages, salaries, overtime pay and other compensation due to its Personnel), the payment for and the provision of benefits and applicable workers' compensation insurance, and withholding of employment related taxes for such individuals and the payment, as applicable, of employment or similar related taxes. No Data Recipient Entity will be deemed an employee, contractor or provider of an FSE Entity as a result of or in connection with the Agreement.

8.2 Replacement. Data Recipient will immediately remove and replace, or ensure that the applicable Data Recipient Entity removes and replaces, any Data Recipient Personnel who interact with an FSE Entity or who access or use the Data Access Method who have been formally charged with a crime described in **Section 8.4** or who Data Recipient is reasonably aware is engaged in the use of illegal drugs. Data Recipient will consider in good faith any request from FSE to remove and replace any other Data Recipient Personnel who interact with an FSE Entity or who access or use the Data Access Method.

8.3 Compliance.

(a) The Data Recipient Entities understand that FSE operates under various Laws that are unique to the security-sensitive banking industry. As such, Persons that provide Data Recipient Services are held to a higher standard of conduct and scrutiny than in other industries or business enterprises. Each Data Recipient Entity represents that it maintains comprehensive hiring policies and procedures and, through its hiring policies and procedures, including Background Checks, it endeavors to hire the best candidates with appropriate character, disposition, and honesty. In the event that a Data Recipient Entity employs non-U.S. citizens to provide Data Recipient Services, such Data Recipient Entity will ensure that all such persons have and maintain appropriate visas to enable them to provide the Data Recipient Services.

(b) FSE will notify Data Recipient of any act of dishonesty or breach of trust committed against any FSE Entity, which may involve Data Recipient Personnel of which FSE becomes aware, and Data Recipient will notify FSE if it becomes aware of any such offense. Following such notice, at the request of FSE and to the extent permitted by Law, the Data Recipient Entities will cooperate with investigations conducted by or on behalf of FSE.

8.4 Background Checks. No Data Recipient Entity will knowingly permit any individual to have access to the Data Access Method, FSE Materials or Account Information who has been convicted of a crime or has agreed to or a pretrial diversion or similar program in connection with a dishonest act or breach of trust as set forth in Section 19 of the Federal Deposit Insurance Act. Each Data Recipient Entity will conduct or cause to be conducted, at its expense, background checks on all of its Personnel who have access to the Data Access Method, FSE Materials or Account Information that are consistent with generally applicable standards in the financial services industry ("**Background Checks**"). Upon FSE's request, Data Recipient will certify to FSE that all Background Checks have been conducted and that all Data Recipient Personnel who have access to FSE Materials or Account Information have passed a Background Check.

8.5 Personnel Monitoring. Data Recipient will be responsible for monitoring and managing the time and efforts expended by Data Recipient Personnel, and will give the Agreement the priority required, so as to meet its obligations under the Agreement.

8.6 Data Recipient Entities.

(a) Prior to the Effective Date and thereafter upon FSE's request, Data Recipient agrees to provide to FSE a list of then-current Data Recipient Subcontractors and Data Recipient Clients. In the event Data Recipient wishes to add a Person to the list of permitted Data Recipient Subcontractors or Data Recipient Clients, Data Recipient will provide FSE with notice at least 10 Business Days prior to such addition. If FSE reasonably determines that a Data Recipient Subcontractor or a Data Recipient Client poses an unacceptable level of risk, FSE will have the right to refuse (or cease to allow) access to, or require Data Recipient to refuse (or cease to allow) access to, a Data Recipient Subcontractor or Data Recipient Client upon notice to Data Recipient prior to such a Data Recipient Subcontractor or Data Recipient Client being added or, once added, upon at least 30 days' prior notice, unless FSE determines that a shorter notice period is appropriate due to an emergency or Major Risk or other legitimate business reason, and without limiting FSE's rights under **Section 11.2(b)**.

(b) Data Recipient will remain responsible for obligations, services and functions performed by Data Recipient Entities to the same extent as if those obligations, services and functions were performed by Data Recipient Personnel. Data Recipient will indemnify, defend and hold harmless FSE and the FSE Entities and each of their respective officers, directors, employees, temporary staff, agents, successors and assigns from any and all claims by Data Recipient Subcontractors and Data Recipient Clients and Losses and threatened Losses, arising from or in connection with any non-compliance or breach of the Agreement by any Data Recipient Entity, including if arising from a contract with a Data Recipient Entity having different terms and conditions from the Agreement. Data Recipient will be FSE's sole point of contact. With respect to a Data Recipient Entity, Data Recipient will not disclose Confidential Information of FSE to such Data Recipient Entity until such Data Recipient Entity, as applicable has executed a nondisclosure agreement that contains terms as stringent as the terms set forth in the Agreement. Data Recipient will promptly pay for all services, materials, equipment and labor used by Data Recipient or Data

Recipient Subcontractors, and Data Recipient will keep the assets and accounts of the FSE Entities and their Representatives free of all encumbrances.

ARTICLE 9 REPRESENTATIONS AND WARRANTIES

9.1 Mutual Representations and Warranties. Each Party represents and warrants that: (a) the Party's execution, delivery and performance of the Agreement: (i) have been authorized by all necessary corporate action, (ii) do not violate the terms of any Law to which such Party is subject or the terms of any material agreement to which such Party or any of its assets may be subject and (iii) except as expressly set forth in the Agreement, are not subject to the consent or approval of any third party; (b) the Agreement is the valid and binding obligation of the representing Party, enforceable against such Party in accordance with its terms; and (c) such Party is not subject to any pending or threatened litigation or governmental action that could interfere with such Party's performance of its obligations hereunder.

9.2 Data Recipient Representations, Warranties and Covenants. Data Recipient represents, warrants and covenants to the FSE Entities on behalf of itself and each Data Recipient Entity that as of the Effective Date and throughout the Term:

(a) it has not violated, and will not violate, any applicable Laws or FSE policies of which Data Recipient has been given prior written notice regarding the offering of inducements in connection with the execution and delivery of the Agreement. If a Data Recipient Entity does not comply with the foregoing, FSE will have the right to terminate the Agreement for cause without affording an opportunity to cure;

(b) it complies with all Laws and Privacy Regulations, including in connection with any Data Recipient Services;

(c) it will render its obligations under the Agreement with promptness and diligence and will execute them in a professional, competent and workmanlike manner, conforming to generally accepted standards applicable to nationally recognized firms specializing in data access, in accordance with the terms of the Agreement;

(d) it will perform its responsibilities under the Agreement in a manner that does not infringe, or constitute an infringement or misappropriation of, the patent, copyright, trademark, trade secret or other proprietary rights of a third party, and any Data Recipient Services and Data Recipient Access Systems do not infringe or misappropriate the patent, copyright, trademark, trade secret or other proprietary rights of a third party;

(e) it will prevent (i) the introduction or proliferation of any Computer Virus into FSE Systems or any other systems used in connection with the provision of the Data Recipient Services and (ii) damage or loss of any FSE System or FSE Materials. Without limiting Data Recipient's other obligations under the Agreement, Data Recipient covenants that if there is any damage or loss to FSE Systems or FSE Materials caused by any Data Recipient Entity or caused or introduced by viruses or a Computer Virus in or passed through the systems of Data Recipient or other resources provided by any Data Recipient Entity, then Data Recipient will mitigate and remediate (including restoration of FSE Materials and FSE Systems) the cause and effects of such damage, loss, viruses or Computer Virus (including restoring or recovering any data or results at no charge to the FSE Entities within a commercially reasonable time);

(f) it will cause any Data Recipient Services and Data Recipient Access Systems to be integrated and compatible with the Data Access Method;

(g) no Data Recipient Entity nor any individual, entity, or organization holding any material ownership interest in any Data Recipient Entity, nor any officer or director, is an individual, entity, or organization with whom any United States Law prohibits United States companies and individuals from dealing, including, without limitation, names appearing on the Specially Designated Nationals and Blocked Persons List (SDN) published by OFAC. Each Data Recipient Entity will covenant to FSE that it will not cause FSE to be in violation of any regulation administered by OFAC; and

it will comply with all applicable rules and regulations of the Fair Credit Reporting Act ("**FCRA**"), if applicable. Data Recipient agrees that it will notify FSE, as legally permitted and practicable, of any regulatory investigation initiated by any regulator with jurisdiction over any Data Recipient Entity involving FCRA. Data Recipient agrees that it will notify FSE if it or any Data Recipient Entity determines that it is covered under the FCRA or begins to comply with the FCRA.

9.3 Anti-Bribery; No Insider Trading.

(a) Each Data Recipient Entity is familiar with, has complied with, and will comply in all respects with the Laws regarding the offering of unlawful inducements (including the U.S. Foreign Corrupt Practices Act, as amended, and other anti-corruption and anti-bribery Laws). Each Data Recipient Entity will comply with applicable FSE policies communicated to Data Recipient in writing regarding unlawful inducements.

(b) Data Recipient will cause all Data Recipient Personnel to agree to prohibitions against using "inside information" and the trading of "insider information" as part of compliance with Data Recipient policies and certify compliance with such policies on an annual basis.

9.4 Assurances. If FSE is concerned about Data Recipient's financial stability, FSE may request, and Data Recipient will provide to FSE, reasonable assurances of Data Recipient's ability to perform its duties hereunder. Failure by Data Recipient to provide such reasonable assurances to FSE will be deemed a material breach of the Agreement. Data Recipient will notify FSE in the event there is a change of control or material adverse change in Data Recipient's business or financial condition after the Effective Date.

ARTICLE 10 COMPENSATION

10.1 Access Fees. *[Note: Choose one of the alternatives]*

[*Alternative #1*: As of the Effective Date, FSE will not charge Data Recipient an access fee or other fees as part of FSE providing Data Recipient with access to the Data Access Method. In the event that FSE elects to charge a fee for such access at such later date or the Agreement is amended to expand the list of Data Recipient Services or Account Information data elements, the Parties will meet to discuss in good faith the circumstances under which FSE may charge, and the amount of the fees, for such access to the Data Access Method and Account Information.]

[*Alternative #2 ADD A NEW EXHIBIT IF THIS SECTION IS ADDED; UPDATE LIST OF EXHIBITS ON SIGNATURE PAGE*: Data Recipient will pay to FSE the fees and charges set forth in **Exhibit [XXX]** relating to the Agreement (the "**Fees**"). FSE will submit invoices to Data Recipient detailing the Fees and other amounts payable by Data Recipient. Data Recipient will be responsible for all taxes associated with the Fees. Data Recipient will remit payment to FSE within 30 days following its receipt of each such invoice. FSE is entitled to interest on the unpaid amount of any invoice that remains unpaid following the due date. The interest rate will be 12% per annum (or, if lower, the maximum rate permitted by applicable Law). Such interest will accrue on a daily basis from the due date until actual payment of the overdue amount.]

10.2 Expenses. *[Note: confirm business deal; amend if there are implementation costs or project expenses to be reimbursed]* Each Party will bear its own expenses incurred in performing its obligations under the Agreement, unless otherwise agreed by the Parties. Accordingly, these expenses will not be separately reimbursable.

ARTICLE 11 TERM, TERMINATION AND SUSPENSION

11.1 Term. The initial term of the Agreement begins on the Effective Date and ends on [●], unless terminated earlier in accordance with the terms of the Agreement (the "**Initial Term**"). Thereafter, the Agreement automatically renews on the same terms and conditions for additional one-year periods (each a "**Renewal Term**" and together with the Initial Term, the "**Term**") on each anniversary of the Effective Date, unless either Party provided the other Party written notice of termination at least 90 days prior to the end of the Initial Term or then-effective Renewal Term, as applicable.

11.2 Termination Events.

(a) FSE may terminate the Agreement in whole or in part (by Data Recipient Service or by Designated Customer) for convenience and without cause at any time by giving Data Recipient at least 180 days' prior written notice designating the termination date. Data Recipient may terminate the Agreement for convenience and without cause at any time by giving FSE at least 30 days' prior written notice designating the termination date.

(b) FSE may terminate the Agreement with immediate effect upon notice to Data Recipient if FSE in good faith believes that its continued participation in the Agreement will result in a violation of any applicable Law or adversely impact the FSE Entities' compliance with Laws (including regulatory guidelines or requirements, or if there is Security Breach).

(c) FSE may, by giving written notice to Data Recipient, terminate the Agreement in whole or in part for cause as of a date specified in a notice of termination if any of the following occurs: (i) a Data Recipient Entity breaches in any material respect any of its obligations under the Agreement which breach is not cured within 30 days after notice of the breach is given by FSE to Data Recipient or such breach is not capable of being cured within 30 days; (ii) a Data Recipient Entity fails to comply with the compliance, confidentiality or data protection or use requirements under the Agreement; (iii) a material control weakness associated with the Agreement is identified that FSE is required to disclose or is advised to disclose in public filings of FSE or an FSE Entity; or (iv) a Data Recipient Entity becomes the subject of any action or investigation by any Government Authority or regulatory agency that in FSE's judgment could render Data Recipient unable to meet its obligations under the Agreement, involves material fraud or financial irregularities by or on behalf of the Data Recipient Entity or any illegal activities by or on behalf of Data Recipient Entity, or in FSE's judgment could negatively impact FSE's reputation.

11.3 Exit Rights. Upon expiration or termination of the Agreement, (a) FSE will have the rights set forth in **Article 12** and Data Recipient will deliver to FSE a copy of all FSE Materials in the possession of any Data Recipient Entities and (b) Data Recipient will (and will cause all Data Recipient Subcontractors and Data Recipient Personnel to) immediately cease all use of the Data Access Method.

11.4 Suspension Rights.

(a) In addition to FSE's termination rights in the Agreement, and subject to this **Section 11.4**, FSE will have the right to suspend Data Recipient's access, in whole or in part, to the Data Access Method (including for a particular Data Recipient Service or Data Recipient Client), for the following reason(s): (i) the occurrence of any event set forth in **Section 11.4(b)**; (ii) FSE's good-faith belief that a Data Recipient Entity is acting in an unauthorized manner with respect to its access to the Data Access Method (where FSE has the technical ability in place to suspend access by Data Recipient Entity, only for the Data Recipient Entity that is acting in an unauthorized manner); (iii) a Designated Customer requests that FSE no longer permit Data Recipient or a Data Recipient Client to access its Account Information (such suspension will only be applied to the requesting Designated Customer); or (iv) FSE's good-faith belief that there is a risk of a Security Breach with respect to the Data Access Method or Data Recipient Access Systems or that suspending access is reasonably necessary to prevent a Major Risk or due to another legitimate business reason.

(b) FSE will provide Data Recipient with notice of the suspension, including if permitted a description of the scope of the suspension and the reasons for the suspension. FSE will provide advance notice of the suspension, if and as possible; provided, that, notwithstanding anything in this **Article 11** to the contrary, in the event there is a Security Breach or any other significant incident compromising the confidentiality and/or integrity of the Data Access Method, any FSE Systems or any Account Information, FSE may suspend access to the Account Information or Data Access Method immediately without prior notice. Upon notice of suspension, the applicable Data Recipient Entities will immediately: (i) cease attempting to access any Account Information, whether through the Data Access Method or through Scraping; and (ii) comply with FSE's reasonable requests to assist FSE in remediating and preventing further harm or loss.

(c) The Parties will work together to remediate the reason for any suspension, with FSE having the final authority as to the duration and extent of any suspension. At any point, upon notice to Data Recipient, FSE will have the right to terminate access to the Data Access Method by providing Data Recipient notice (which will be at least 30 days' notice unless FSE determines that a shorter period is appropriate to prevent a Major Risk or due to another legitimate business reason). FSE may suspend access to the Data Access Method as necessary to perform maintenance and changes.

ARTICLE 12 DATA AND OTHER PROPRIETARY RIGHTS

12.1 FSE Systems and Resources. FSE will own perpetually all right, title and interest in and to, together with any and all Intellectual Property Rights, inherent in and appurtenant to FSE Systems and FSE Materials. Data Recipient will only use the FSE Materials as expressly permitted by FSE and in accordance with the terms of the Agreement, and only in connection with the specific purpose for which FSE provides such FSE Materials to Data Recipients.

12.2 Adverse Claims. Data Recipient will promptly notify FSE in writing, of any threat, or the filing of any action, suit or proceeding, against any Data Recipient Entity (a) alleging infringement, misappropriation or other violation of any Intellectual Property Rights related to any Data Recipient Access Systems, or (b) in which an adverse decision would reasonably be expected to have a material adverse effect on any Data Recipient Entity.

12.3 Trademarks.

(a) Each Party (the "**Using Party**") agrees that, with respect to its use of the other Party's (the **"Owning Party**'s") trademarks, marks, logos and trade names ("**Marks**") approved by the Owning Party for the Using Party's use: (i) as between the Parties, all rights in and to such Marks are owned by the Owning Party, (ii) the Using Party will do nothing inconsistent with such ownership, (iii) all uses of such Marks, including all associated goodwill, will inure to the sole benefit of and be on behalf of the Owning Party, (iv) it will use the Owning Party's Marks in strict accordance with any guidelines for the use of such Marks as provided by the Owning Party from time to time, (v) it will not alter any such Marks and will use only exact reproductions thereof as supplied by the Owning Party, and (vi) at the Owning Party's reasonable request, all depictions of such Marks which the Using Party intends to use will be submitted to the Owning Party for approval. The Parties agree in good faith to discuss the uses of Marks during the Term.[4]

(b) Except as permitted in the Agreement, neither Party will issue any media releases, public announcements or public disclosures relating to the Agreement or use the Owning Party's Marks, including in promotional or marketing material, provided that nothing in this paragraph will restrict any disclosure required by Law. The Using Party will provide a copy of any proposed disclosure required by Law for the Owning Party's review and approval, unless prohibited by Law.

12.4 Other Terms. Except as specifically provided in the Agreement, FSE does not grant to any Data Recipient Entity any right or license, express or implied, in any FSE Materials or any other intellectually property of the FSE Entities. Except as specifically provided in the Agreement, Data Recipient does not grant to FSE, either itself or on behalf of any Data Recipient Client or Data Recipient Subcontractor, any right or license, express or implied, in the Data Recipient Access Systems or any Data Recipient Service. Except as expressly agreed to by the Parties in writing, Data Recipient will not, and will ensure that no Data Recipient Entity does, (a) reverse engineer, disassemble, decompile or otherwise attempt to derive source code from the Data Access Method or the FSE Systems, (b) make the Data Access Method or the FSE Systems available to any third parties other than as expressly permitted in the Agreement, (c) modify, adapt, translate or create derivative works based on the Data Access Method or the FSE Systems, (d) reproduce any portion of the Data Access Method or the FSE Systems except as expressly permitted in the Agreement, or (e) permit or authorize any party to do any of the foregoing.

ARTICLE 13 CONFIDENTIALITY AND DATA PROTECTION

13.1 Definitions. "**Confidential Information**" means information that is disclosed by a Party in connection with the Agreement that is not generally known to the public and, at the time of disclosure, is identified as, or would reasonably be understood by the receiving Party to be, proprietary or confidential. Subject to the foregoing, with respect to each Party, Confidential Information includes: (a) business plans, strategies and analyses and sales and marketing information; (b) financial information; (c) business processes, methods, and models; (d) employee, customer, business partner, and supplier information; (e) product and service specifications; (f) the non-public records compiled in connection with enforcement responsibilities, reports of examination, supervisory correspondence, investigatory files, and internal memoranda; and (g) the terms of the Agreement. FSE Materials and the Data Access Method are Confidential Information of FSE. Data Recipient Access Systems (and the related Data Recipient documentation) are Confidential Information of Data Recipient.

[4] Add any branding requirements, if any, to be included on the Account Information, including any disclaimers.

13.2 Obligations. Each Party will treat all Confidential Information of the other Party as confidential and will disclose such Confidential Information only to those individuals with a reasonable need to know within their organizations (provided that such individuals are bound by the confidentiality obligations in the Agreement). Each Party will use at least the same degree of care to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure, publication or dissemination of its own information of a similar nature, but in no event less than a reasonable standard of care. A Party may disclose Confidential Information of the other Party to advisors, Auditors and other Representatives necessary to perform, assess or interpret such Party's obligations under the Agreement, and subject to such third party agreeing to confidentiality obligations substantially equivalent to those set forth in the Agreement, where (a) the use of such an entity is authorized under the Agreement or such disclosure is reasonably necessary to or otherwise naturally occurs in that third party's scope of responsibility and solely for the benefit and (b) the disclosure is in accordance with the Agreement. Neither Party will (i) make any use or copies of the Confidential Information of the other except as necessary to perform its obligations under the Agreement, (ii) acquire any right in or assert any lien against the Confidential Information of the other, or (iii) refuse for any reason (including a default or material breach of the Agreement by the other Party) to promptly provide the other Party's Confidential Information (including all copies thereof) to it if requested in writing to do so. Upon the expiration or termination for any reason of the Agreement and the concomitant completion of a Party's obligations under the Agreement, each Party will (except as otherwise provided for in the Agreement) return or Delete and Destroy, as the other may direct, all documentation in any medium that contains, refers to, or relates to the other Party's Confidential Information, and retain no copies (other than required by Law). In addition, Data Recipient will ensure that Data Recipient Entities comply with these confidentiality provisions, and that all Data Recipient Entities handling such Confidential Information have been appropriately trained in the implementation of the applicable information security policies and procedures. Data Recipient is responsible and liable for all acts and omissions of all Data Recipient Entities. Data Recipient must regularly audit and review the respective information security policies and procedures of the Data Recipient Entities to ensure their continued effectiveness and determine whether adjustments are necessary in light of circumstances including changes in technology, customer information systems or threats or hazards to Confidential Information. Notwithstanding anything to the contrary set forth elsewhere in the Agreement, each Party will be permitted to (1) identify the other Party by name, and (2) disclose the existence of the Agreement and the terms and conditions of the Agreement to its advisors, Auditors and other Representatives.

13.3 Required Disclosures. To the extent legally permitted, Data Recipient will notify FSE of any actual or threatened requirement of Law to disclose Confidential Information promptly upon receiving actual knowledge thereof and will cooperate with FSE's reasonable, lawful efforts to resist, limit or delay disclosure. Nothing in this Section will require any notice or other action by FSE in connection with requests or demands for Confidential Information by regulators or examiners.

13.4 Exceptions. The obligations of confidentiality in this **Article 13** will not apply to any information that (a) a Party rightfully has in its possession when disclosed to it, free of obligation to the other Party to maintain its confidentiality; (b) a Party independently develops without access to the other Party's Confidential Information; (c) is or becomes known to the public other than by breach of the Agreement or (d) is rightfully received by a Party from a third party without the obligation of confidentiality. Any combination of Confidential Information disclosed with information not so classified will not be deemed to be within one of the foregoing exclusions merely because individual portions of such combination are free of any confidentiality obligation or are separately known in the public domain.

13.5 Privacy Regulations. Data Recipient acknowledges that FSE is required to comply with the information security standards required by the Privacy Regulations. If applicable, Data Recipient will comply with (and cause all other Data Recipient Entities to comply with), and assist FSE in complying with, Privacy Regulations and the FSE Security Requirements.

13.6 Control and Oversight. During the Term, Data Recipient will ensure the following:

(a) Adequate governance and risk assessment processes are in place to maintain controls over Confidential Information. A security awareness program must be in place or implemented that communicates security policies to all Data Recipient Entities having access to Confidential Information.

(b) Notification to FSE of changes that may impact the security of Confidential Information. Such changes requiring notification include, by way of example and not limitation, outsourcing of computer networking, data storage, management and processing or other information technology functions or facilities and the implementation of external web-enabled (Internet) access to Confidential Information.

(c) Use of strong, industry-standard encryption of Confidential Information transmitted over public networks (e.g., Internet, non-dedicated leased lines) and backup tapes residing at off-site storage facilities.

13.7 Data Safeguards Generally.

(a) The FSE Security Requirements as of the Effective Date are set forth in **Exhibit 2**. FSE may make changes to the FSE Security Requirements from time to time upon reasonable notice to Data Recipient. The Data Recipient Entities will comply with the FSE Security Requirements.

(b) Data Recipient will establish and maintain an Information Security Program that meets the FSE Security Requirements, including safeguards against the disclosure, destruction, loss, or alteration of FSE Materials, Account Information or Personal Information in the possession of any Data Recipient Entity. The Data Recipient Entities will not attempt to access, and will not access or allow access to, FSE Materials, Account Information or Personal Information to which it is not entitled or that is not required under the Agreement. Without limiting the foregoing, the Data Recipient Entities will institute security measures consistent with best practices in the financial services industry to guard against the unauthorized access, alteration, destruction or loss of FSE Materials, Account Information or Personal Information.

(c) Data Recipient will make available to FSE a copy of its written Information Security Program for evaluation. The Information Security Program will conform at a minimum to the FSE Security Requirements. Data Recipient will deliver to FSE an updated Information Security Program (including Data Recipient Security Controls) or confirm that no changes have been made to the Information Security Program, each year on the anniversary of the Effective Date. Data Recipient will require any Data Recipient Entities to implement and administer an information protection program and plan that complies with FSE Security Requirements.

(d) The Data Recipient Entities will implement and maintain Data Recipient Security Controls in compliance with FSE Security Requirements. In connection with the review of Data Recipient Security Controls, the Data Recipient Entities will (i) participate in FSE's assessment process including completion of an online assessment questionnaire; (ii) engage in periodic discussions between Personnel of the FSE Entities and the Data Recipient Entities to review Data Recipient Security Controls; and (iii) deliver to FSE network diagrams depicting perimeter controls and security policies and processes relevant to the protection of Confidential Information. Data Recipient will be responsible for security controls management, including compliance with Data Recipient and FSE controls.

(e) Additionally, whenever a Data Recipient Entity has FSE Materials, Account Information or Personal Information and to the extent 16 C.F.R. Part 681 is applicable to a Data Recipient Entity, Data Recipient will ensure that there are policies and procedures to detect patterns, practices, or specific activity that indicates the possible existence of identity theft ("**Red Flags**") that may arise in the performance of any obligations under the Agreement and report the Red Flags to FSE and take appropriate steps to prevent or mitigate identity theft.

(f) The Data Recipient Entities will cooperate with FSE in connection with efforts to assess and remediate a Cyber Risk.

(g) The Data Recipient Entities will only transfer (including internal transfers that occur beyond the internal firewalls of Data Recipient or a Data Recipient Client) the FSE Materials, Account Information and Personal Information in a secure and confidential manner, including, at a minimum, encrypting the data in accordance with FSE policies and restrictions set forth in **Exhibit 2** or through establishing a virtual private network with the FSE Entities in a manner as approved by FSE, and will comply with all security provisions and procedures set forth in FSE's data protection policies and procedures set forth in **Exhibit 2**.

(h) The Information Security Program will be consistent with the generally accepted industry standards, including "Generally Accepted Principles and Practices for Securing Information and Technology Systems" (GAPPs) issued by the National Institute of Standards & Technology and the ISO 27000 series unless instructed otherwise by FSE. Data Recipient may revise such security procedures from time to time upon written approval from FSE.

(i) Data Recipient and Data Recipient Subcontractors will use an FSE approved real-time intrusion detection system on all Data Recipient Access Systems. Data Recipient will actively monitor the intrusion detection system for activities that correspond to attempts at breaking the security of the Data Recipient Access Systems. Along with the deployment of such an intrusion detection system, Data Recipient and Data Recipient Subcontractors will adopt and follow operational procedures to disable the source of any perceived attack and escalation procedures to notify FSE and Data Recipient security groups for follow-up action.

(j) Data Recipient and Data Recipient Subcontractors will provide real-time security event logging data for all Data Recipient Access Systems that contain, process, transact or in any way make up the control or processing environment of the FSE Entities' data or systems, to a log retention server that FSE designates and operates.

13.8 <u>Breach of Security</u>.

(a) In the event a Data Recipient Entity discovers or is notified of a Security Breach relating to the Confidential Information of FSE , Data Recipient will immediately (and in any event in accordance with notice requirements under applicable Law within sufficient time to comply with notice obligations if applicable) (i) notify FSE of such breach or potential breach and (ii) if the Confidential Information of FSE was in the possession of or under the control of a Data Recipient Entity at the time of such breach or potential breach or caused by a Data Recipient Entity, investigate and remediate the cause and effects of the breach or potential breach and provide FSE with assurance satisfactory that such breach or potential breach will not reoccur.

(b) In the event a Data Recipient Entity discovers or is notified of a Security Breach relating to Account Information or Personal Information of a Designated Customer, (i) Data Recipient will immediately notify FSE, (ii) Data Recipient will notify the affected individuals in accordance with notice requirements under applicable Law and (iii) if the Confidential Information of FSE was in the possession of or under the control of a Data Recipient Entity at the time of such breach or potential breach or caused by a Data Recipient Entity, (1) immediately investigate and remediate the cause and effects of the breach or potential breach and (2) provide FSE with assurance satisfactory to FSE that such breach or potential breach will not reoccur.

(c) The Parties agree to reasonably cooperate with each other during the investigation of a Security Breach, including the delay of remediation, and as otherwise required by law enforcement. FSE will have the right to participate in any security investigation relating to the Agreement, Confidential Information of FSE or FSE Systems.

ARTICLE 14 LIABILITY

14.1 Data Recipient Indemnification. Data Recipient will indemnify, defend (subject to **Section 14.3**), and hold harmless FSE, the FSE Entities and their Representatives, successors and permitted assigns from and against any and all claims made or threatened by any third party and all related losses, including expenses, damages, costs and liabilities and reasonable attorneys' fees and expenses incurred in investigation or defense, (such losses collectively, "**Losses**"), to the extent such claims or Losses arise out of or relate to the following:

(a) any grossly negligent act or omission or willful misconduct by any Data Recipient Entity or any breach in a representation, covenant or obligation of any Data Recipient Entity included in the Agreement;

(b) any actual or alleged improper or unauthorized use, transmission, access, disclosure, sale, distribution, display, storage, loss, or Security Breach of any FSE Materials, Account Information or Personal Information accessed or caused by or in the possession of or under the control of any Data Recipient Entity, or actual or alleged breach by any Data Recipient Entity of any of the confidentiality or data protection provisions in the Agreement;

(c) any actual or alleged infringement, violation, or misappropriation of the Intellectual Property Rights of any third person with respect to the services provided by, and/or the resources, materials, work product, software, equipment or other assets used or provided by, any Data Recipient Entity, including (i) any Data Recipient Services; or (ii) a Designated Customer's use of any Data Recipient Services (including FSE's transmission of data in support of such use);

(d) any Data Recipient Services or Data Recipient Access Systems; and

(e) a breach by a Data Recipient Client or its Personnel of a Required General Provision or a Required Audit and Security Provision (as set forth in **Section 4.10)**.

14.2 FSE Indemnification. FSE will indemnify, defend (subject to **Section 14.3**), and hold harmless Data Recipient, successors and permitted assigns from and against any and all claims made or threatened by any third party and all related Losses to the extent such Losses arise out of or relate to the following:

(a) any grossly negligent act or omission or willful misconduct by FSE or an FSE Entity; and

(b) any actual or alleged infringement, violation, or misappropriation of the Intellectual Property Rights of any third person with respect to the Data Access Method.

14.3 Indemnification Procedures. Each indemnified party will provide the indemnifying party with prompt written notice of any claim, demand or action for which the indemnified party is seeking or may seek indemnification hereunder (provided that the failure of the indemnified party to promptly notify the indemnifying party hereunder will not relieve the indemnifying party of any liability with respect to the claim, except to the extent the indemnifying party demonstrates that the defense of the claim is prejudiced by such failure). The indemnifying party will keep the indemnified party fully informed concerning the status of any litigation, negotiations or settlements of any such claim, demand or action. The indemnified party will be entitled, at its own expense, to participate in any such litigation, negotiations and settlements with counsel of its own choosing. The indemnifying party will not have the right to settle any claim if such settlement arises from or is part of any criminal action or proceeding, or contains a stipulation to, or an admission or acknowledgement of, any wrongdoing (whether in tort or otherwise) on the part of the indemnified party without the prior written consent of such indemnified party. Notwithstanding the foregoing, if a Government Authority brings a claim against any FSE Entity that is the subject of the indemnities in **Section 14.1**, FSE will have the right to assume control of the defense of any such claim; and Data Recipient will reimburse the FSE Entities for all reasonable costs of defense. The Data Recipient Entities will cooperate, at its own cost, in all reasonable respects with FSE and its attorneys in the investigation, trial and defense of such claim and any appeal arising therefrom, and may participate in such defense at its own cost.

14.4 LIABILITY.

(a) EXCEPT AS SET FORTH IN **SECTIONS 14.4(B) AND (C)**, NEITHER PARTY WILL BE LIABLE TO THE OTHER PARTY FOR INDIRECT, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, PUNITIVE, OR SPECIAL DAMAGES, INCLUDING LOST PROFITS OR LOST REVENUES, REGARDLESS OF THE FORM OF THE ACTION OR THE THEORY OF RECOVERY, EVEN IF THAT PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

(b) Liability arising from or relating to the following will not be subject to any exclusion: death, bodily injury, or real or tangible property damage; fraud, theft, gross negligence, or willful or reckless misconduct; indemnification claims; breach of compliance with Laws duties; breach of confidentiality under **Article 13**; and limitations or exclusions not permitted by applicable Law.

(c) Data Recipient will reimburse FSE on demand for reasonable and customary out of pocket costs and expenses incurred by the FSE Entities, to the extent attributable to any breach of the confidentiality or data protection obligations of the Data Recipient Entities with respect to safekeeping of Account Information or Personal Information or relating to Account Information or Personal Information in the possession or control of any Data Recipient Entity, including costs and expenses associated with addressing and responding to any such violation, including: (a) preparation and mailing or other transmission of notifications; (b) preparation and mailing or other transmission of communications to customers, agents and others required by Law, required or recommended by a Government Authority or a reasonable mechanism for mitigating the breach; (c) establishment of a call center and other communications procedures in response to such violation (e.g., customer service FAQs, talking points and training); (d) public relations and other similar crisis management services; (e) reasonable legal and accounting fees and expenses associated with investigation of and response to such event; (f) costs for commercially reasonable credit reporting services; and (g) all claims for government fines, penalties and interest imposed by a Government Authority.

ARTICLE 15 MISCELLANEOUS PROVISIONS

15.1 Survival. The following terms will survive after the expiration or termination of the Agreement: **Section 1.2** (*Interpretation*), **Article 2** (*Definitions*), **Section 4.9** (*Disclaimers*), **Section 5.5** (*Customer Issues and Complaints*), **Section 6.3** (*Notice of Issues*), **Section 6.4** (*Retention of Records*), **Section 6.5** (*Audits*), **Section 8.1** (*Personnel*), **Section 8.6** (*Data Recipient Entities*), **Article 9** (*Representations and Warranties*), **Section 10.2** (*Expenses*), **Section 11.3** (*Exit Rights*), **Article 12** (*Data and Other Proprietary Rights*), **Article 13** (*Confidentiality and Data Protection*), **Article 14** (*Liability*), this **Article 15** (*Miscellaneous Provisions*), **Exhibit 2** (*FSE Security Requirements*) and **Exhibit 3** (*Insurance*), as well as any other terms that expressly or by their nature contemplate performance after such expiration or termination.[5]

15.2 Insurance. Data Recipient's insurance requirements are set forth in **Exhibit 3**.

15.3 Relationship of the Parties. For the purposes of the Agreement, Data Recipient will be deemed to be acting as an independent contractor and neither any Data Recipient Entity nor Data Recipient Personnel will be deemed an agent, legal representative, joint venturer or partner of any FSE Entity. Neither Party is authorized under the Agreement to bind the other with respect to any other person or entity. Nothing in the Agreement will confer any rights upon any person other than the Parties and their respective successors and permitted assigns.

15.4 Assignment. Neither Party may assign or transfer, by change in Control, operation of Law, the Agreement (in whole or in part), or any of obligations hereunder, without the prior written consent of the other Party. All of the terms of the Agreement will be binding upon and will inure to the benefit of each Party's successors and permitted assigns. Any assignment, delegation, or transfer in violation of this provision will be void and without legal effect.

15.5 Dispute Resolution. If a dispute arises out of or in connection with the Agreement, the disputing Party may request a meeting to resolve the dispute. Should the Parties not be able to resolve the dispute within 30 days after the meeting first being requested, then either Party may commence any court or other formal proceedings. Nothing in the Agreement will prevent either Party from taking such action as it deems appropriate (including any application to a relevant court) for injunctive or other emergency or interim relief.

15.6 Governing Law; Jurisdiction. The Agreement is governed by and will be construed in accordance with the Laws of the State of *[Fill in State*] and the United States. The Parties hereby agree to the exclusive jurisdiction of the courts of the State of *[Fill in State*] for the purposes of any action or proceeding brought by either of them in connection with the Agreement. The Parties agree that the foregoing will preclude the jurisdiction and application of any other forum and Law. In any action relating to the Agreement, each of the Parties irrevocably (a) waives the right to trial by jury and (b) consents to service of process by first-class certified mail, return receipt requested, postage prepaid, to the address at which the Party is to receive notice.

15.7 Equitable Relief. The violation of the provisions of **Article 13** may cause immediate and irreparable harm to each Party for which money damages may not constitute an adequate remedy at Law. Therefore, in the event of a breach or threatened breach of said provisions by FSE or a Data Recipient Entity, the Party is not in breach or not threatening to breach will have the right to seek, in any court of competent jurisdiction, an injunction to restrain said breach or threatened breach, without posting any bond or other security.

15.8 Notices. All notices provided for or permitted under the Agreement must be in writing and delivered by (a) hand, (b) commercial overnight courier with written verification of receipt, or (c) certified or registered mail, postage prepaid and return receipt requested, to the Party to be notified, at the address for such Party set forth on the signature page of the Agreement. Notices will be deemed effective upon receipt.

15.9 Severability; Waiver. Any provision of the Agreement that is determined to be invalid or unenforceable in any jurisdiction will be ineffective to the extent of such invalidity or unenforceability in such jurisdiction, without rendering invalid or unenforceable the remaining provisions of the Agreement or affecting the validity or enforceability of such provision in any other jurisdiction. No term or provision of the Agreement will be considered waived, and no breach consented to, unless such waiver or consent is in writing and signed on behalf of the Party against whom it is asserted.

15.10 Counterparts. The Agreement may be executed in any number of counterparts and/or by facsimile or other electronic means agreed to by the Parties, each of which will be deemed an original, but all of which taken together will constitute one single agreement between the Parties, and will become effective when one or more such counterparts have been signed by each of the Parties and delivered to the other Party.

15.11 Remedies. The remedies under the Agreement are cumulative and not exclusive. Election of one remedy will not preclude pursuit of other remedies available under the Agreement or at law or in equity.

15.12 Construction. Notwithstanding the general rules of construction, both FSE and Data Recipient acknowledge that both Parties were given an equal opportunity to negotiate the terms and conditions contained in the Agreement, and agree that the identity of the drafter of the Agreement is not relevant to any interpretation of the terms and conditions of the Agreement.

[5] References to be confirmed prior to finalizing draft.

15.13 Entire Agreement. The Agreement is the entire agreement between the Parties with respect to the subject matter hereof. In the event of a conflict between the terms of the General Terms and the Exhibits, the General Terms will prevail. The Agreement supersedes any other oral or written communications, advertisements or understandings with respect to such subject matter. By entering into the Agreement, Data Recipient waives all terms and conditions contained in any of its documents that are different from or additional to the terms and conditions set forth in the Agreement, and such different or additional terms and conditions will have no legal effect between the Parties.