

Statement of Work (“SOW”)
Project Name: Fraud Anomaly Detection: Phase 2

This Statement of Work (“SOW”), dated March 1, 2018 (the “**Effective Date**”) is entered into by and between Synchrony Financial (the “**Company**”) and PricewaterhouseCoopers Advisory Services LLC (the “**Service Provider**” or “PwC”) pursuant to the Master Services Agreement dated November 5, 2015 by and between Retail Finance International Holdings, Inc. (“**RFIH**”) and PricewaterhouseCoopers LLP (“**PricewaterhouseCoopers**”) (the “**Agreement**”). All terms used in this SOW and not otherwise defined will have the same meaning as in the Agreement.

Check any applicable box:

1. ☐ The Services or Deliverables include software code, application or system to be delivered to the Company.
2. ☐ The Services or Deliverables will involve Service Provider having possession of or storing or processing on Service Provider’s premises or systems Company Confidential Information concerning an identified or identifiable natural person (including customers and employees), including name, address, telephone number, email address, business contact information, social security number, driver’s license number , financial account number or other financial information or medical or health related information (but excluding name, position and contact information for employees working with Service Provider or to whom Service Provider reports).
3. ☐ The Services or Deliverables concern matters that Company or a Company Affiliate is likely to discuss with or disclose to regulators of financial institutions (any such discussion or disclosure being subject to Sections 5.16, 8.4 and other relevant terms of the Agreement).
4. ☐ The Services are Covered Services. “**Covered Services**” means (i) Tax Services; (ii) Transaction Services; (iii) Accounting Advisory Services; (iv) Services involving prospective financial information; (v) Services involving the selection or assessment of third party vendors, insurance claims and other Services where third party interests will be significantly impacted (including, without limitation, Services involving Company’s sharing with Service Provider of personal financial information or personally identifiable information (“PII”)); and (vi) Services that the parties otherwise elect to treat as Covered Services.

If any of the boxes 1-4 is checked, this SOW is not valid and Company shall have no obligation to pay service provider unless this SOW is further approved by the RFIH chief procurement officer and by a representative of the RFIH legal department as evidenced by their signatures at the end of this SOW.

I. RELATIONSHIP OF THIS SOW TO THE AGREEMENT:

- A. This SOW shall not amend, supplement or conflict with the Agreement unless the specific section of the Agreement is specified in this Section I.A.

<u>Section of Agreement Overridden</u>	<u>Specific Overriding Provision of this SOW</u>

B. In no event will this SOW amend, supplement or conflict with the following Sections of the Agreement: Section 1.5 (No Exclusivity), Section 1.6 (Related Parties), Section 1.9 (Order of Precedence) Section 4.3 (Termination for Convenience), Section 7 (Representations and Warranties, except that additional representations, warranties and covenants may be added with respect to the Services contemplated by the applicable SOW), Section 9 (Confidentiality and Material Non-Public Information), Section 10 (Indemnification), Section 11 (Insurance), Section 12.1 (Background Checking), Section 13 (Data Protection and IT Security, except for the formation and modification of Agreed Security Controls as contemplated by such section or Section 1.7 as in effect on the date of the Agreement), Section 16 (Alternative Dispute Resolution), Section 17 (Limitations of Liability), Section 18 (Miscellaneous Provisions and Amendment), or Attachment 3 to the Agreement (Form of SOW).

C. Except as may be described above, this SOW specifically incorporates all of the provisions of the Agreement.

II. PURPOSE AND SCOPE OF THIS SOW.

(a) Purpose. This SOW sets forth the Services to be provided, deliverables, timing, staffing and fees for this project.

(b) Scope. This SOW covers Phase 2 of an engagement to provide advisory and tactical execution support toward the development of the Company's Big Data Machine Learning Anomaly Detection ("AD") system, as part of a Fraud Management Program enhancement effort. For Phase 2, the Company is looking for assistance in standardizing and automating a suite of anomaly detection analytics to help increase both the effectiveness of the current rule inventory and the efficiency of the fraud alert dispositioning process for transaction and merchant monitoring, and account management. The Company would like the Service Provider to evaluate the current process, introduce leading practices, suggest enhancements, and help build recommendations for an automated solution to support the ultimate goal of a proactive anomaly detection solution for use within the Fraud Management Program. The Service Provider will accomplish the objectives of Phase 2 through the execution of ten agile sprints, each focused on the rapid execution of a series of tasks. Specifically, as part of the Phase 2 process, the Service Provider will help to develop repeatable scripts that can be executed in the analytics environment and allow for the calling of other programmatic routines, if required. As part of the Phase 2 automation assistance, the Service Provider will develop the scripts in small, re-usable blocks, so there is flexibility in sequencing and deploying them if strategic priorities change.

(c) **Standard of Performance.** Service Provider agrees that the Services shall be performed in accordance with the terms of the Agreement. Check the following box if applicable and provide detailed descriptions

- ☐ *Services are subject to Service Level Requirements: Attach Service Level Agreement covering certain remedies upon the failure to meet such Service Level Requirements.*

Check the appropriate box or boxes if the Services fall under any of the following categories:

- ☐ Tax Services (Attachment 1 of the Agreement applies).
- ☐ Accounting Advisory Services (Attachment 2 of the Agreement applies).
- ☐ Transaction Services (Attachment 2 of the Agreement applies).
- ☒ Other Covered Services.

This SOW does not cover audit, attestation or other assurance services or services which would require Service Provider to undertake any compliance obligations, with respect to the financial reporting or controls of the Company or its Affiliates, under the Sarbanes Oxley Act of 2002.

III. SERVICES AND DELIVERABLES

(a) **Services to be provided by Service Provider.** The Services to be provided by the Service Provider are set forth in this SOW. As discussed, Phase 2 support of the Big Data Machine Learning AD system will be executed in ten agile sprints performed over 20 elapsed weeks by the Service Provider, in collaboration with the Company. Each of those agile sprints is described below.

Sprint 1 – Ongoing Implementation of REW & SIFT Queue Alert Prioritization, proposed timing of 3/19/2018 to 3/30/2018

Develop and support testing of microservices to automate incremental data processing and application decision science for alert prioritization within the REW & SIFT queues in the current case management ecosystem.

- Liaise with support central administrators to provide guidance for testing code in development and/or staging environments throughout the sprint
- Develop small, modularized code sets for automated incremental data processing and anomaly detection decision science for alert prioritization
- Develop code for integration with the case management system
- Support the execution of testing agile microservices

Deliverable is a testing summary based on the execution of testing by the Company to help to evaluate packaged code is performing within development environment.

Sprint 2 – Current State Assessment of Transaction, Merchant and Customer Account Compromise Detection, proposed timing of 4/2/2018 to 4/13/2018

Identify current repository of data available for transaction and merchant fraud compromise detection, and high risk account management behavior, and develop a baseline dictionary of rules, logic and red flags that are currently performed and/or assessed by analysts to identify potential fraud risk.

- Study existing documentation on current state detection rules for transaction and merchant compromise, and high risk account behaviors, including data sources, mechanics, and escalation protocols
- Perform interviews with analysts to walk through data preparation and data enrichment process, and identify additional detection logic and criteria used in evaluating and dispositioning alerts
- Perform interviews with system owners to identify additional data repositories and sources available for potential incorporation into analyses
- Develop standardized framework of anomaly detection rules and logic across transaction, merchant, and customer account behavior use case inventory

Deliverable is a current state assessment report, including but not limited to the inventory of current anomaly detection rules, current state process flows, and data lineage and data flow schematics.

Sprint 3 – Effectiveness Evaluation of Transaction Compromise Detection, proposed timing of 4/16/2018 to 4/27/2018

Perform testing of logic and/or red flags that were identified in the current inventory of transaction compromise detection rules as identified in the second sprint for the purposes of quantifying the effectiveness of the rule inventory based on historical customer data.

- Calculate the current effectiveness of each rule in the inventory, potentially including, but not limited to the following:
 - Accuracy (“A”)
 - Misclassification (“E”), also known as “error rate”, equivalent to 1 minus “E”
 - True Positive Rate (“TPR”), also known as “sensitivity” or “recall”
 - False Positive Rate (“FPR”)
 - Average Fraud Loss (\$) per account
 - Average Credit Limit (\$) per account
 - Average Utilization per account
- Calculate potential rule redundancy rates (unique results a rule provides) of current inventory of rules
- Perform rule pruning analysis and optimization to identify recommended parameters of the transaction compromise rule set
- Recommend the final set of rules based on pruning and optimization of rules

Deliverable is a transaction compromise rules effectiveness report, including the effectiveness of each individual rule, documentation of pruning and optimization logic, and potential recommendations to the transaction compromise detection segment based on evaluation of the rules.

Sprint 4 – Machine Learning Enhancements for Transaction Compromise Detection, proposed timing of 4/30/2018 to 5/11/2018

Conduct unsupervised and/or supervised learning techniques to identify additional or enhanced discriminatory features and/or rules for transaction compromise detection

- Identify a historical population of customers and corresponding data based on a sampling strategy that includes the relevant business units and required labels, as agreed upon by Company and Service Provider
- Perform benchmarking of current transaction fraud detection rules to help identify any additional features that could provide additional discriminatory value
- Perform machine learning techniques to potentially identify new or augment existing features that provide additional discriminatory value
- Suggest potential enhancements to current fraudulent transaction detection analytics

Deliverable is the documentation of any additional feature engineering specifications and/or potential rules based on the application of machine learning techniques and/or proprietary information provided by the Service Provider.

Sprint 5 – Effectiveness Evaluation of Merchant Compromise Detection, proposed timing of 5/14/2018 to 5/25/2018

Perform testing of logic and/or red flags that were identified in the current inventory of merchant compromise detection rules as identified in the second sprint for the purposes of quantifying the effectiveness of the rule inventory based on historical customer data. This sprint would include, among other scenarios, the specific evaluation and recommendation for the merchant risk of fraudulent fallback transactions.

- Calculate the current effectiveness of each rule in the inventory, potentially including, but not limited to the following:
 - Accuracy (“A”)
 - Misclassification (“E”), also known as “error rate”, equivalent to 1 minus “E”
 - True Positive Rate (“TPR”), also known as “sensitivity” or “recall”
 - False Positive Rate (“FPR”)
 - Average Fraud Loss (\$) per account
 - Average Credit Limit (\$) per account
 - Average Utilization per account
- Calculate potential rule redundancy rates (unique results a rule provides) of current inventory of rules
- Perform rule pruning analysis and optimization to identify recommended parameters of the merchant compromise rule set
- Recommend the final set of rules based on pruning and optimization of rules

Deliverable is a merchant compromise effectiveness report, including the effectiveness of each individual rule, documentation of pruning and optimization logic, and potential recommendations to the merchant compromise detection segment based on evaluation of the

rules. This sprint would also include specific recommendations to combat merchant fallback transaction fraud risk.

Sprint 6 – Machine Learning Enhancements for Merchant Compromise Detection, proposed timing of 5/28/2018 to 6/8/2018

Conduct unsupervised and/or supervised learning techniques to identify additional or enhanced discriminatory features and/or rules for merchant compromise detection

- Identify a historical population of customers and corresponding data based on a sampling strategy that includes the relevant business units and required labels, as agreed upon by Company and Service Provider
- Perform benchmarking of current merchant detection rules to help identify any additional features that could provide additional discriminatory value
- Perform machine learning techniques to potentially identify new or augment existing features that provide additional discriminatory value
- Suggest potential enhancements to current fraudulent merchant compromise detection analytics

Deliverable is the documentation of any additional feature engineering specifications and/or potential rules based on the application of machine learning techniques and/or proprietary information provided by the Service Provider.

Sprint 7 – Effectiveness Evaluation of Customer Account Management Compromise Detection, proposed timing of 6/11/2018 to 6/22/2018

Perform testing of logic and/or red flags that were identified in the current inventory of high risk customer account management detection rules as identified in the second sprint for the purposes of quantifying the effectiveness of the rule inventory based on historical customer data.

- Calculate the current effectiveness of each rule in the inventory, potentially including, but not limited to the following:
 - Accuracy (“A”)
 - Misclassification (“E”), also known as “error rate”, equivalent to 1 minus “E”
 - True Positive Rate (“TPR”), also known as “sensitivity” or “recall”
 - False Positive Rate (“FPR”)
 - Average Fraud Loss (\$) per account
 - Average Credit Limit (\$) per account
 - Average Utilization per account
- Calculate potential rule redundancy rates (unique results a rule provides) of current inventory of rules
- Perform rule pruning analysis and optimization to identify recommended parameters of the customer account management compromise rule set
- Recommend the final set of rules based on pruning and optimization of rules

Deliverable is a customer account management compromise effectiveness report, including the effectiveness of each individual rule, documentation of pruning and optimization logic, and potential recommendations to the customer account management compromise detection segment based on evaluation of the rules.

Sprint 8 – Machine Learning Enhancements for Customer Account Management Compromise Detection, proposed timing of 6/25/2018 to 7/13/2018

Conduct unsupervised and/or supervised learning techniques to identify additional or enhanced discriminatory features and/or rules for customer account management compromise detection

- Identify a historical population of customers and corresponding data based on a sampling strategy that includes the relevant business units and required labels, as agreed upon by Company and Service Provider
- Perform benchmarking of current anomaly detection rules to help identify any additional features that could provide additional discriminatory value
- Perform several machine learning techniques to potentially identify new or augment existing features that provide additional discriminatory value
- Suggest potential enhancements to current fraudulent transaction detection analytics

Deliverable is the documentation of any additional feature engineering specifications and/or potential rules based on the application of machine learning techniques and/or proprietary information provided by the Service Provider.

Sprint 9 – Tactical Short Term Implementation of Recommendations, proposed timing of 7/9/2018 to 7/20/2018

Develop tactical plan to deploy and test sets of microservices to automate incremental data processing and detection decision science for transaction, merchant, and customer management compromise, including rule fusion, prioritization logic, and potential for promotion to visualization and case management tools; execute short term testing as part of the tactical plan.

- Develop tactical roadmap to assist short term recommendations from anomaly detection enhancements
- Liaise with IT administrators to mitigate challenges in testing code in staging environments throughout the sprint
- Develop small, modularized code sets for automated incremental data processing and anomaly detection decision science
- Test execution of agile microservices

Deliverable is a short term tactical plan for deployment of recommendations, and an inventory of select modularized code and corresponding report based on the testing performed by the Company to evaluate packaged code is performing within development environment.

Sprint 10 – User Acceptance Testing Framework & Governance, proposed timing of 7/23/2018 to 8/3/2018

Develop user acceptance testing approach for suite of anomaly detection rules with supporting documentation, educational / training materials, and test cases; develop long term governance recommendations for continuous improvement.

- Develop user acceptance testing approach based on leading practices, including but not limited to the success criteria to inform a go/no-go decision, sampling

strategy to identify test cases, draft test scripts, supporting documentation, and associated education materials

- Develop long term governance plan for continuous improvement, including RACI matrix and longer term strategic plan

Deliverable is a user acceptance test plan, including but not limited to the success criteria to inform a go/no-go decision, sampling strategy to identify test cases, draft test scripts, supporting documentation, associated education materials, and long term governance plan with RACI matrix of organizational stakeholders.

(b) Personnel.

The Service Provider shall provide a team in accordance with the following criteria: each resource possessing core analytics capabilities, including but not limited to data collection and management, statistical methods, computational methods, artificial intelligence, and fraud business strategy. The anticipated resources are the following

- Frank Badalamenti (Principal, New York, NY)
- Michael Hogan (Managing Director, Atlanta, GA)
- Corey Cederquist (Director, New York, NY)
- Fermin Gonzalez (Manager, Mexico City, MX)
- Zhongqiao Jin (Senior Associate, New York, NY)
- Sumanth Sudheer (Senior Associate, New York, NY)
- Kay Lim (Senior Associate, Chicago, IL)
- Colin McCarthy (Experienced Associate, New York, NY)
- Sasindra Gopalakrishnan (Director, Mumbai, India)
- Shaz Hoda (Manager, Mumbai, India)
- Vidhi Tembhurnikar (Senior Associate, Mumbai, India)
- Jyoti Aurora (Senior Associate, Mumbai, India)
- Pratik Lodha (Experienced Associate, Mumbai, India)

The Service Provider Project Manager is Corey Cederquist.

The Company Project Manager is Thomas Prendergast.

(c) Deliverables. The Services to be provided include the following, and may include unbranded deliverables: Deliverables are to be agreed prior to each of the agile sprints, as proposed in section (a)

(d) Acceptance. Notwithstanding anything to the contrary set forth in this SOW or in the Agreement, it is agreed that, based on the Company's discretion, and mutually agreed upon between the Company and the Service Provider (collectively the "Parties"), the Parties may adjust or extend the specified Completion Date ("CD") for any of the sprints mentioned above via an email transmission sent by one Party to this SOW to the other provided that (1) all other terms of this SOW, including the pricing or fees set forth herein, will remain in full force and effect, (2) the

emails are sent by the then current Project Managers, and (3) no other terms are added or amended by the CD extension.

The invoicing related to this SOW will be milestone based, such that each sprint payment to the Service Provider is contingent on the client's acceptance of the sprint deliverable(s). Company will be provided [five (5)] business days to review draft Deliverables and will (a) accept such or (b) request resolution of defects within such review period. Company may reject Deliverables that are not materially in conformity with the applicable written description as set forth in this SOW. If Company rejects a Deliverable, Company will provide prompt written notice with a complete description of the reasons of such rejection to Service Provider. If no notice and/or reasons for rejection is provided within [five (5)] business days following Service Provider's submission of the Deliverable, the Deliverable is deemed accepted and Service Provider is entitled to rely upon the Deliverable as complete for the purpose of the Services. Changes related to accepted Deliverables are handled via mutually acceptable change orders. For Deliverables that require resolution of defects, Service Provider will resubmit the corrected Deliverable for Company's review and the review period will start over.

(e) Company's Responsibilities.

- Company will provide a lead project manager or key contact who will assist Service Provider when it is engaging with Company personnel, in planning and coordinating meetings, assigning Company resources, resolution of aged or outstanding requests, and otherwise administering day-to-day activities, as needed.
- Company should provide Service Provider timely access to:
 - Business requirements and any other supporting documentation describing existing Anomaly Detection rules and processes
 - Management, Operations, and Technology personnel with familiarity with the existing Anomaly Detection rules and processes
 - Relevant customer, account, transaction, and non-monetary event data and associated documentation
 - Access to the big data analytics environment and relevant scripting, analytics, testing, and visualization software applications necessary to complete the tasks under this statement of work
 - Access to Company issued workstations and/or laptops allowing Service Provider to access the relevant systems throughout the engagement performance period
- Electronic and paper documents requested for Service Provider's analysis will be provided by Company within a reasonable timeframe. Modifications or delays in providing documentation and access to key information and systems may impact project timeline or the scheduling of each of the sprints.
- Data and information provided by Company for Service Provider's analysis will reside within Company's systems and IT infrastructure, and will be accessed by the Service Provider through

Company-issued workstations or laptops. Service provider will be restricted from downloading or moving data from the Company network environment onto Company issued workstation or laptop hard drives.

- Data elements constituting PII that appear within data made available to Service Provider will be masked or tokenized such that their contents will not be visible to Service Provider resources in their native form.

(f) **Timing.** The timing of the services to be provided hereunder is as follows:

Project Start Date:	3/19/2018
Estimated Project Completion Date:	8/3/2018

(g) **Use of Services and Deliverables:** The Services and Deliverables will be used in the manner implied by the description of the Services and Deliverables. The Company acknowledges that the Service Provider retains all worldwide right, title and interest in and to its Service Provider Materials, including all Intellectual Property Rights developed while providing the Services. The Service Provider provides the Company non-exclusive rights for non-commercial use.

IV. PAYMENT; EXPENSES; AND INVOICES

A Purchase Order, required solely for Company billing purposes, shall be issued by Company prior to any work being initiated.

For all Services except where such Services are “Fixed Price” agreements or other non-rate/hour arrangements (provided, however, Company reserves the right to receive a cost breakdown for these categories), a budget is attached detailing the cost estimate by work segment broken down by person, hours and hourly rate, which will then serve as the budget for the assignment and used to compare to the ongoing review of the progress of this project. For projects greater than \$250,000, billing status reviews are required upon the following milestones being obtained:

- i) 33% of budget fees being actually incurred
- ii) 66% of budget fees being actually incurred
- iii) At any time the total fees are projected to exceed the original estimate by 10%

(a) **Fees.** The Service Provider will perform Services and provide Deliverables under this Work Order on a fixed fee basis. The total amount of Project Fees (excluding expenses) is comprised of a fixed fee not to exceed **Eight Hundred and Seven Thousand, Five Hundred (\$807, 500) dollars**. Each sprint will be invoiced as an equal component of the total fixed fee, not to exceed **Eighty Thousand, Seven Hundred Fifty (\$80,750) dollars** upon acceptance of sprint Deliverables.

(b) **Supporting Data.** List supporting data required to be submitted with each invoice in addition to requirements of Section 2.5 of the Agreement.

(c) **Expenses.** List any expenses not included in Fees to the extent permitted by Section 2.7 of the Agreement.

Travel and living expenses are additional and are not reflected in the Estimated Total Fees set forth above. Travel and living expenses will be no more than 12 percent of the fixed fee, or **Ninety Six Thousand, Nine Hundred (\$96,900) dollars**. Any increase in the Estimated Total Expenses set forth herein must be mutually agreed upon in writing between the Company and the Service Provider prior to being incurred by Service Provider. Absent such prior written agreement, Service Provider relieves the Company of any obligations or claims for amounts over the Estimated Total Expenses stated herein. All expenses will be billed as incurred without markup. In order to be reimbursed, all such expenses will be incurred in accordance with the Company's expense policies.

If travel and living expenses are authorized, specify the policy applicable:

☒ RFIH's Travel and Expenses Policy

☐ Service Provider's T&L Policy

IV. MISCELLANEOUS:

(a) **Change Requests.** Any change to the Services, Deliverables, method or timing of performance of the Services or any action that shall have an impact on the performance or delivery of the Services or the Deliverables or the total cost to the Company of the Services, shall be made in writing in accordance with Section 5.7 of the Agreement and result in submission of a Change Control Form (Attachment 6 to the Agreement).

(b) **Document Retention.** Service Provider shall retain documents relating to this SOW in accordance with its internal document retention policy, which provides for a minimum retention of seven (7) years, or for such longer period as may be required (i) by any applicable government agency, law, rule or regulation, or, (ii) in connection with any ongoing or, upon written notice from Company, threatened litigation, suit or proceeding relating to the Services. All document retention requirements are subject to the confidentiality provisions of Section 9 of the Agreement, including Section 9.7 with respect to return or destruction of Company Confidential Information.

(c) **Service Provider Materials.** To the extent Service Provider Materials are incorporated in or necessary for the implementation of the Deliverables, Company's non-exclusive license therein for its own internal use and only for purposes for which they are delivered and to the extent that they form part of the Deliverables shall extend to use by the following authorized users ("Authorized Users") and, upon written agreement by Service Provider not to be

unreasonably withheld, to such replacements for them as Company may from time to time request for purposes of Sections 8.1 and 10.1 of the Agreement:

The Authorized Users are service providers to Company and Company Affiliates and shall use the Deliverables solely for the benefit of Company and Company Affiliates.

(d) Third Party Materials. If any Third Party Material is included in a Deliverable and is reasonably required to enable Company or Company Affiliates to use and support the Deliverables in a cost effective manner, specify the commercially available license thereof and if such license is not available, specify any limitations on the license thereof to be provided by Service Provider as contemplated by Section 8.2 of the Agreement:

(e) Subcontractors. List any subcontractors (other the PricewaterhouseCoopers Firms) that are permitted to provide services with respect to this SOW.

(f) Score Cards. If Service Provider is required to provide data and information scorecards, specify the scorecards to be used by Service Provider and each scorecard format.



(g) Confidentiality and Material Nonpublic Information. Certain Company Confidential Information may include material nonpublic information subject to Section 10(b) of the Securities Exchange Act of 1934 and Rules 10b-5 and 10b5-1 promulgated thereunder. Nothing in this SOW shall modify the obligations and responsibilities of Service Provider, its subcontractors and Administrative Vendors with respect to any such material nonpublic information under law or the Agreement, provided, however, that if the following box is checked the parties will take the additional steps specified below.

- ☐ Company will provide access to Service Provider to Company Confidential Information that Company designates as material nonpublic information necessary to perform the Services only through Company systems and hardware and, accordingly, Administrative Vendors are not to have access to such information ("designated restricted information"). Accordingly Service Provider will not maintain such designated restricted information on its systems and it will, therefore, not be accessible to Administrative Vendors. <If this box is checked the parties need to discuss and agree to the scope of the Company Confidential Information to be shared.>

(h) Representation, Warranty and Covenant of Service Provider. Service Provider hereby represents, warrants and covenants that it is under no obligation or restriction, nor will it assume any such obligation or restriction, that does or would in any way interfere or conflict with, or would prevent, limit, or impair in any way the performance by Service Provider of any of the terms of this SOW or of the Services and/or Deliverables.

IN WITNESS WHEREOF, the parties referenced above have caused this SOW to be executed by their authorized representatives.

By:

Service Provider			
Signature	Printed Name	Title	Date
	Frank Badalamenti	Principal Client Service	3/21/2018
Company entity entering into this SOW			
Authorized Signature	Printed Name	Title	Date
 <small>Kevin Egan (Mar 21, 2018)</small>	Kevin Egan	SVP, CPO	Mar 21, 2018