UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 8-K

CURRENT REPORT
Pursuant to Section 13 or 15(d)
of the
Securities Exchange Act of 1934

Date of Report (date of earliest event reported): June 15, 2016

CUSTOMERS BANCORP, INC.

(Exact Name of Registrant as specified in its charter)

Pennsylvania	**001-35542**	**27-2290659**
(State or other jurisdiction of incorporation)	(Commission File Number)	(I.R.S. Employer Identification No.)

1015 Penn Avenue
Suite 103
Wyomissing PA 19610
(Address of principal executive offices, including zip code)

(610) 933-2000
(Registrant's telephone number, including area code)

None
(Former name or former address, if changed since last report)

Check the appropriate box below if the Form 8-K filing is intended to simultaneously satisfy the filing obligations of the registrant under any of the following provisions (see General Instructions A.2. below):

☐ Written communications pursuant to Rule 425 under the Securities Act (17 CFR 230.425)

☐ Soliciting material pursuant to Rule 14a-12 under the Exchange Act (17 CFR 240.14a-12)

☐ Pre-commencement communications pursuant to Rule 14d-2(b) under the Exchange Act (17 CFR 240.14d-2(b))

☐ Pre-commencement communications pursuant to Rule 13e-4(c) under the Exchange Act (17 CFR 240.13e-4(c))

Item 1.01 Entry into a Material Definitive Agreement.

The information included in Item 2.01 below with respect to the Transition Services Agreement is incorporated by reference into this Item 1.01.

Item 2.01 Completion of Acquisition or Disposition of Assets.

On June 15, 2016, Customers Bancorp, Inc. ("Customers Bancorp") and its subsidiary, Customers Bank ("Customers Bank," and, together with Customers Bancorp, "Customers") completed the previously announced acquisition by Customers of substantially all of the assets and the assumption of certain liabilities of the One Account Student Checking and Refund Management Disbursement business (the "Disbursement business") from Higher One, Inc. and Higher One Holdings, Inc. (together, "Higher One"). The acquisition was completed pursuant to the terms of an Asset Purchase Agreement (the "Purchase Agreement") dated as of December 15, 2015 between Customers and Higher One.

The transaction contemplates aggregate guaranteed payments to Higher One of $42 million. The aggregate purchase price payable by Customers is $37 million in cash, with the payments to be made in three installments: (i) $17 million in cash upon the closing of the acquisition, (ii) $10 million upon the first anniversary of the closing and (iii) $10 million upon the second anniversary of the closing. In addition, concurrently with the closing, the parties have entered into a Transition Services Agreement pursuant to which Higher One will provide certain transition services to Customers through June 30, 2017. As consideration for these services, Customers will pay Higher One an additional $5 million in cash. Customers also will be required to make additional payments to Higher One if, during the three years following the closing, revenues from the Disbursements business exceed $75 million in a year. The possible payment will be equal to 35% of the amount the Disbursements business related revenue exceeds $75 million in each year.

Item 7.01 Regulation FD Disclosure.

On June 16, 2016, Customers issued a press release relating to the closing of the transaction with Higher One described above in Item 2.01, attached hereto as Exhibit 99.1, which is incorporated in this Item 7.01 by reference.

The information in this Item 7.01, including Exhibit 99.1 attached hereto and incorporated by reference into this Item 7.01, shall not be deemed "filed" for purposes of Section 18 of the Securities Exchange Act of 1934, as amended, or otherwise subject to the liabilities under that Section. Furthermore, such information, including Exhibit 99.1 attached hereto, shall not be deemed incorporated by reference into any of Customers' reports or filings with the Securities and Exchange Commission, whether made before or after the date hereof, except as expressly set forth by specific reference in such report or filing. The information in this Item 7.01, including Exhibit 99.1 attached hereto, shall not be deemed an admission as to the materiality of any information in this Item 7.01 that is required to be disclosed solely to satisfy the requirements of Regulation FD.

Item 9.01 Financial Statements and Exhibits

(a) - (b) By letter dated May 19, 2016, in response to a request submitted by Customers, the staff of the Securities and Exchange Commission agreed that it would not object to Customers' request to present abbreviated statements of assets and liabilities assumed and revenues and direct expenses relating to the Disbursement business. Customers will provide this required financial information with respect to the Disbursement business acquisition described in Item 2.01 above by amendment to this Current Report on Form 8-K not later than 71 days after the date on which this Current Report on Form 8-K is required to be filed pursuant to Item 2.01.

(d) Exhibits.

Exhibit No.	Description
2.1	Asset Purchase Agreement dated as of December 15, 2015 by and among Customers Bancorp, Customers Bank, Higher One, Inc. and Higher One Holdings, Inc., incorporated by reference to Exhibit 2.3 to the Customers Bancorp Form 10-K filed with the SEC on February 26, 2016.
10.1	Transition Services Agreement dated as of June 15, 2016 by and among Customers Bancorp, Customers Bank, Higher One, Inc. and Higher One Holdings, Inc.
99.1	Press Release dated June 16, 2016.

SIGNATURE

Pursuant to the requirements of the Securities Exchange Act of 1934, the Registrant has duly caused this report to be signed on its behalf by the undersigned hereunto duly authorized.

CUSTOMERS BANCORP, INC.

By: /s/ Robert E. Wahlman
Name: Robert E. Wahlman
Title: Executive Vice President and Chief Financial Officer

Date: June 16, 2016

EXHIBIT INDEX

Exhibit No.	Description
2.1	Asset Purchase Agreement dated as of December 15, 2015 by and among Customers Bancorp, Customers Bank, Higher One, Inc. and Higher One Holdings, Inc., incorporated by reference to Exhibit 2.3 to the Customers Bancorp Form 10-K filed with the SEC on February 26, 2016.
10.1	Transition Services Agreement dated as of June 15, 2016 by and among Customers Bancorp, Customers Bank, Higher One, Inc. and Higher One Holdings, Inc.
99.1	Press Release dated June 16, 2016.

Exhibit 10.1
Execution Copy

TRANSITION SERVICES AGREEMENT

This TRANSITION SERVICES AGREEMENT (this " Agreement ") is made as of June !5, 2016 between Higher One, Inc., a Delaware corporation (" Seller ") and Customers Bank, a bank chartered under the laws of the Commonwealth of Pennsylvania (" Buyer "). Seller and Buyer are referred to herein collectively as the " Parties " and individually as a " Party ."

INTRODUCTION

WHEREAS, Seller and Buyer have entered into an Asset Purchase Agreement, dated as of December 15, 2015 (the " Purchase Agreement ") (capitalized terms not defined in this Agreement shall have the meanings indicated in the Purchase Agreement);

WHEREAS, under the Purchase Agreement, Buyer has agreed to purchase from Seller certain assets related to Seller's business of disbursing refunds for its higher education institutional clients and servicing student-oriented checking accounts for the students of those clients (the " Business "), and the Purchase Agreement contemplates that the Parties shall execute and deliver this Agreement at the Closing; and

WHEREAS, Buyer and Seller desire that, after the Closing, Seller and/or certain of its Affiliates shall provide to Buyer, and Buyer and/or certain of its Affiliates shall provide to Seller, certain services on a transitional basis, as set forth herein.

NOW, THEREFORE, in consideration of the promises and covenants set forth herein and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the Parties hereby agree as follows:

ARTICLE I
TRANSITION SERVICES

Section 1.1 Transition Services .

(a) Scope and Duration of Seller Transition Services . Seller, itself and/or by and through its Affiliates, and its and their respective employees, agents or contractors, shall provide or cause to be provided to Buyer, solely for the benefit of Buyer, those services set forth on Annex A hereto, as it may be amended from time to time by mutual written agreement of the Parties (collectively, the " Seller Transition Services ") until the earlier of (i) expiration of the service period applicable to such Transition Services as set forth with respect to each applicable Seller Transition Service on Annex A hereto, or (ii) expiration of the Term (as defined below). Seller shall not be obligated to provide any services other than the Seller Transition Services expressly provided herein. Seller shall not be required to perform Seller Transition Services hereunder in any manner that violates any applicable law or regulation. It is acknowledged by Seller that the objective of this Agreement is to obligate Seller to provide, throughout the Term, any and all services and functions that Buyer is unable to perform with respect to the assets purchased and employees hired pursuant to the Purchase Agreement in order for the Business to perform at a comparable level of operation and functionality achieved during the 180 days prior to the closing under the Purchase Agreement. In addition, Seller shall provide consulting services to Buyer related to the One Account structure and operation, marketing and managing relationships with colleges and universities, regulatory compliance matters, Department of Education introductions and relationship advice, product pricing matters, and contractual matters (with vendors as well as colleges and universities).

(b) Scope and Duration of Buyer Transition Services . Buyer, itself and/or by and through its Affiliates, and its and their respective employees, agents or contractors, shall provide or cause to be provided to Seller, solely for the benefit of Seller, those services set forth on Annex B hereto, as it may be amended from time to time by mutual written agreement of the Parties (collectively, the " Buyer Transition Services ", and together with the Seller Transition Services, the " Transition Services ") until the earlier of (i) expiration of the service period applicable to such Buyer Transition Services as set forth with respect to each applicable Buyer Transition Service on Annex B hereto, or (ii) expiration of the Term (as defined below).

(c) Modified Transition Services . Any modifications to the Transition Services shall be subject to mutual agreement pursuant to ARTICLE IX hereof.

(d) Subcontractors . Upon prior consent of the other Party, which consent shall not be unreasonably withheld, conditioned or delayed, Seller or Buyer may subcontract with an unaffiliated third party (a " Subcontractor ") to provide any Transition Services; provided that no notice shall be required with respect to the continued use of subcontractors in the manner utilized by Seller in connection with the Business immediately prior to the Closing, or with respect to changes in subcontractors which are consistent with Seller's operation of the Business immediately prior to the Closing. Notwithstanding any subcontracting of Seller's or Buyer's obligations under this Agreement, each Party shall, for the term of this Agreement, remain primarily liable for the delivery and performance of the Transition Services.

Section 1.2 Service Coordinators and Issue Resolution .

(a) Seller and Buyer each hereby appoint as service coordinators their respective employees identified on Schedule 1.2 hereto (each, a " Service Coordinator ") to be the primary point of contact between Seller and Buyer with respect to the Transition Services, including, and subject to the terms of this Schedule 1.2 , with respect to disputes between the Parties arising out of or relating to this Agreement or the provision of Transition Services hereunder. Each Party shall have the right, upon reasonable advance written notice to the other Party, to replace its Service Coordinator with an employee or officer of such Party with comparable knowledge, expertise and decision-making authority.

(b) In the event the Service Coordinators fail to resolve any dispute arising between the Parties in connection with the Transition Services within a reasonable time of receiving notice of such dispute from a Party, and in any event within ten (10) Business Days of such notification, then Buyer shall designate an officer or officers holding the office of Senior Vice President (or equivalent office) or above (such officers, the " Senior Officers ") and such Senior Officers shall attempt in good faith to conclusively resolve any such dispute (i) with the members of an operating committee designated by Seller, and (ii) in the event the Senior Officers and operating committee fail to resolve the dispute, an executive committee shall be designated by Seller and Buyer. If the Senior Officers and the operating and executive committees designated by Seller and Buyer cannot resolve such dispute within a reasonable period of time, and in any event within twenty (20) Business Days of the referral of such dispute to them, either Party may submit the dispute to litigation as provided for in Section 10.8.

(c) Any dispute arising out of or relating to this Agreement shall be submitted for resolution pursuant to this Section 1.2 before any Party may commence any legal proceeding in connection therewith. A Party's failure to comply with the preceding sentence shall constitute cause for the dismissal without prejudice of any such legal proceeding. This Section 1.2(c) is without prejudice to either Party's right to seek interim relief against the other Party (such as an injunction) to protect its rights and interests, or to enforce the obligations of the other Party and the parties need not negotiate disputes with respect to equitable remedies prior to seeking relief from a court of competent jurisdiction.

Section 1.3 Migration Plan .

(a) On or prior to the date hereof, the Parties shall have negotiated and materially finalized a plan to transition from the performance of the Seller Transition Services by Seller and its Affiliates to the performance of such services by Buyer, including moving the information technology systems and data used in the Business from Seller's infrastructure to Buyer's or its designee's infrastructure (" Migration ") (such plan, the " Migration Plan "). The Migration Plan shall include a governance and arbitration process, in which both Parties shall agree to participate, which shall be subject to the change control process set forth in ARTICLE IX.

(b) Buyer shall be responsible for the Migration, including the construction and deployment of any systems or physical space required for the Migration. Seller shall use commercially reasonable efforts to assist Buyer in completing the Migration. Buyer shall be responsible for all fees and expenses incurred by Buyer and reasonable out-of-pocket third party costs of Seller incurred in the course of providing any assistance with the Migration requested by Buyer.

(c) The Parties acknowledge that the Migration Plan is a document that may change, and any such material changes will be subject to the change control process set forth in ARTICLE IX. Each Party shall use its commercially reasonable efforts to perform its obligations under the Migration Plan according to the schedule set forth in the Migration Plan, and each Party shall use sufficient and qualified resources and personnel to implement the Migration Plan, taking into account the need to reasonably manage the cost of such transition and minimize the disruption to the ongoing business activities of the Parties.

Section 1.4 Additional Transition Services . If requested by either Party, the other Party shall provide services in addition to the Transition Services (" Additional Transition Services "), as may be agreed pursuant to the Change Control process set forth in ARTICLE IX. The scope of any such Additional Transition Services, as well as the prices and other terms applicable to such additional services, shall be as mutually agreed by Buyer and Seller, as further contemplated by ARTICLE IX.

Section 1.5 Standard of Performance . Each Party shall use commercially reasonable efforts to perform or procure the provision of the Transition Services for the other Party to standards of performance comparable in all material respects to which such Transition Services were performed by Seller or its Affiliates in connection with the Business immediately prior to Closing; provided that Seller shall not be responsible for the performance of any product programs or features developed and/or implemented by Buyer after the Closing Date.

Section 1.6 Access . Each Party shall use good faith efforts to provide the other Party with access to information and computer systems, facilities, networks (including voice or data networks) or software to the extent reasonably necessary to enable the provision of Transition Services contemplated by this Agreement, subject to Section 7 hereof. The Party requesting access shall give the other Party reasonable prior written notice and justification of the need for such access.

Section 1.7 Independent Contractor . For all purposes hereof, each Party shall at all times act as an independent contractor and shall have no authority to represent the other Party in any way or otherwise be deemed an agent, lawyer, employee, representative, joint venturer or fiduciary of such other Party nor shall this Agreement or the transactions contemplated hereby be deemed to create any joint venture between the Parties. Each Party shall not declare or represent to any third party that such Party shall have any power or authority to negotiate or conclude any agreement, or to make any representation or to give any undertaking on behalf of the other Party in any way whatsoever.

ARTICLE II
SERVICE FEES AND EXPENSES

Section 2.1 Service Fees .

(a) Subject to adjustment in accordance with this Section 2.1, Buyer shall pay a fee for the Seller Transition Services and Additional Transition Services it receives during the Term as follows (collectively, the " Buyer Service Fees "):

(i) with respect to the Seller Transition Services, $5,000,000, payable in twelve (12) equal monthly instalments of $416,666.67, each of which shall be due and payable on the fifteenth (15 th) day of each month; and

(ii) with respect to any Additional Transition Services provided by Seller, on the timetable and in the amount agreed by the Parties and set out in the executed amendment to this Agreement under which such Additional Transition Services are provided as contemplated in Article IX.

(b) Subject to adjustment in accordance with this Section 2.1, Seller shall pay a fee (the " Seller Service Fee ", and together with the Buyer Service Fees, the " Service Fees ") for the Additional Transition Services it receives from Buyer during the Term on the timetable and in the amount agreed by the Parties and set out in the amendment to this Agreement under which such Additional Transition Services are provided, which shall be entered into in accordance with ARTICLE IX.

(c) The Service Fees are exclusive of any sales tax, transfer tax, value-added tax, goods and services tax or similar tax (" Taxes "). Any Taxes (but excluding any Tax based upon net income) payable with respect to the Service Fees shall be invoiced by the Party providing such services (the " Providing Party ") and paid to such Party by the other Party (the " Receiving Party ") within thirty (30) days of receipt of such invoice. The Party providing the service shall be responsible for remitting any such Taxes to the appropriate taxing authority.

(d) If the cost to either Party of providing a Transition Service increases as a result of actions taken outside the scope of this Agreement by or at the request of the Receiving Party or as a result of any change in applicable law or regulation or action of any Government Entity (collectively, " Imposed Changes "), then the resulting increase in costs will be passed through to the Receiving Party by means of an increase in the relevant Service Fees in the amount of such actual increase in the cost of the provision of such Transition Services, plus any direct, out of pocket, up-front costs of modifying the Transition Services as a result of such Imposed Changes, provided , however , that (i) in no event shall the Party providing the service be obligated to perform any service hereunder other than in accordance with applicable law and regulation, and (ii) the Party providing the service shall not be obligated to perform such Service unless the Receiving Party agrees to pay such costs of modifying the Transition Services to comply with such Imposed Changes and such increased Service Fees.

Section 2.2 Expenses . The Party receiving services shall be responsible for any direct third-party out-of-pocket costs or expenses incurred by the Party providing the services and disclosed in writing to the other Party prior to the date of this Agreement in connection with providing the Transition Services.

Section 2.3 Records . Each Party shall maintain records of all receipts, invoices, reports and other documents relating to the Transition Services rendered hereunder in accordance with applicable law and regulation and its standard accounting practices and procedures, which practices and procedures are employed by such Party in its provision of services for itself and its Affiliates.

ARTICLE III
PAYMENT

Section 3.1 Invoicing and Payment . For the Transition Services described on Annex A on the date hereof, Buyer shall pay the net monthly fees set forth in Section 2.1 on or before each due date for such fee, without an invoice from Seller. For any Additional Transition Services, the net monthly fee shall be adjusted and paid by Buyer in accordance with the executed amendment to this Agreement under which such Additional Transition Services are provided. For any third-party expenses incurred by either Party in connection with providing the Transition Services and payable by Receiving Party in accordance with Section 2.2 hereof, Providing Party shall invoice Receiving Party, and Receiving Party shall remit payment to Providing Party for all such invoiced expenses within thirty (30) calendar days after receipt of each such invoice. Any undisputed amount unpaid after the expiration of thirty (30) calendar days after the due date shall bear interest equal to one-half percent (0.5%) per month of the overdue amount. Each invoice for expenses shall set forth in reasonable detail, for the period covered by such invoice, the source of the expenses incurred.

Section 3.2 No Set Off . Buyer shall not have the right to set off any claims of damages, under this Agreement, the Purchase Agreement or any other arrangement between Buyer and Seller, against payments owed under this Agreement with the exception of costs incurred under Section 2.2.

ARTICLE IV
TRANSITION

Section 4.1 Return of Materials . Promptly at the end of the service period with respect to a Transition Service, at the end of the Term or upon termination of this Agreement in accordance with ARTICLE VI, as the case may be, the Receiving Party shall, at the other party's expense and written direction, return or destroy and certify the return or destruction of, any and all of the other Party's books, records, files, databases, intellectual property (including embodiments thereof), Confidential Information (as defined below) or information related to customer data in the possession, custody or control of the Receiving Party (the " Materials "); provided that a Receiving Party shall be permitted to retain one copy of the Materials solely as required in order to comply with applicable law and regulation, or for audit, compliance or regulatory purposes to the extent permitted by applicable law and regulation; and provided , further , that a Receiving Party shall not be obligated to destroy any Materials if such destruction would, in the reasonable opinion of counsel to such Receiving Party, constitute a violation of applicable law or regulation.

ARTICLE V
INTELLECTUAL PROPERTY

Section 5.1 Title to Intellectual Property .

(a) Each of the Parties agrees that any intellectual property of the other Party made available to it in connection with the Transition Services, and any derivative works, additions, modifications or enhancements thereof created by the other Party pursuant to this Agreement, are and shall remain the sole property of the other Party, and such Party hereby irrevocably assigns any and all right, title and interest therein to such other Party. Each Party agrees not to use, and to cause its Affiliates not to use, intellectual property of the other Party for any purpose other than in connection with the performance of the Transition Services during the Term.

(b) Each Party acknowledges that the other Party may be providing services similar to the Transition Services to its own businesses and/or to other third parties during the Term, without restriction hereunder.

Section 5.2 Use of Trademarks . Except as expressly set forth in the Purchase Agreement, neither Party shall use the other Party's trademarks, service marks, trade names, domain names or other source identifiers without such Party's prior written consent.

Section 5.3 Software Licenses and Data Subscriptions . Except as provided in the Purchase Agreement or as set forth on Schedule 5.3 hereto, Seller and its Affiliates shall not be required to transfer or assign to Buyer any third-party software licenses, data subscriptions or any software or hardware owned by Seller or any of its Affiliates in connection with the provision of the Seller Transition Services.

ARTICLE VI
TERM AND TERMINATION

Section 6.1 Term . The term of this Agreement (the " Term ") shall commence on the Closing and continue from the Closing Date until June 30, 2017 (the " Termination Date "); provided that the Term of any individual Transition Service may be for a shorter period of time as may be set forth on Annex A hereto or as mutually agreed by the parties in writing.

Section 6.2 Termination for Cause . Either Party (the " Terminating Party ") may terminate this Agreement with immediate effect by notice in writing to the other Party (the " Other Party ") on or at any time after the occurrence of any of the following events:

(a) the Other Party is in default of any of its material obligations under this Agreement and (if the breach is capable of remedy) has failed to remedy the breach within thirty (30) days after receipt of notice in writing from the Terminating Party giving particulars of the breach;

(b) the Other Party shall commence a voluntary case or other proceeding seeking liquidation, reorganization or other relief with respect to itself or its debts under any bankruptcy, insolvency or other similar law now or hereafter in effect or seeking the appointment of a trustee, receiver, liquidator, custodian or other similar official for it or any substantial part of its property, or shall consent to any such relief or to the appointment of or taking possession by any such official in an involuntary case or other proceeding commenced against it, or shall make a general assignment for the benefit of creditors, or shall fail generally to pay its debts as they become due, or shall take any corporate action to authorize any of the foregoing;

(c) an involuntary case or other proceeding shall be commenced against the Other Party seeking liquidation, reorganization or other relief with respect to it or its debts under any bankruptcy, insolvency or other similar law now or hereafter in effect or seeking the appointment of a trustee, receiver, liquidator, custodian or other similar official for it or any substantial part of its property, and such involuntary case or other proceeding shall remain undismissed and unstayed for a period of sixty (60) days.

Section 6.3 Survival . Section 2.2 (Expenses), Section 2.3 (Records), ARTICLE III (Payments)(to the extent such fees accrued prior to termination, cancellation or expiration), Section 4.1 (Return of Materials), Section 5.1 (Intellectual Property), this Section 6.3 (Survival), Section 7.1 (Confidentiality), Section 8.2 (Limitations of Liability) and Article X (Miscellaneous) shall survive any termination or expiration of this Agreement.

ARTICLE VII
CONFIDENTIALITY

Section 7.1 Confidentiality .

(a) Each Party acknowledges that, in connection with the performance by a Party of its obligations hereunder, such Party may be provided with information about confidential and proprietary information of the other Party and third parties with which the other Party conducts business. The confidential information of such other Party and third parties is defined below and is collectively referred to as " Confidential Information ." In recognition of the foregoing, each Party covenants and agrees:

(i) that it will keep and maintain all Confidential Information in confidence, using such degree of care as is appropriate to avoid unauthorized use or disclosure;

(ii) that it will not, directly or indirectly, disclose any Confidential Information to anyone outside of the other Party, except with the other Party's prior written consent or as may be permitted under this Article VII;

(iii) that such Party will not make use of any Confidential Information for its own purpose or the benefit of anyone or any other entity other than the other Party, provided that Buyer can make use of any Confidential Information related to the Business in its operation of the Business; and

(iv) that such Party will take no action with respect to the Confidential Information that is inconsistent with its confidential and proprietary nature.

(b) Each Party shall be permitted to disclose the Confidential Information only as follows:

(i) to its employees, agents, auditors, counsel, directors, officers and contractors (" Related Parties ") and Subcontractors, having a need to know such information in connection with the performance of the Transition Services. Each Party shall be responsible for all its Related Parties and Subcontractors' compliance with the terms of this Agreement; and

(ii) if disclosure is required by applicable law or regulation, provided that a Party shall notify the other Party in writing as soon as reasonably practicable in advance of such disclosure, and provide the other Party with copies of any related information so that the other Party may take appropriate action to protect the Confidential Information.

(c) For purposes of this Agreement, Confidential Information shall include all business information of the other Party, including the following:

(i) information relating to the other Party's planned or existing computer systems and systems architecture, including computer hardware, computer software, source code, object code, documentation, methods of processing and operational methods;

(ii) sales, profits, organizational restructuring, new business initiatives and financial information;

(iii) information that describes the other Party's products, including product designs, and how such products are administered and managed;

(iv) information that describes the other Party's product strategies, tax interpretations, tax positions and treatment of any item; and

(v) confidential information and software of, and contracts with (and any information related thereto), third parties with which the other Party conducts business.

(d) Notwithstanding the foregoing, Confidential Information shall not include information that (i) is or becomes generally available to the public other than as a result of a disclosure directly or indirectly by a Party or its Related Parties or Subcontractors, (ii) was available to a Party on a non-confidential basis prior to its disclosure to such Party by the other Party or the other Party's Related Parties or Subcontractors or (iii) is or becomes available on a non-confidential basis to a Party from a Person other than the other Party, provided that such Person was not known to the receiving Party to be bound by any agreement with the disclosing Party to keep such information confidential or to be otherwise prohibited from transmitting the information. Each Party acknowledges that the disclosure of Confidential Information may cause irreparable injury and damages, that money damages would not be a sufficient remedy for any actual or threatened disclosure and that a Party shall (without proof of actual damages) be entitled to equitable relief, including an injunction and specific performance, as a remedy if the other Party breaches or threatens to disclose Confidential Information in violation hereof. A breaching Party shall not object to the entry of an injunction or other equitable relief against such Party on the basis that an adequate remedy is available at law or lack of irreparable harm. Without limitation of the foregoing, each Party shall advise the other Party promptly in the event that it learns or has reason to believe that any person or entity, which has had access to Confidential Information, has violated or intends to violate the terms of this Agreement. This provision shall not in any way limit such other remedies as may be available to either Party at law or in equity.

(e) With regard to any Confidential Information of the type specified in Section 7.1(c)(v), each Party agrees to execute any commercially reasonable document or take any commercially reasonable action required by any vendor or licensor of software to the other Party in order to access and use such vendor's software in connection with such vendor's contracts with the other Party.

Section 7.2 Systems Security . When Buyer is given access to Seller's computer system(s), facilities, networks (including voice or data networks) or software (" Systems ") in connection with the Seller Transition Services or Migration Plan, Buyer shall comply with all lawful security regulations reasonably required by Seller from time to time " Security Regulations "), including without limitation the requirements set forth on Annex C hereto, and will not tamper with, compromise or circumvent any security or audit measures employed by Seller. Buyer's Related Parties may be required to execute a separate system access agreement for individuals who are to have access to Seller's Systems. Buyer shall ensure that only those users who are specifically authorized to gain access to Seller's Systems as necessary to utilize the Seller Transition Services or assist with the Migration gain such access and that such users do not engage in unauthorized destruction, alteration or loss of information contained therein. If at any time a Party determines that any personnel of Buyer has sought to circumvent or has circumvented Seller's Security Regulations or other security or audit measures or that an unauthorized person has accessed or may access Seller's Systems or a person has engaged in activities that may lead to the unauthorized access, destruction or alteration or loss of data, information or software, to the extent within Buyer's control, Buyer or Seller, as appropriate, shall immediately terminate any such person's access to Seller's Systems and immediately notify Seller. In addition, a material failure to comply with the Security Regulations shall be a breach of this Agreement; in which case, Seller shall notify Buyer and both Parties shall work together to rectify said breach. If the breach is not rectified within ten (10) days of its occurrence, the Service Coordinators of both Parties shall be advised in writing of the breach and work together to rectify said breach. If the breach has not been rectified within ten (10) days from such notice to the Service Coordinators, Seller shall be entitled to immediately terminate the Seller Transition Services to which the breach relates until such time as the breach is remedied.

Section 7.3 Insurance . To the extent it has not already done so, Buyer and Seller each shall obtain, within ninety (90) days of the date hereof, from a financially sound and reputable insurer, cyber security and data breach liability insurance in an amount equal to at least $10,000,000 on terms and conditions reasonably satisfactory to the other Party, and will cause such insurance policy to be maintained until the Termination Date.

ARTICLE VIII
REPRESENTATIONS AND WARRANTIES

Section 8.1 Representations and Warranties .

(a) Each Party represents and warrants that, on the Closing Date, it has the authority to enter into this Agreement and its performance under this Agreement will not conflict with any other obligation or agreement of such Party.

(b) Except as expressly provided in this Agreement, no representation, warranty or condition, express or implied, statutory or otherwise, as to condition, quality, satisfactory quality, performance or fitness for purpose or otherwise is given by either Seller or Buyer and all such representations, warranties and conditions are excluded except to the extent that their exclusion is prohibited by applicable law.

Section 8.2 Limitations of Liability .

(a) THE AGGREGATE LIABILITY OF EITHER PARTY IN CONNECTION WITH THE PERFORMANCE, DELIVERY OR PROVISION OF THE TRANSITION SERVICES UNDER THIS AGREEMENT SHALL, WITH THE EXCEPTION OF A DATA BREACH, BE LIMITED TO $2,500,000 CUMULATIVELY.

(b) EXCEPT FOR DAMAGES ARISING FROM THE GROSS NEGLIGENCE OR WILFUL MISCONDUCT OF SELLER, THE PARTIES EXPRESSLY WAIVE AND FOREGO ANY RIGHT TO RECOVER EXEMPLARY, LOST PROFITS, CONSEQUENTIAL OR SIMILAR DAMAGES IN ANY LITIGATION ARISING OUT OF OR RESULTING FROM ANY CONTROVERSY OR CLAIM RELATING TO THIS AGREEMENT OR ANY OF THE TRANSITION SERVICES PROVIDED HEREUNDER, WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY) OR OTHERWISE, EVEN IF AN AUTHORIZED REPRESENTATIVE OF SUCH PARTY IS ADVISED OF THE POSSIBILITY OR LIKELIHOOD OF THE SAME.

ARTICLE IX
CHANGE CONTROL

Section 9.1 Change Control .

(a) Subject to this Article IX, either Party may propose any change or addition to the Transition Services by written notice to the other Party specifying the proposed change in reasonable detail (such notice, a " Change Request ").

(b) Seller or Buyer shall provide the other Party with a reasonably detailed written outline specification describing the nature of the change, an assessment of the impact of the change on the Transition Services, the Service Fees (as applicable) and an estimate of the time required to implement the change, the costs associated with the change and the terms for payment of such costs (such outline, an " Evaluation Report ") within twenty (20) Business Days of receiving the Change Request.

(c) The approving Party shall notify the requesting Party within ten (10) Business Days of the date on which the Evaluation Report was received whether or not the approving Party wishes to proceed with the Change Request; provided, however, that the Parties shall in good faith negotiate the terms and pricing of the Change Request before the requesting Party provides such notice to proceed.

(d) Within ten (10) Business Days of receipt of the requesting Party's notice to proceed with the Change Request, the approving Party shall produce a final Evaluation Report which shall include a comprehensive list of the charges for the implementation of the Change Request (" Change Request Charges "). Any Change Request Charges shall be calculated in a manner consistent with Section 2.1.

(e) Both the Seller and Buyer shall act in good faith in relation to Change Requests, and shall not unreasonably withhold any consent, or cause any delay in relation to them; provided that, notwithstanding anything to the contrary herein, the approving Party shall have sole discretion regarding whether to provide Additional Transition Services which were not performed by Seller or Buyer for the Business at any time during the one hundred eighty (180) day period prior to Closing. If the Seller and Buyer cannot agree upon a Change Request or the approving Party's final Evaluation Report (including the Change Request Charges), each of the Seller and Buyer may refer the matter to be resolved in accordance with Section 1.2.

(f) The Seller shall not have any obligation to commence work in connection with any change to the approving Party Transition Services or any Additional Transaction Services until the relevant Change Request and Evaluation Report has been agreed to by each Party in writing.

ARTICLE X
MISCELLANEOUS

Section 10.1 No Third Party Beneficiaries . This Agreement shall not confer any rights or remedies upon any Person other than the Parties and their respective successors and permitted assigns and, to the extent specified herein, their respective Affiliates.

Section 10.2 Entire Agreement . This Agreement (including the Annexes and Schedule hereto), together with the Purchase Agreement and any other documents delivered by the Parties in connection herewith or therewith, constitutes the entire agreement between the Parties with respect to the subject matter hereof and thereof and supersede any prior agreements or understandings between the Buyer, on the one hand, and the Seller, on the other hand.

Section 10.3 Notices . All notices, requests, demands, claims and other communications hereunder shall be in writing. Any notice, request, demand, claim or other communication hereunder shall be deemed duly delivered four (4) Business Days after it is sent by registered or certified mail, return receipt requested, postage prepaid, or one (1) Business Day after it is sent for next Business Day delivery via a reputable nationwide overnight courier service, in each case to the intended recipient as set forth below:

If to the Buyer:

1015 Penn Avenue, Suite 103
Wyomissing, PA 19610
Attention: Robert Wahlman,
Chief Financial Officer
E-mail: rwahlman@customersbank.com

Copy to:

Stradley Ronon Stevens & Young, LLP
2600 One Commerce Square
Philadelphia, PA 19103
Attention: Christopher S. Connell, Esquire
Facsimile: 215-564-8120
E-mail: cconnell@stradley.com

If to the Seller:

Higher One, Inc.
115 Munson St.
New Haven, CT 06511
Attention: Christopher Wolf, Executive
VP and Chief Financial Officer
Email: christopher.wolf@higherone.com

Copies to:

Wiggin and Dana LLP
One Century Tower
265 Church Street
New Haven, CT 06508
Attention: Paul Hughes
Email: phughes@wiggin.com

Any Party may give any notice, request, demand, claim, or other communication hereunder using any other means (including personal delivery, expedited courier, messenger service, ordinary mail, or electronic mail), but no such notice, request, demand, claim or other communication shall be deemed to have been duly given unless and until it actually is received by the party for whom it is intended. Any Party may change the address to which notices, requests, demands, claims and other communications hereunder are to be delivered by giving the other Parties notice in the manner herein set forth.

Section 10.4 Amendment; Waiver . Subject to ARTICLE IX and Sections 1.4 and 10.10, any provision of this Agreement may be amended or waived if, and only if, such amendment or waiver is in writing and signed, in the case of an amendment, by both Parties, or in the case of a waiver, by the Party against whom the waiver is to be effective. No failure or delay by any Party in exercising any right, power or privilege hereunder shall operate as a waiver thereof nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any other right, power or privilege.

Section 10.5 Severability . Any term or provision of this Agreement that is invalid or unenforceable in any situation in any jurisdiction shall not affect the validity or enforceability of the remaining terms and provisions hereof or the validity or enforceability of the offending term or provision in any other situation or in any other jurisdiction. If the final judgment of a court of competent jurisdiction declares that any term or provision hereof is invalid or unenforceable, the Parties agree that the body making the determination of invalidity or unenforceability shall have the power to reduce the scope, duration or area of the term or provision, to delete specific words or phrases, or to replace any invalid or unenforceable term or provision with a term or provision that is valid and enforceable and that comes closest to expressing the intention of the invalid or unenforceable term or provision, and this Agreement shall be enforceable as so modified.

Section 10.6 Binding Agreement; Assignment . No Party may assign either this Agreement or any of its rights, interests, or obligations hereunder without the prior written approval of the other Party, which written approval shall not be unreasonably withheld, delayed or conditioned. Notwithstanding the foregoing, this Agreement, and all rights, interests and obligations hereunder, may be assigned, without such consent, by either Party to an Affiliate thereof or an entity that acquires all or substantially all of such Party's or such Affiliate's business or assets. This Agreement shall be binding upon and inure to the benefit of the Parties and their respective successors and permitted assigns.

Section 10.7 Governing Law . This Agreement and any disputes hereunder shall be governed by and construed in accordance with the internal laws of the State of New York without giving effect to any choice or conflict of law provision or rule (whether of the State of New York or any other jurisdiction) that would cause the application of laws of any jurisdiction other than those of the State of New York.

Section 10.8 Submission to Jurisdiction . Subject to Section 1.2 hereof, each of the Parties to this Agreement (a) agrees that all actions arising out of or relating to this Agreement or any of the transactions contemplated by this Agreement shall be heard and determined in the Federal Courts of the United States of America or the courts of the State of New York, in each case located in the City of New York and County of New York, (b) irrevocably consents to submit itself to the exclusive jurisdiction and venue of such courts in any action, (c) agrees that all claims in respect of such action shall be heard and determined in any such court, (d) agrees that it shall not attempt to deny or defeat such personal jurisdiction by motion or other request for leave from any such court, and (e) agrees not to bring any action arising out of or relating to this Agreement or any of the transactions contemplated by this Agreement in any other court. Each of the Parties hereto waives any defense of inconvenient forum to the maintenance of any action so brought and waives any bond, surety or other security that might be required of any other Party with respect thereto. Any Party hereto may make service on another Party by sending or delivering a copy of the process to the Party to be served at the address and in the manner provided for the giving of notices in Section 10.3. Nothing in this Section 10.8, however, shall affect the right of any Party to serve legal process in any other manner permitted by law.

Section 10.9 Waiver of Jury Trial . To the extent permitted by applicable law, each Party hereby irrevocably waives all rights to trial by jury in any action (whether based on contract, tort or otherwise) arising out of or relating to this Agreement or the transactions contemplated hereby or the actions of any Party in the negotiation, administration, performance and enforcement of this Agreement. Each Party (a) certifies that no Representative of the other Party has represented, expressly or otherwise, that such Party would not, in the event of any action, seek to enforce the foregoing waiver and (b) acknowledges that it and the other Party have been induced to enter into this Agreement, by among other things, the mutual waiver and certifications in this Section 10.9.

Section 10.10 Force Majeure . If either Party is prevented from complying, either totally or in part, with any of the terms or provisions of this Agreement by reason of fire, flood, storm, strike, lockout or other labor trouble, any law, order, proclamation, regulation, ordinance, demand or requirement of any governmental authority, riot, war, terrorist act, rebellion or other causes beyond the reasonable control of such Party, or other acts of God (a " Force Majeure Event "), then, upon written notice to the other, the affected provisions and/or other requirements of this Agreement shall be suspended or reduced by an amount consistent with reductions made to the other operations of such Party affected by the Force Majeure Event during the period of such disability and the affected Party shall have no liability to the other in connection therewith. Each Party shall use reasonable commercial efforts to remove such disability within fifteen (15) days of giving notice of such disability.

Section 10.11 Mutual Drafting . This Agreement is the mutual product of the Parties, and each provision hereof has been subject to the mutual consultation, negotiation and agreement of each of the Parties, and shall not be construed for or against any Party. Each Party acknowledges and represents that it has been represented by its own legal counsel in connection with the transactions contemplated hereby, with the opportunity to seek advice as to its legal rights from such counsel.

Section 10.12 Headings . The headings in this Agreement are for convenience of reference only and will not affect the construction of any provisions hereof.

Section 10.13 Conflicts . To the extent any term or provision of the Purchase Agreement, or any other document or other agreement executed in connection with the Purchase Agreement, is in conflict with any term or provision of this Agreement or any Annex or Schedule hereto, the terms and provisions of this Agreement and the Annexes or Schedules hereto shall govern solely to the extent of any such conflict. To the extent any term or provision of this Agreement is in conflict with any term or provision of any Annex or Schedule hereto, the terms and provisions of the Annex or Schedule hereto shall govern solely to the extent of any such conflict.

Section 10.14 Counterparts and PDF Signature . This Agreement may be signed in any number of counterparts, each of which shall be an original, with the same effect as if the signatures thereto and hereto were upon the same instrument. The electronic transmission of any signed original counterpart of this Agreement shall be deemed to be the delivery of an original counterpart of this Agreement.

Section 10.15 Interpretation . For purposes of this Agreement, (a) the words "include," "includes" and "including" shall be deemed to be followed by the words "without limitation"; (b) the word "or" is not exclusive; and (c) the words "herein," "hereof," "hereby," "hereto" and "hereunder" refer to this Agreement as a whole. Unless the context otherwise requires, references herein: (x) to Articles, Sections, Schedules and Exhibits mean the Articles and Sections of, and Schedules and Exhibits attached to, this Agreement; (y) to an agreement, instrument or other document means such agreement, instrument or other document as amended, supplemented and modified from time to time to the extent permitted by the provisions thereof and (z) to a statute means such statute as amended from time to time and includes any successor legislation thereto and any regulations promulgated thereunder. This Agreement shall be construed without regard to any presumption or rule requiring construction or interpretation against the Party drafting an instrument or causing any instrument to be drafted. The Schedules and Exhibits referred to herein shall be construed with, and as an integral part of, this Agreement to the same extent as if they were set forth verbatim herein.

[End of Text; Signature Page Follows]

IN WITNESS WHEREOF, the Parties hereto have executed this Transition Services Agreement as of the date first written above.

HIGHER ONE, INC.

By: /s/ Marc Scheinbaum
Name: Marc Scheinbaum
Title: President & CEO

CUSTOMERS BANK

By: /s/ Robert E. Wahlman
Name: Robert E. Wahlman
Title: Executive Vice President & CFO

ANNEXES

ANNEX A	SELLER TRANSITION SERVICES
ANNEX B	BUYER TRANSITION SERVICES
ANNEX C	HIGHERONE SECURITY REQUIREMENTS

SCHEDULE 1.2

SERVICE COORDINATORS

Seller
Services Coordinator:

Cozzell Wilson
Chief Information Officer
203-776-7776 ext 4599
Cozzell.wilson@higherone.com

Buyer
Services Coordinator:

Jack Allison
Chief Informaiton Officer – Bankmobile
1015 Penn Ave
Wyomissing, PA 19610
856-581-1197
jallison@bankmobile.com

ANNEX A
TRANSITION SERVICES

Transition Services Agreement (TSA)
Annex A – Section 1

Information Technology

Scope of Services

Seller, itself and/or by and through its Affiliates, shall provide or cause to be provided to Buyer the following information technology services in the manner set forth below:

- Chennai Resources
  - o Provide engineering services relating to the Business furnished by personnel located in Chennai, India.
  - o Provide the Chennai resources listed below (the " Chennai Resources "):

Manoj Kumar Ramesh	Senior Quality Analyst	Quality Assurance
Saravan Kumar Ekambaram	Senior Quality Analyst	Quality Assurance
Tamil Selvan Mohan	Project Lead	Quality Assurance
Gavathri Selvam	Jr. Software Engineer	Quality Assurance
Aishwariya Kandaswamy	Technology Trainee	Quality Assurance
Dhanalakshmi Sekar	Technology Trainee	Quality Assurance
Bharathkumar Sainathan	Associate Project Lead	Mobile Development
Anandababu Sivaprakasam	Sr. Software Developer	Mobile Development
Varun Muthu	Sr. Quality Analyst	Mobile Development
Hari Babu Goggi	Lead Developer	OD/OA Development
Mahesh Perumal	Sr. Project Lead	OD/OA Development
Suresh Allareddy	Associate Project Lead	OD/OA Development
Jeevakumar Jenadoss	Lead Developer	OD/OA Development
Praveen Rajan	Sr. Software Developer	OD/OA Development

; subject to the following terms: (i) from September 19, 2016 until December 31, 2016, the Chennai Resources will be provided at an additional cost to Buyer of $25,000 per month, (ii) the Chennai Resources will be provided to Buyer until December 31, 2016, provided that Buyer may extend the use of such resources until the Termination Date upon ninety (90) days' written notice to Seller, (iii) the Chennai Resources shall be directed by a Manager selected by Buyer, (iv) onsite support shall be provided by Bala Meenakshisundarm (or other person at the sole discretion of Seller),and (v) Seller will provide support to Buyer in connection with Buyer's efforts to fill any vacancies created as a result of attrition of the Chennai Resources.

- Consulting
    - Provide up to 1600 "SME" consulting hours during the Term, not to exceed more than 140 hours per month. SME consulting hours are for consultation on the planning and design of Buyer's future operating environment. SME consulting hours are in addition to the hours required to support the tasks set forth below under the "Operations; IT Infrastructure" heading. Any consulting hours in excess of 1600 shall be provided upon Seller's written approval, at a mutually agreed upon price.

- Computers and Access
    - Maintain ("break/fix") Transferred Employee computers, onsite and remote access, office phones, local and long distance service, print services and current network connectivity at current support levels for Seller employees; provided that Buyer shall be responsible for the replacement cost of any Transferred Employee or Other Transferred Employee computers or parts therefor. Changes to computers' configurations and installed software will not occur during the Term.
    - Process new access/access change requests from Transferred Employees to systems supported by Seller.
    - Process new password reset requests from Transferred Employees to systems supported by Seller.
    - Create and support new access requests for up to twenty (20) Buyer employees who are not Transferred Employees to Seller IT systems, utilizing a computer provided by Seller that will use VPN with two-factor authentication for the sole purpose of accessing systems maintained on Seller's internal networks. All costs incurred by Seller in connection with transferred computer hardware and installed software will be reimbursed by Buyer.

- Email and Phone Systems
    - Maintain email accounts and "read only" access to email accounts for Transferred Employees for a period of 45 days after the date hereof.
    - Forward inbound emails to new Buyer email accounts until October 15, 2016.
    - In accordance with Seller's data retention policies, maintain historical email files to allow customer requested research, customer complaint related research and regulatory inquiries. Seller data retention policies are subject to change.
    - Maintain Phone setup, configuration and system maintenance for Transferred Employees.
    - Provide support to offshore contact center configuration, similar to what was provided prior to the transfer date.
    - Provide Transferred Employees the ability to access and take certain actions as required on certain internal email accounts.

- <u>Operations; IT Infrastructure</u>
  - Maintain and support the production and backup environments located at the Seller data centers in New Haven, CT and Altanta, GA for the OneDisburse/OneAccount application. This includes all systems that are involved in supporting the OneDisburse/OneAccount application, including but not limited to the WAN and LAN network infrastructure, the security infrastructure, database infrastructure, application server infrastructure, monitoring systems, SAN/NAS infrastructure and appliances (Terradata, load balancers). All current vulnerability and penetration testing, patch management policies, applicable vendor relations and software licenses will be maintained. Support and maintenance contracts for the data center facilities, which include HVAC, UPS, fire suppression systems, access control and generators, will be maintained at current levels.
  - Maintain and support the development environment located at the New Haven Seller data center for the OneDisburse/OneAccount application. This includes all systems that are involved in supporting the OneDisburse/OneAccount application, including but not limited to the WAN and LAN network infrastructure, the security infrastructure, database infrastructure, application server infrastructure, monitoring systems, SAN/NAS infrastructure and appliances (Terradata, load balancers). Also included are development tools utilized in the development of the OneDisburse/OneAccount software, including code repositories, testing tools, and required tools for audit and security. All current patch management policies, applicable vendor relations and software licenses will be maintained. Support and maintenance contracts for the data center facilities, which include HVAC, UPS, fire suppression systems, access control and generators, will be maintained at current levels.
  - Maintain and support the QA/testing environment located at the New Haven Seller data center for the OneDisburse/OneAccount application. This includes all systems that are involved in supporting the OneDisburse/OneAccount application, including but not limited to the WAN and LAN network infrastructure, the security infrastructure, database infrastructure, application server infrastructure, monitoring systems, SAN/NAS infrastructure and appliances (Terradata, load balancers). Also included are QA/testing tools utilized in the QA/testing of the OneDisburse/OneAccount software, including code repositories, testing tools, and required tools for audit and security. All current patch management policies, applicable vendor relations and software licenses will be maintained. Support and maintenance contracts for the data center facilities, which include HVAC, UPS, fire suppression systems, access control and generators, will be maintained at current levels.
  - Maintain and support back office systems that are currently in place and used by the OneDisburse/OneAccount employees, including but not limited to the file shares, Microsoft Exchange, Bugzilla, Chat and ALM. Seller will also maintain all access to 3 rd party SaaS applications that are currently in place and used by the OneDisburse/OneAccount employees, including but not limited to WebEx, ADP, SalesForce and RightNow. Seller will maintain and support the underlying infrastructure, which includes but is not limited to the WAN and LAN network infrastructure, the security infrastructure, database infrastructure, application server infrastructure, monitoring systems and SAN/NAS infrastructure. All current patch management policies, applicable vendor relations and software licenses will be maintained. A list of the current back office systems and 3 rd party SaaS applications are provided in the application and 3 rd party SaaS application documents.
  - Provide IT operations management reports at the same intervals such reports were generated prior to the Closing, including root cause analysis for systems outages impacting OneDisburse and/or OneAccount, Client Facing Systems Up Time, Quarterly Support Desk Metrics, Quarterly Ubiquity Ticket Volume, Quarterly Refunds Service Outage Report, Quarterly Product Change Management Report, any other IT operations management reports regularly generated by Seller prior to Closing, and any other reports mutually agreed upon by the Parties.
  - Data extracts and configuration information or system clones, as determined by the Migration Plan, will be supplied for systems where data and configuration information has been agreed to be migrated to Buyer, including but not limited to Bugzilla, ALM, source code repositories, and "H" drive.
  - Support implementation of Buyer initiated circuits.
  - Continue providing the current disk storage for electronic files, data backups and backups of production and development environments.
  - Continue to support existing integration between OneDisburse and CashNet (including Single Sign-on, refund data on ePayment and OneAccount as tender type on CashNet).

- Provide DNS services for critical websites, including bankmobileadminsupport.com, and vibeaccount.com.
- Provide data security services for Seller's existing IT environment, including threat and event management, security monitoring, change management, access management, vulnerability and patch management, and information security review for vendors with access to non-public personal information.
- Buyer shall be responsible for any costs associated with changes to the existing computing environment proposed by Buyer and accepted by Seller.

- Governance
  - A member of the Buyer transition team will be invited to the Seller change management board meetings for the OneDisburse/OneAccount environment and supporting systems changes. Buyer will create one or more distribution groups for system notifications which will be added to the Seller notification process.
  - Define a mutually agreed upon governance process and participate with Buyer to support changes to the application environment and software for OneDisburse/OneAccount.
  - Deploy OneDisburse/OneAccount code releases that are consistent with the OneDisburse/OneAccount product roadmap. Any releases that require changes to the existing computing environment shall be mutually agreed upon by Buyer and Seller.

- Audit
  - Cooperate with Buyer, perform and maintain all current audit schedules for the SSAE16 and SOX audits on the OneDisburse/OneAccount environment during the Term. Seller is only responsible for performing and maintaining the current audit schedules for the environments under the Seller's control. Audits of environments that are implemented by the Buyer that are either in front of or behind the OneDisburse and/or OneAccount environments will be the responsibility of the Buyer.
  - Cooperate with Buyer-initiated audits (financial, internal audit or any other audits) to the extent such audits are not duplicative of any audits performed by Seller.
  - Perform the current DR testing plan one time on the OneDisburse/OneAccount environment during the Term, unless otherwise agreed by the Parties.

Duration of Services

- Cooperate with Buyer to identify and hire temporary staff resources in order to meet current demand.

Unless otherwise set forth herein, the service period applicable to the Seller Transition Services set forth in this Annex A – Section 1 shall begin on the Closing Date and end on the Termination Date.

Transition Services Agreement (TSA)
Annex A – Section 2

Accounting

Scope of Services

Seller, itself and/or by and through its Affiliates, shall provide or cause to be provided to Buyer the following accounting services in the manner set forth below:

- Forward OneDisburse/OneAccount vendor invoices received by Seller after Closing.
- Provide access to the Accounts Receivable System (ACCPAC) for the purpose of creating client invoices.

Duration of Services

The service period applicable to the Seller Transition Services set forth in this Annex A – Section 2 shall begin on the Closing Date and end on the Termination Date.

Transition Services Agreement (TSA)
Annex A – Section 3

Legal

Scope of Services

Seller, itself and/or by and through its Affiliates, shall provide or cause to be provided to Buyer the following legal services in the manner set forth below:

- Assist Buyer's legal team with the transfer of OneDisburse/OneAccount dedicated vendor contracts.
- Assist Buyer's legal team with the separation of vendor contracts that support both OneDisburse/One Account and the other businesses of Seller.
- Advise Buyer's legal team with respect to the transfer of customer agreements.
- Complete, at Buyers' reasonable request, any attestations required of Seller under Title IV regulations.

Duration of Services

The service period applicable to the Seller Transition Services set forth in this Annex A – Section 3 shall begin on the Closing Date and end on the Termination Date.

Transition Services Agreement (TSA)
Annex A – Section 4

Facilities

Lease

The provision of space described in this Section 4 is included in this Annex A for informational purposes only. The provision of the space, and other details in this Section 4, shall not constitute a Transition Service, or any other service or commitment, under this Agreement. The provision of the space shall be only as set forth in, and subject in all respects to, the Lease Agreement, dated as of the Closing Date, between Seller and Buyer (the "Lease").

Scope of Services

Seller, itself and/or by and through its Affiliates, shall provide or cause to be provided to Buyer the following facilities services in the manner set forth below:

- Provide office space at 115 Munson Street, New Haven.
- Maintain New Haven and Atlanta sites to current standards.
- Maintain employee access to Seller facilities for employees transferred to Buyer.
- Provide access to Seller facilities for Buyer employees who are not Transferred Employees.
- Provide mailroom services to employees at the New Haven location.
- Provide access to existing office equipment (e.g. copier, fax machine) at the New Haven location at a pass-through cost.
- Provide secure space for hard copy files at the New Haven location.
- Maintain existing copy files located at Iron Mountain and enable access to Transferred Employees.
- For so long as Seller provides food service to its employees in New Haven, provide food service to Buyer employees in New Haven, including lunch three times per week (Tuesday – Thursday), and coffee daily from 8:00a - 10:30a.
- Integrate into Buyer's business continuity and disaster recovery plan as related to data center operations and closures of New Haven and/or Atlanta Facilities.

Duration of Services

The service period applicable to the Seller Transition Services set forth in this Annex A – Section 4 shall begin on the Closing Date and end on the Termination Date.

ANNEX B
BUYER TRANSITION SERVICES

Transition Services Agreement (TSA)

Scope of Services

Buyer, itself and/or by and through its Affiliates, shall provide or cause to be provided to Seller the following services in the manner set forth below:

- Banking Operations
  - Provide sufficient ATM-related resources to complete Buyer's ATM Removal and Disposition Project. Such project, and the individuals involved therein, shall be directed by VP Deposit Operations or other appropriate manager appointed by Buyer.
  - Provide ability for members of Seller's payments banking staff to process batch transactions to the Fiserv Signature Core for the purposes of posting entries and obtaining statement data. If such access is not provided, Buyer shall post entries and create statement copies for Seller.
  - Seller will be solely responsible for the data and the results of processing batch transactions in the Fiserv Signature Core.

- Legal
  - Provide assistance and cooperation as needed in connection with Seller's implementation of the consent orders relating to the matters set forth in Section 2.04(e) of the Disclosure Schedules (including the Restitution Plans which have been accepted by the Federal Reserve and which received a non-objection from the FDIC) (the " Consent Orders ") until the expiration of the period applicable to each Consent Order. The assistance and cooperation shall include the following:
    - Provide to Seller promptly upon its request such account information, including name, postal address, email address, account balance, transaction detail, web site access, or other information as is necessary for Seller to make restitution payments (including credits for open and active accounts and checks for dormant or closed accounts) as is necessary for Seller to fully implement the Restitution Plans, including any audit, verification procedures required or information requests from the Federal Reserve or FDIC.
    - Provide Seller such access to information technology personnel, software, data retrieval systems, and vendors as is necessary to implement the Restitution Plans efficiently and cost effectively.
    - Provide Seller such access to and assistance of the Transferred Employees as is reasonably necessary for Seller to comply with the Consent Orders.
    - Maintain, establish and modify as required by the Restitution Plans and as otherwise required by the Federal Reserve or the FDIC the web page announcement referenced in Paragraph 7 of the Federal Reserve Consent Order and Paragraph 27 of the FDIC Consent Order. If third party costs are required, Seller shall be solely responsible.
    - Provide data and information as reasonably requested by Seller in connection with any Consent Order or other legal or regulatory matters to which Seller may be subject, for the duration of the applicable legal matter.
    - Provide assistance and cooperation as needed to WEX Bank in connection its compliance obligations under the Consent Orders and any other regulatory compliance obligations related to OneAccount.

  - The service period applicable to the Buyer Transition Services set forth under this "Legal" heading shall begin on the Closing Date and end when the latter of the Federal Reserve and the FDIC determines that restitution is complete pursuant Paragraphs 10 and 34 of the Consent Orders, respectively.

- Information Technology
    - o Continue to support existing integration between OneDisburse and CashNet (including Single Sign-on and ePayment data presented on OneDisburse).
    - o Provide a secure method of communication between Buyer and Seller.
    - o During the term of the TSA, Seller shall maintain current business continuity services for the primary data center located in New Haven, CT from the backup data center located in Atlanta, GA.

- Finance
    - o Continue to provide access to HOBIT (Business Intelligence) to allow retrieval of payments reports (including MMDA Alert Report, MMDA Detail Report, Transaction Report with Account and Date Prompt, Transaction Report with Product Code and Date Prompt, Trial Balance Lookup with Account and Date Prompt, and Trial Balance Lookup with Product Code and Date Prompt).
    - o Provide payment of expenses for Seller's employees through existing OneAccount system. Seller shall reimburse Buyer for any such payments.

- Client Operations
    - o Provide clients of Seller's payments division access to the e-Train site (Moodlerooms) to retrieve training materials, software release notes and documents.

Duration of Services

Unless otherwise set forth herein, the service period applicable to the Buyer Transition Services set forth in this Annex B shall begin on the Closing Date and end on the Termination Date.

ANNEX C
HIGHERONE SECURITY REQUIREMENTS

ACCESS TO HIGHER ONE CONFIDENTIAL INFORMATION

Higher One's Information Security Program is comprised of a number of policies, standards and guidelines, developed with reference to the source documents cited previously, as well as with consideration of the Company's business and regulatory needs. When referencing the Information Security Program any or all of these policies are included.

Privacy Policy

Overview

Higher One may log user system activity, record building access, monitor Internet usage and use security cameras to monitor building facilities. User's work output, regardless of storage format (e.g., paper, electronic, etc.) is the property of Higher One. The output, and any tools used to generate that output, is subject to review or monitoring by the Company at its discretion. User personal information is not used or disclosed except to comply with laws, and to protect our rights. It is used solely for business purposes including establishing, maintaining or terminating employment or contractual agreements between the user and Higher One.

Standards

Audits or investigations may be conducted to:

1) Ensure integrity, confidentiality and availability of information and resources.

2) Investigate possible security incidents.

3) Ensure conformance to security policies.

4) Monitor system or user activity where appropriate.

During an audit, all required data will be provided to the Information Security Office upon request. For the purpose of performing an investigation, any access required will be provided to the Information Security team members for the duration of the investigation. Such access may include:

1) User and/or system level access to any computing or communications device.

2) Access to information, whether electronic or hard copy, that may be produced, transmitted or stored on Company equipment or premises.

3) Access to work areas such as labs, offices, cubicles or storage areas.

4) Access to interactively monitor and log traffic on networks.

Password Management Policy

Overview

Higher One's Password Management Policy is directed to ensuring only strong, secure passwords are used on all accounts, systems and equipment. Password standards define the minimum length, composition, aging and re-use parameters, as well as lock out limitations. Password standards are enforced to protect Company systems, Company and customer data, as well as Higher One's reputation. Password guidelines provide additional information to assist users in protecting passwords and account access.

Standards (General)

All passwords must meet minimum requirements, within the capabilities of the applicable system. Password cracking exercises may be performed on a periodic basis by the Information Security Office. Passwords that are exposed during such an exercise will result in the user being required to change to a more secure password immediately.

Except where otherwise defined or dictated, minimum password requirements are:

1) At least 8 (eight) characters in length, where applicable.

2) Contain both upper and lower case letters.

3) Contain at least one number.

4) Contain at least one special character (within the bounds of those special characters supported by the system in question).

5) May not contain more than 3 (three) consecutive identical characters.

6) System level passwords must expire and be changed no more than every 42 days.

7) At a minimum, the prior 13 (thirteen) passwords may not be reused.

8) Users must have the ability to change a password at any time.

9) Accounts must be locked after at least 5 (five) unsuccessful login attempts.

10) User accounts with elevated privileges must have a password that is unique to that account and not the same as lower-privileged account(s) held by the same user.

11) Passwords are to be treated as sensitive and confidential information and are not to be shared, written down or stored in an unsecured manner.

12) Passwords are not to be conveyed via email.

13) Passwords must not be displayed in clear text (e.g., must be masked) while being entered.

14) Default vendor or manufacturer accounts and passwords should be changed as soon as reasonably possible.

15) If a password is suspected to have been compromised, change the password immediately and report the incident to the IT Operations Support Desk, which will inform the Information Security Office.

16) Where Simple Network Management Protocol("SNMP") is used, the community strings must be defined as something other than the standard defaults of "public", "private" and "system", and must be different than the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

17) Passwords must be changed in the event of a user's departure.

Guidelines

The guidelines provided herein are intended to assist users in protecting both their passwords, their access and their accounts from unauthorized use. These guidelines constitute established best practices. None of the examples cited below should be used as passwords.

- Avoid poor, weak or common passwords such as *Welcome123* , *Password1* , or *ChangeMe123* .
- Avoid common words, even if spelled backwards or with the addition of a number, such as *secret1* , *1secret* , or *terces* .
- Avoid patterns of numbers or letters such as *aabbcc* , *qwerty* , or *12344321* .
- Avoid commonly known personal information such as birthdates, addresses, names of family members, friends or pets.
- Avoid work-related information such as company names, building sites, etc.
- Should not contain common nouns, proper names or dictionary words.
- To create a secure but memorable password, consider creating a passphrase based on a song title, affirmation or memorable phrase that contains multiple words. For instance, *This May Be One Way To Remember* could become the password *TmB1w2R!* or *I saw my favorite band last Friday night!* becomes IsmF3lFn!.

Standards (Service Accounts)

Service Accounts are defined as system-level accounts that are not associated with one specific individual, but are used for administration, management, or maintenance of a system or application, or are required by a system or application. Service Accounts may also be either interactive or non-interactive.

Interactive Service Accounts are defined as those that meet all of the following criteria:

1) Are highly privileged (e.g., have root level access on a Linux system, local or domain administrator access on a Microsoft Windows system, sa level access on a Microsoft SQL Server system, sys/system on an Oracle database, etc.).

2) Permits interactive logons (e.g., a user can use ssh to open a shell prompt on a Linux system, use Remote Desktop Services to access a desktop on a Microsoft Windows system, may use SQL Studio to perform queries on a Windows system, etc.).

3) The account passwords are retained (e.g., stored in Password Safe, Password Manager or some other location for future access).

Non-interactive Service Accounts are defined as those that meet any of the following criteria:

1) Are not highly privileged (e.g., do not have root level access on a Linux system, local or domain administrator access on a Microsoft Windows system, sa level access on a Microsoft SQL Server system, sys/system on an Oracle database, etc.).

2) Does not permit interactive logons (e.g., a user cannot use ssh to open a shell prompt on a Linux system, use Remote Desktop Services to access a desktop on a Microsoft Windows system, or use SQL Studio to perform queries on a Windows system, etc.).

3) The account passwords are not retained (e.g., not stored in Password Safe, Password Manager or some other location for future access). This circumstance applies to accounts where there is no need to use the password in the future and so the password is set to a long random value and not saved.

Service Account standards must meet the criteria outlined in Standards (General) section, with the following exceptions:

1) At least 12 (twelve) characters in length.

2) Service accounts shall have Deny Logon Locally or comparable attribute set if supported on the operating system.

3) Interactive Service Account passwords will expire and must be changed no more than every 90 days.

4) Non-interactive Service Account passwords will expire and must be changed no more than every 720 days.

5) In the event that the account password cannot be changed or the application vendor recommends against changing the password because it would adversely impact the application, an exception will be documented and approved by the Information Security Officer and that password will be exempt from periodic changes.

Initial Passwords and Password Resets

Where supported by the system in question, initial passwords must be set to a temporary and unique value, and be reset by the user upon first use.

In the event a password must be reset, a temporary and unique value must be provided, and must be reset by the user at the time of successful login.

Identity and Access Policy

Overview

The Identity and Access Policy defines the tasks that principals can perform, resources they can access and defines which activities will be audited for regulatory compliance purposes. Access controls are established, documented and periodically reviewed, based on business needs and external requirements.

Standards

1) Access Administration: This area focuses on ensuring authorized user access, and preventing unauthorized user access, to information and information systems.

   a. Procedures covering all stages in the life-cycle of user access, from provisioning and modification to de-provisioning.

   b. Documentation of approval from the hiring Supervisor or System Owner for each user's access, where appropriate.

   c. Ensuring restricted or sensitive access is not granted until all authorization procedures are completed.

   d. Special attention to control of privileged ("super-user") access rights.

2) Compliance

   a. Attestation - Confirmation by a reviewing Supervisor or designee that each user's access is consistent with business purposes and with other security controls (e.g., segregation of duties).

   b. Access Permissions Review - A formal process must be conducted periodically (quarterly) by System Owners to review user access rights to critical systems. This review shall be documented / approved by System Owners and retained by the Information Security Office (as defined below) for audit verification purposes. Each System Owner is accountable for identifying inappropriate access and inactive user access in a timely manner to the Security Administrators.

   c. Access to non-critical systems will be reviewed based on risk but no less frequently than annually.

User Identity Verification Policy

Overview

Higher One's User Identification Verification Policy contains information and requirements for verifying the identity of a system user when unlocking an account, resetting a password or otherwise assisting with logging in. This policy also defines the systems that are within the scope of the policy.

Standards

1) This policy applies to the following systems:

    a. Active Directory, any domain

    b. RSA SecurID PIN

    c. CASHNet/IDC

    d. LDAP (Corporate and Production)

    e. Higheronesupport.com

    f. TPP Applications

    g. NetPay Applications

2) A user's identity must be verified prior to resetting his/her password on any in-scope system.

    a. If the request is made in person, photo identification is an acceptable means of verifying the user's identity.

    b. If the request is made by telephone, the user must provide a matching and valid Employee ID which will be verified against records.

    c. Requests by email will not be accepted, and the user will be instructed to telephone.

3) In the event the user cannot provide a valid Employee ID, the user's manager or (if a contractor) employee sponsor can verify the user's identity, after verifying his/her own identity.

Privileged Account Policy

Overview

Privileged accounts are valid credentials used to gain access to information systems. Privileged credentials provide elevated, non-restrictive access to the underlying platform that non-privileged user accounts do not have access to. Root, local administrator, domain administrator and enable passwords are all examples of privileged accounts that have elevated access beyond that of a normal user.

If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required clearly justifies using privileged access. In addition, passwords for privileged accounts should be randomized, not memorized by anyone, and changed frequently. Whenever technically possible, gaining and using privileged access should be audited.

Privileged access to information systems is granted only to authorized individuals based on clearly defined and documented business need.

Standards

1) System Approval and Authorization

    a. Providing clarity on what administrative privileges are necessary.

    b. Minimizing the use of shared administrative accounts.

    c. Having a method of being able to verify the privileges associated with each account.

2) Privileged User ID Activity Logging: All ID creation, deletion, and privilege change activity performed by Systems/Security Administrators and others with privileged user IDs must be securely logged.

3) Privileged Account Types

    a. Domain Administrative Accounts: These accounts give privileged administrative access across all workstations and servers within a Windows domain. While these accounts are few in number, they provide the most extensive and robust access across the network.

    b. Emergency Accounts: These provide unprivileged users with administrative access to secure systems in the case of an emergency and are sometimes referred to as 'firecall' or 'breakglass' accounts. Access to these accounts typically requires managerial approval for security reasons.

    c. Service Accounts: These can be privileged local or domain accounts that are used by an application or service to interact with the operating system. In some cases, these service accounts have domain administrative privileges depending on the requirements of the application they are being used for. Local service accounts can interact with a variety of Windows components

    d. Application Accounts: These are accounts used by applications to access databases, run batch jobs or scripts, or provide access to other applications. These privileged accounts usually have broad access to underlying company information that resides in applications and databases.

Remote Access Policy

Overview

Remote Access rules and requirements are designed to minimize the potential exposure to Higher One from damages which may result from unauthorized use of Higher One resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Higher One internal systems, and fines or other financial liabilities incurred as a result of those losses.

It is the responsibility of Higher One users with remote access privileges to Higher One's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Higher One. This policy applies to remote access connections used to do work on behalf of Higher One, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Higher One networks.

Standards

1) Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases.

2) Authorized Users shall protect their login and password, even from family members.

3) All hosts that are connected to Higher One internal networks (including employee owned equipment) via remote access technologies must use up-to-date anti-virus software. Third party connections must comply with requirements as stated in the Third Party Agreement.

4) Users must not leave workstations unattended without locking or logging off the system.

5) Users must use personal desktop firewall software on any device connecting to Higher One networks or resources.

6) Higher One users who wish to implement non-standard Remote Access solutions to the Higher One production network must obtain prior approval from the Information Security Office.

7) The use of third-party managed remote access connections such as Webex and Go2MyPC can only be used for remote access in a support situation where personnel are present at both the asset being accessed and the system being used to obtain the remote access. This type of managed connection is explicitly not to be used to allow a user to remotely access a device which has been left unattended on the Higher One network.

8) Higher One Client VPN with the use of two-factor (FOB with Pin/Token plus password) authentication is required to connect to the HigherOne corporate network.

Third-Party/Vendor Access Policy

Overview

Companies or entities with a business relationship with Higher One should only be permitted the least access required to any internal network or application system, based on the business need. The access mechanism may include direct connectivity to Higher One assets, or the exchange of electronic information.

Higher One must actively control third party access to information systems. Business needs should be considered and a risk assessment must be carried out to determine security implications and control requirements.

This section is not intended to restrict or control access to integrated third-party systems required by Higher One products.

Standards

1) Controls and confidentiality clauses must be agreed on and defined in a contract with the third party.

2) All third party requests for Higher One data or connections to the Higher One network must be justified by business requirements, assessed for potential risks and control requirements, and then directed to appropriate Higher One management for review and approval.

3) All third party connections require approval from the Information Security Office.

4) Third-Parties must adhere to all Vendor Management Program requirements.

5) Reviews to ensure third-party access is still required and appropriate will be conducted periodically.

6) There are three methods allowed for direct connectivity between Higher One and third parties.

   a. Dedicated circuits - A leased line obtained through a telephony-communication provider.

   b. Site-to-Site Virtual Private Network (VPN) over the Internet – A two-way encrypted communications session between two networks that protect against eavesdropping by an unauthorized source and provides non-repudiation.

   c. Client-based VPN

Requirements for Connectivity

1) Before connectivity is established with a third party, a risk assessment must be performed as part of the vendor management assessment to validate that there are no high-risk issues involved with connecting to an external entity's network. A third party must not be immediately trusted and given immediate access to Higher One's network or application system without performing an appropriate level of due diligence.

2) Firewalls must restrict third party access to Higher One's network and application systems for which they have a defined business purpose.

   a. Explicit source and destination IP and ports must be defined in the firewall rules

   b. Must not be able to access other business partners' networks.

3) Firewalls must restrict Higher One's users from unlimited access to the third party network.

   a. Explicit source and destination IP and ports must be defined in the firewall rules

   b. Must only be able to access business partners' networks for which the user has a business purpose.

4) A list of approved third party connections must be maintained by the Information Security Office.

Data Classification

Overview

A data classification system sorts and labels every resource with its value, importance, sensitivity, cost, and other concerns in order to guide the implementation of security and prescribe processes of management and use. Assigning classification labels, such as public, private, sensitive, internal only, confidential, proprietary, etc., helps workers understand how to use and handle resources properly. Those resources with moderate to high value and sensitivity require greater control, tighter security, and stricter authentication. Often classification can improve the organizations defense against social engineering and other information leakage attacks. If workers know that certain information cannot be communicated via instant message, e-mail, or over the phone, then most socially guided attacks through those mediums will fail.

Asset Inventory

Higher One shall maintain a current inventory of all information assets, including hardware, software licenses and applications. The asset inventory must include at least the following elements:

1) A clear definition of each asset, including its business purpose and security classification.

2) Location of the asset.

3) Whether or not the asset contains personally identifiable customer information or card-related data.

Data Classification and Confidentiality

Higher One business units must classify information to indicate its level of sensitivity. Classifications dictate the priority and necessary degree of protection required to properly secure the information. Data classification classes are:

1) **Restricted** - The Restricted class applied to business and customer related information requiring the highest level of protection. If Restricted Data is disclosed, it could result in financial loss, violation of privacy and other laws or Regulations and significant negative publicity. Disclosure of Restricted Data may require initiating state or federal disclosure requirements. (e.g., PCI, PII, HIPAA)

2) **Confidential** - The Confidential class applies to business and customer related information that requires role-based protection and is sensitive enough to require elaborate controls. If Confidential Data is disclosed, employees or customers could be negatively impacted, initiating possible state or federal disclosure requirements.

3) **Private** - The Private classification applies to business and customer related information that requires some level of protection but is not sensitive enough to require extensive controls. Disclosure of Private data should be avoided but will have minimal impact.

4) **Public** - The Public class applies to information that has been made available for public distribution through authorized Higher One channels or information that will not cause any damage to Higher One if accidentally disclosed.

Credit Card Information Processing Applications

1) All applications dealing with the processing or retrieval of cardholder information, must, where there is not a business need to display full primary account numbers (PAN), mask displayed PAN to no more than the first six (6) and last four (4) digits of the full PAN.

2) If the application is designed for a specific purpose in which the full PAN must be displayed, approval must be given by the Information Security Office during the Requirements Phase as described in the SDLC process. In all cases the application must limit the display of the full PAN to the fewest number of users possible.

Credit Card Storage Applications

1) All Higher One application systems dealing with the storage of cardholder data must be on an internal network segregated from the demilitarized zone ("DMZ").

2) All access to networked storage devices containing cardholder data shall have its authentication communication encrypted.

3) The Primary Account Number ("PAN") must be rendered unreadable through one of the following:

   a. Strong one-way hash functions (hashed indexes) such as Secure Hash Algorithm 1) SHA-1 with salts.

   b. Truncation.

   c. Index tokens and pads (pads must be securely stored).

   d. Strong cryptography, based on industry-tested and accepted algorithms, with proper key management processes and procedures.

4) The PAN must never be stored in clear text in databases, files, or removable media.

5) The PAN must not be written to audit logs.

6) Full PAN must never be emailed or sent via instant messaging programs.

Technology Equipment Policies

Overview

Desktop, laptops, servers and virtual computers, as well as the software contained thereon, are resources that are provided to Higher One users for the purpose of conducting business on behalf of the Company. Administration, installation and maintenance of technology equipment are the responsibility of the Information Technology departments.

Warning Banners

Overview

A warning banner sets appropriate expectations for users accessing a system or device regarding the appropriate use of the resource, and warnings regarding monitoring of usage or activities while using the resource.

Standards

1) Higher One computing systems and devices, where supported by the device, must display a warning banner during the system login process. The message must state that the system must only be used for Higher One business purposes and is subject to monitoring.

2) Warning banners must be in a language consistent with the system's interface language.

3) The word "Welcome" or any similar language shall not be displayed prior to a successful user login.

Physical and Virtual Workstations

Overview

Desktops, laptops and virtual workstations are provided to users based on job role, need, and are based on company standard hardware configurations.

Standards

In addition to those items detailed in the Acceptable Use Policy,

1) Equipment is to be protected from theft or damage, including damage caused by foreign substances, impacts or misuse.

2) All laptop computers will be encrypted.

3) Online backup accounts will be provided to laptop users to ensure recoverability of data stored locally on the device.

4) Ensure that all vendor supplied defaults are changed before the system goes into production.

5) All desktops and laptops shall have personal firewall software which users should not be able to disable.

6) All desktops and laptops used to remotely access Higher One systems shall have VPN Client software capable of supporting the company's 2-factor authentication solution.

7) Workstation Configuration Standards will be reviewed on a periodic basis.

Guidelines

Physical security of computing devices can include the following:

- Having actual possession of a computer at all times.
- Locking the computer in an unusable state to an object that is immovable.
- Never leaving a laptop or other portable computing device unattended in a conference room, hotel room or on an airplane seat, etc.
- Locking the device in a hotel safe when traveling.

Server and Network Devices

Overview

The purpose of this policy is to establish standards for the base configuration of internal server and network equipment that is owned and/or operated by Higher One. Effective implementation of this policy will minimize unauthorized access to Higher One proprietary information and technology.

Unsecured and vulnerable servers continue to be a major entry point for malicious threat actors. Consistent Server installation policies, ownership and configuration management are all about doing the basics well.

Standards (Security)

All internal servers deployed at Higher One must be owned by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by IT and each application team, based on business needs and approved by Information Security.

1) All servers and network devices should be designated for a single primary purpose where possible.
2) All servers and network devices, prior to deployment in the production environment must conform to the Company's System Configuration and Hardening Standards.
3) Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
4) Ensure that all vendor or manufacturer supplied defaults are changed before the server goes into production.
5) Servers storing or processing confidential or restricted information shall have file integrity monitoring software installed.
6) File integrity monitoring software shall alert IT personnel to unauthorized modification of critical system or content files. The file integrity monitoring software shall be configured to perform critical file comparisons at least daily and should be logged. Information Security should be alerted to any abnormal activity.
7) All servers must have anti-virus software installed.
8) Information in the server inventory list must be kept up-to-date.
9) Configuration changes for production servers must follow the appropriate change management procedures.
10) Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.

11) Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.

12) If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using Secure Shell ("SSH") or Internet Protocol Security "IPSec").

13) Servers should be physically located in an access-controlled environment.

14) Servers are specifically prohibited from operating from uncontrolled cubicle areas.

15) For security, compliance, and maintenance purposes, authorized Information Security personnel may monitor and audit equipment, systems, processes, and network traffic.

Standards (Configuration)

1) Operating System configuration should be in accordance with approved System Configuration and Hardening Standards.

2) A valid business justification must exist for all deviations from published configuration standards. Deviations require written approval by the Chief Information Officer and must be noted on the asset inventory for the server.

3) Services and applications that will not be used must be disabled where practical.

4) All servers and network devices must be configured to use an internal authoritative time source to maintain time synchronization with other servers in the environment.

5) Server and network device Configuration Standards will be updated as new public standards become available and are approved by the Information Security Office and Information Technology.

Standards (Monitoring)

1) All security-related events on critical or sensitive systems must be logged and audit trails saved.

2) Security-related events will be reported to Information Security, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:

   a. Port-scan attacks.

   b. Evidence of unauthorized access to privileged accounts.

   c. Anomalous occurrences that are not related to specific applications on the host.

Cellular Device Policy

Overview

The Cellular Device Policy applies to any device that uses a wireless cellular network for communication, whether the device is supplied by Higher One or personally owned by the employee and used for business-related purposes. This policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

1) Tablets

2) Mobile/Cellular/Smart Telephones

3) Mobile Broadband devices (MiFis)

Standards

1) IT reserves the right to refuse the ability to connect mobile devices to the Higher One infrastructure.

Higher One's Cellular Device Policy can be found on the ADP portal under the heading Resources > Tools/References.

Equipment Disposal

Proper disposal of technology equipment is environmentally responsible and often required by law. To ensure that Higher One's electronic data, which may be stored on various types of storage media, is secured, all storage media must be completely erased or destroyed prior to release for disposal.

Standards

1) All information assets or office equipment which may contain a storage media component is in scope or this policy. This includes such items as computer workstations, servers, storage arrays, fax machines, printers, and copiers.

2) All forms of electronic media (e.g., fixed hard disks, flash memory, external drives, CDs, DVDs, tapes, USB drives) are within the scope of this policy.

3) At the time an in scope device or media is decommissioned or replaced, the item shall be destroyed, disabled or disposed of using methods and timing consistent with Higher One's Record Retention policies, any applicable retention laws and with due consideration for any litigation hold requirements currently in force.

   a. Hard drives will be erased to Department of Defense standards (DoD 5220.22M) or

   b. Physically destroyed by drilling or shredding.

4) When a computer workstation is transferred to a new user, the storage media will be:

   a. Replaced, if under a litigation hold, with the original component stored as per Higher One's procedures.

   b. Reformatted, if not subject to litigation hold.

5) The Facilities department will ensure that vendors remove any storage media contained within copiers, printers and fax machines prior to removing any such item from Higher One's premises.

6) Information Technology will maintain:

   a. Procedures for the proper erasure of data and/or destruction of storage media.

   b. Procedures for secure storage of media prior to destruction or disposal.

Software Installation Policy

Overview

Allowing users to install software on company computing devices opens the organization up to unnecessary exposure to risks such as the introduction of malware from infected installation files or software, unlicensed software, and programs which can be used to hack the organization's network.

Standards

1) Users may not install software on Higher One's computing devices operated within the Higher One network.

2) Software must be selected from an approved software list, maintained by the Information Technology department, unless no selection on the list meets the requestor's need.

3) Requests for software installations must first be approved by the requestor's manager and then submitted to the IT Support Desk in writing.

4) Any requests for software not on the approved list must be reviewed and approved by Information Technology and Information Security before purchase or installation.

The Information Technology Department will obtain and track the licenses and perform the software installation .

Exhibit 99.1

Customers Bancorp, Inc.

Customers Bancorp
1015 Penn Avenue
Wyomissing, PA 19610

Contacts:
Jay Sidhu, Chairman & CEO 610-935-8693
Richard Ehst, President & COO 610-917-3263
Investor Contact:
Robert Wahlman, CFO 610-743-8074

CUSTOMERS BANCORP, INC. COMPLETES ACQUISITION OF STUDENT CHECKING AND REFUND DISBURSEMENT BUSINESS

Wyomissing, Pa, June 16, 2016—Customers Bancorp, Inc. ("Customers") (NYSE—CUBI), announced it has successfully completed its previously announced acquisition of the OneAccount Student Checking and Refund Management Disbursement Services business ("Disbursements") of Higher One, Inc. ("Higher One") through its subsidiary Customers Bank. Customers acquired the Disbursements business pursuant to an Asset Purchase Agreement dated December 15, 2015, in which Customers agreed to purchase all of the assets of the Disbursements business, including all property and equipment, all contractual relationships with educational institutions, and all intellectual property. Effective with completion of the asset purchase, Customers will hire approximately 225 employees who previously managed the business and worked for Higher One.

Customers will combine the acquired Disbursements business with BankMobile, a division of Customers Bank. BankMobile provides no fee or very low fee banking deposit accounts, 55,000 surcharge-free ATMs across the country, and other banking services to over 2 million customers. It is anticipated that the combined business will generate in excess of 500,000 new deposit accounts annually. The OneAccount product offerings of Higher One will be rebranded as BankMobile products. Customers further anticipates that it will report BankMobile as a separate business segment in its communications with investors beginning with the third quarter of 2016 reporting cycle.

"Customers' acquisition of the Disbursements business is a wonderful strategic transaction that will accelerate the development of BankMobile as a profitable business segment," said Jay S. Sidhu, Chairman and Chief Executive Officer of Customers. "This transaction and combination of BankMobile with the Disbursements business will provide extremely compliant "best-in-class" deposit account services to 2 million college students and our many existing BankMobile customers while providing a platform for future growth," Mr. Sidhu continued. "We believe this opportunity to become the bank of choice for students entering the workforce upon completion of their education will drive the growth and expansion of services to the post graduate population and drive Customers' long-term shareholder value."

Mr. Sidhu continued, "I would like to welcome our new team members previously employed by Higher One. We look forward to working together to realize the many benefits of this strategic acquisition and building the bank of the future today."

About Customers Bancorp, Inc. and Customers Bank
Customers Bancorp, Inc. is a bank holding company located in Wyomissing, Pennsylvania engaged in banking and related business through its bank subsidiary, Customers Bank. Customers Bank is a community-based, full-service bank with assets of approximately $9.0 billion that was named one of Forbes magazine's 2016 100 Best Banks in America (there are over 6,200 banks in the United States). A member of the Federal Reserve System with deposits insured by the Federal Deposit Insurance Corporation, Customers Bank is an equal opportunity lender that provides a range of banking services to small and medium-sized businesses, professionals, individuals and families through offices in Pennsylvania, New York, Rhode Island, New Hampshire, Massachusetts and New Jersey. Committed to fostering customer loyalty, Customers Bank uses a High Tech/High Touch strategy that includes use of industry-leading technology to provide customers better access to their money, as well as Concierge Banking® by appointment at customers' homes or offices 12 hours a day, seven days a week. Customers Bank offers a continually expanding portfolio of loans to small businesses, multi-family projects, mortgage companies and consumers.

Customers Bancorp, Inc.'s voting common shares are listed on the New York Stock Exchange under the symbol CUBI. Additional information about Customers Bancorp, Inc. can be found on the Company's website, www.customersbank.com.

About BankMobile
Established in 2015, BankMobile, a division of Customers Bank with its headquarters in New York, is America's first no-fee digital bank. It provides target customers –millennials, the underbanked and middle income households – a digital, effortless, and financially empowering experience. BankMobile offers checking, savings, lines of credit, joint accounts and access to over 55,000 surcharge-free ATMs nationwide (BankMobile VIP customers have free access to every ATM in the country, which is more than 400,000 ATMs), a guaranteed higher savings rate than the top four banks in the nation, a personal banker for all customers, and a free financial advisor for VIP customers. For more information, please visit www.bankmobile.com.

"Safe Harbor" Statement

In addition to historical information, this press release may contain "forward-looking statements" within the meaning of the "safe harbor" provisions of the Private Securities Litigation Reform Act of 1995. These forward-looking statements include statements with respect to Customers Bancorp, Inc.'s strategies, goals, beliefs, expectations, estimates, intentions, capital raising efforts, financial condition and results of operations, future performance and business. Statements preceded by, followed by, or that include the words "may," "could," "should," "pro forma," "looking forward," "would," "believe," "expect," "anticipate," "estimate," "intend," "plan," or similar expressions generally indicate a forward looking statement. These forward-looking statements involve risks and uncertainties that are subject to change based on various important factors (some of which, in whole or in part, are beyond Customers Bancorp, Inc.'s control). Numerous competitive, economic, regulatory, legal and technological factors, among others, could cause Customers Bancorp, Inc.'s financial performance to differ materially from the goals, plans, objectives, intentions and expectations expressed in such forward-looking statements. In addition, important factors relating to the acquisition of the disbursements business of Higher One and Customer Bancorp's plans to combine its BankMobile business with the acquired business also could cause Customers Bancorp's actual results to differ from those in the forward-looking statements. Customers Bancorp, Inc. cautions that the foregoing factors are not exclusive, and neither such factors nor any such forward looking statement takes into account the impact of any future events. All forward-looking statements and information set forth herein are based on management's current beliefs and assumptions as of the date hereof and speak only as of the date they are made. For a more complete discussion of the assumptions, risks and uncertainties related to our business, you are encouraged to review Customers Bancorp, Inc.'s filings with the Securities and Exchange Commission, including its most recent annual report on Form 10-K for the year ended December 31, 2015 and subsequently filed quarterly reports on Form 10-Q. Customers Bancorp, Inc. does not undertake to update any forward looking statement whether written or oral, that may be made from time to time by Customers Bancorp, Inc. or by or on behalf of Customers Bank.