

Customer: City of Columbia, MO	Contact: Mr. Randy Cole
Address: 701 E Broadway Columbia, MO 65201	Phone: 573-874-6321
Services: Company will use commercially reasonable efforts to provide Customer the services described in the Services Statement of Work (“SOW”) attached as Exhibit A hereto (the “Services”).	
Services Fees: \$6,480.00 per year, payable annually in advance, subject to the terms of Section 4 and Per User Pricing attached as Exhibit D hereto.	Initial Service Term: One (1) year from Effective Date
Implementation Services: Company will use commercially reasonable efforts to provide Customer the services described in the Implementation Services Statement of Work attached as Exhibit C hereto (“Implementation Services”), and Customer shall pay Company the Implementation Fee at Effective Date.	
Implementation Fee (one-time): \$5,600.00	

SAAS SERVICES AGREEMENT

This Services Agreement (“Agreement”) is entered into on the date of the last signatory noted below (the “Effective Date”) between Benevate, Inc., a corporation organized in the State of Delaware with a place of business at 3423 Piedmont Rd. NE, Suite 373, Atlanta, GA 30305 (“Company”), and the City of Columbia, Missouri (“Customer”). Company and Customer are each individually referred to herein as a “Party” and collectively as the “Parties.”

WITNESSETH:

WHEREAS, the City of Columbia is in need of software to manage its housing programs;
and

WHEREAS, Company has submitted a proposal to provide the software and services outlined in this Agreement; and

WHEREAS, Customer has selected Company based upon Company’s representations that Company is qualified to complete the Services and to provide the software in accordance with the terms of this Agreement.

NOW, THEREFORE, the Parties hereto, for good and sufficient consideration, the receipt of which is hereby acknowledged, intending to be legally bound, do hereby agree as follows:

TERMS AND CONDITIONS

1. SAAS SERVICES AND SUPPORT

1.1 Company will use commercially reasonable efforts to provide Customer the services described in the Statement of Work ("SOW") attached as Exhibit A hereto.

1.2 Subject to the terms of this Agreement, Company will use commercially reasonable efforts to provide Customer the Services as described in in accordance with the Service Level Terms attached hereto as Exhibit B.

1.3 Company's Software, Services and Support shall comply with the requirements set forth in Exhibit E. Customer shall conduct acceptance testing according to the requirements set forth in Exhibit E. Should Customer determine that Company's software and services fail the acceptance testing, Customer may terminate the agreement for cause and or pursue such remedies as may be available to Customer at law or in equity.

2. RESTRICTIONS AND RESPONSIBILITIES

2.1 Customer will not, directly or indirectly: reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, know-how or algorithms relevant to the Services or any software, documentation or data related to the Services ("Software"); modify, translate, or create derivative works based on the Software (except to the extent expressly permitted by Company or authorized within the Services); use the Services or any Software for timesharing or service bureau purposes. The Parties agree that Customer may use the software, support and services for Customer's work related to the Columbia Community Land Trust.

2.2 Customer represents, covenants, and warrants that Customer will use the Services in compliance with all applicable laws and regulations.

2.3 Customer shall be responsible for obtaining and maintaining any equipment and ancillary services needed to connect to, access or otherwise use the

Services, including, without limitation, modems, hardware, servers, software, operating systems, networking, web servers and the like (collectively, "Equipment").

3. CONFIDENTIALITY; PROPRIETARY RIGHTS

3.1 Each party (the "Receiving Party") understands that the other party (the "Disclosing Party") has disclosed or may disclose business, technical or financial information relating to the Disclosing Party's business (hereinafter referred to as "Proprietary Information" of the Disclosing Party). Proprietary Information of Company includes non-public information regarding features, functionality and performance of the Service. Proprietary Information of Customer includes non-public data provided by Customer to Company to enable the provision of the Services ("Customer Data"). The Receiving Party agrees: (i) to take reasonable precautions to protect such Proprietary Information, and (ii) not to use or divulge to any third person any such Proprietary Information.

3.2 Customer shall own all right, title and interest in and to the Customer Data, as well as any data that is based on or derived from the Customer Data and provided to Customer as part of the Services.

3.3 Company shall own and retain all right, title and interest in and to (a) the Software, all improvements, enhancements or modifications thereto, (b) any software, applications, inventions or other technology developed by Company in connection with Implementation Services or support, and (c) all intellectual property rights related to any of the foregoing.

3.4 Customer is subject to the Missouri Sunshine Law. The Parties agree that the Agreement shall be interpreted in accordance with the provisions of the Missouri Sunshine Law, as amended. Company shall maintain the confidentiality of information and records which are not subject to public disclosure under the Sunshine Law. Company shall not disclose to any third party or use for any purpose inconsistent

with this Agreement any confidential information or data it receives in connection with its performance of the services. Company shall not give any confidential or proprietary information to the Customer to maintain. If it is required under this Agreement or by law that the Customer maintain any confidential or proprietary information or documents about Company's business, operations, financial condition, technology, systems, no-how, products, services, suppliers, clients, marketing data, plans, and models, and personnel, the documents and information shall be clearly marked as such.

3.5 DATA SECURITY.

Company and its software and services shall comply with the requirements of this Section. Company shall require its subcontractors or third party software providers to at all times comply with the requirements of this section.

Company's Software and services shall at all times comply with the terms of this Agreement, the Contract Documents, Good Financial Industry and Accounting Practices, Applicable Laws, Customer's Red Flag Policy, and SAS70 auditing standards. Company shall comply with the Customer's Red Flag policy and timely report any Red Flags to the Customer's Program Administrator. Said report shall include Red Flags detected by Company or its subcontractors or subsidiaries and Company's response to the Red Flags so detected.

If any Software module or Software upgrade includes the storage or use of credit cards and debit cards, Company shall comply and shall warrant that the Company's software and services (including any modifications, customizations or interfaces) comply with the Payment Card Industry (PCI) Data Security Standards; Good Financial Industry and Accounting Practices; SAS70 auditing standards; Visa, Mastercard, and Discover Card Rules and Regulations; NACHA (The Electronic Payments Association) Rules; and the Customer's Red Flag Policy.

If any Software module or Software upgrade includes the storage or use of protected health information under Health Insurance Portability and Accountability

Act (HIPAA), Company shall warrant that its software complies with HIPAA.

Company shall maintain the security of Customer content and data and that of Customer's customers and any user that is stored in or in any way connected with Software Products and applications. If either Party believes or suspects that security has been breached or data compromised whether it be from harmful code or otherwise, the Party shall notify the Other Party of the issue or possible security breach within twenty-four (24) hours.

BINDING SUBCONTRACTORS AND SUBSIDIARIES TO DATA SECURITY STANDARDS. Company shall include similar provisions in Company's agreements with subcontractors and subsidiaries who perform work or services related to these Software Products and or the Customer's Data contained therein or in the cloud storage.

NO HARMFUL CODE. Company warrants that the Software Products do not contain Harmful Code. For purposes of this Agreement, "Harmful Code" is any code containing any program, routine, or device which is designed to delete, disable, deactivate, interfere with or otherwise harm any software, program, data, device, system or service, including without limitation, any time bomb, virus, drop dead device, malicious logic, worm, Trojan horse or trap or back door. Company shall include in contracts with any subcontractor a provision which prohibits the use of Harmful Code.

DATA OWNERSHIP AND SECURITY

Company covenants that any data from the Customer, its employees or customers or derived therefrom shall be stored in the United States of America. The data or any information derived therefrom shall not be transferred, moved, or stored to or at any location outside the United States of America. All such data and any information derived therefrom shall be confidential and proprietary information belonging to either the Customer or its customers or the users of the Software. Company covenants that Company, its subsidiaries or subcontractors shall not sell or give away any such Customer data or information derived

therefrom.

4. PAYMENT OF FEES

4.1 Fees. For the initial term, customer shall pay six thousand four hundred and eighty dollars (\$6,480.00) per year payable in advance, subject to the terms set forth herein and per the user pricing attached as Exhibit D. For the implementation services, Customer will pay Company five thousand six hundred dollars (\$5600.00). Company reserves the right to change the Fees or applicable charges and to institute new charges and Fees at the end of the Initial Service Term or then-current renewal term, upon thirty (30) days prior notice to Customer (which may be sent by email). Per User Pricing, set forth on Exhibit D, shall increase by no more than three percent (3%) (the "Renewal Price Cap"), applied to the then-effective Per User Pricing set forth on Exhibit D at the time of renewal. The aforementioned Renewal Price Cap shall be forfeited if the Services are not renewed prior to the termination date of the initial Service Term; in which case, the fees for any subsequent renewal shall be calculated according to Company's then-current pricing.

4.2 If Customer believes that Company has billed Customer incorrectly, Customer must contact Company no later than sixty (60) days after the closing date on the first billing statement in which the error or problem appeared, in order to receive an adjustment or credit. Inquiries should be directed to Company's customer support department.

4.3 Company may choose to bill through an invoice, in which case, full payment for invoices must be received by Company thirty (30) days after the mailing date of the invoice. Unless tax exempt, Customer shall be responsible for all taxes associated with Services other than U.S. taxes based on Company's net income.

5. TERM AND TERMINATION

5.1 The Term of this Agreement shall commence on the Effective Date and shall continue until the date that is one year following the Effective Date. Thereafter, the Agreement shall automatically renew for additional periods of one (1) year (collectively, the "Term"), unless either party requests termination at

least thirty (30) days prior to the end of the then-current term.

5.2 In addition to any other remedies it may have, either party may also terminate this Agreement upon thirty (30) days' notice (or without notice in the case of nonpayment), if the other party materially breaches any of the terms or conditions of this Agreement. Customer will pay in full for the Services up to and including the last day on which the Services are provided.

5.3 Upon the termination of this Agreement Company shall, within five (5) business day following the termination of this Agreement, provide Customer, without charge and without any conditions or contingencies whatsoever (including but not limited to the payment of any fees due to Service Provider), with a final extract of the Customer Data in electronic format acceptable to Customer. Further, Company shall certify to Customer the destruction of any Customer Data within the possession or control of Company, but such destruction shall occur only after the Customer Data has been returned to Customer. This Section shall survive the termination of this Agreement.

6. WARRANTY AND DISCLAIMER

Company shall use reasonable efforts consistent with prevailing industry standards to maintain the Services in a manner which minimizes errors and interruptions in the Services and shall perform the Implementation Services in a professional and workmanlike manner. Services may be temporarily unavailable for scheduled maintenance or for unscheduled emergency maintenance, either by Company or by third-party providers, or because of other causes beyond Company's reasonable control, but Company shall use reasonable efforts to provide advance notice in writing or by e-mail of any scheduled service disruption.

7. INDEMNITY

7.1 Company shall hold Customer harmless from liability to third parties resulting from infringement by the Service of any United States patent or any copyright or misappropriation of any trade secret, provided Company is promptly notified of any and all

threats, claims and proceedings related thereto and given reasonable assistance and the opportunity to assume sole control over defense and settlement; Company will not be responsible for any settlement it does not approve in writing.

7.2 HOLD HARMLESS: To the fullest extent not prohibited by law, Company shall indemnify and hold harmless the City of Columbia, its directors, officers, agents, and employees from and against all claims, damages, losses, and expenses (including but not limited to attorney's fees) for bodily injury and/or property damage arising by reason of any act or failure to act, negligent or otherwise, of Company, of any subcontractor (meaning anyone, including but not limited to consultants having a contract with Company or a subcontractor for part of the services), of anyone directly or indirectly employed by Company or by any subcontractor, or of anyone for whose acts the Company or its subcontractor may be liable, in connection with providing these services. This provision does not, however, require Company to indemnify, hold harmless, or defend the City of Columbia from its own negligence.

8. Limitation of Liability

To the extent permitted by law and notwithstanding anything contained in this Agreement to the contrary, the total cumulative liability of Company for any and all claims arising from this Agreement, including attorneys' fees, and whether caused by negligence, errors, omissions, strict liability, breach of contract or contribution IS LIMITED TO THE COVERAGE ACTUALLY AFFORDED BY COMPANY'S INSURANCE POLICY, SUMMARY OF WHICH IS ATTACHED HERETO AS EXHIBIT F.

9. MISCELLANEOUS

9.1 If any provision of this Agreement is found to be unenforceable or invalid, that provision will be limited or eliminated to the minimum extent necessary so that this Agreement will otherwise remain in full force and effect and enforceable.

9.2 This Agreement shall inure to the benefit of and be binding upon the Parties and their respective successors and permitted assigns. Neither Party shall assign this Agreement or any of its rights or obligations hereunder without the prior written consent of the other Party.

9.3 This Agreement is the complete and exclusive statement of the mutual understanding of the parties and supersedes and cancels all previous written and oral agreements, communications and other understandings relating to the subject matter of this Agreement, and that all waivers and modifications must be in a writing signed by both parties, except as otherwise provided herein.

9.4 No agency, partnership, joint venture, or employment is created as a result of this Agreement and Customer does not have any authority of any kind to bind Company in any respect whatsoever.

9.5 All notices under this Agreement will be in writing and will be deemed to have been duly given when received, if personally delivered; when receipt is electronically confirmed, if transmitted by facsimile or e-mail; the day after it is sent, if sent for next day delivery by recognized overnight delivery service; and upon receipt, if sent by certified or registered mail, return receipt requested.

9.6 This Agreement shall be governed by the laws of the State of Missouri and/or the laws of the United States, as applicable. The venue for all litigation arising out of, or relating to this contract document, shall be in Boone County, Missouri, or the United States Western District of Missouri. The Parties hereto irrevocably agree to submit to the exclusive jurisdiction of such courts in the State of Missouri. The Parties agree to waive any defense of forum non conveniens.

9.7 No Third-Party Beneficiary. No provision of the Agreement is intended to nor shall it in any way inure to the benefit of any other third party, so as to constitute any such Person a third-party beneficiary under the Agreement.

9.8 **Amendment.** No amendment, addition to, or modification of any provision hereof shall be binding upon the Parties, and neither Party shall be deemed to have waived any provision or any remedy available to

it unless such amendment, addition, modification or waiver is in writing and signed by a duly authorized officer or representative of the applicable Party or Parties.

9.9 General Laws. Company shall comply with all federal, state, and local laws, rules, regulations, and ordinances.

9.10 Employment of Unauthorized Aliens Prohibited. Company shall comply with Missouri State Statute Section 285.530 in that Company shall not knowingly employ, hire for employment, or continue to employ an unauthorized alien to perform work within the State of Missouri. As a condition for the award of this contract, Company shall, by sworn affidavit and provision of documentation, affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services. Company shall also sign an affidavit affirming that it does not knowingly employ any person who is an unauthorized alien in connection with the contracted services. Company shall require each subcontractor to affirmatively state in its contract with Company that the subcontractor shall not knowingly employ, hire for employment or continue to employ an unauthorized alien to perform work within the State of Missouri. Company shall also require each subcontractor to provide Company with a sworn affidavit under the penalty of perjury attesting to the fact that the subcontractor's employees are lawfully present in the United States.

9.11 Nature of Customer's Obligations. All obligations of the Customer under this Agreement, which require the expenditure of funds, are conditional upon the availability of funds budgeted and appropriated for that purpose.

9.12 No Waiver of Immunities. In no event shall the language of this Agreement constitute or be construed as a waiver or limitation for either party's rights or defenses with regard to each party's applicable sovereign, governmental, or official immunities and protections as provided by federal and state constitutions or laws.

9.13 Company shall maintain, on a primary basis and at its sole expense, at all times during the life of

the Agreement the following insurance coverages, limits, including endorsements described herein. The requirements contained herein, as well as the Customer's review or acceptance of insurance maintained by Company is not intended to, and shall not in any manner limit or qualify the liabilities or obligations assumed by Company under the Agreement. Coverage to be provided as follows by a carrier with A.M. Best minimum rating of A- VIII.

- a. Workers' Compensation & Employers Liability. Company shall maintain Workers' Compensation in accordance with Missouri State Statutes or provide evidence of monopolistic state coverage. Employers Liability with the following limits: \$500,000 for each accident, \$500,000 for each disease for each employee, and \$500,000 disease policy limit.
- b. Commercial General Liability. Company shall maintain Commercial General Liability at a limit of not less than \$1,000,000 Each Occurrence, \$2,000,000 Annual Aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations, Contractual Liability or Cross Liability.
- c. Business Auto Liability. Company shall maintain Business Automobile Liability at a limit not less than \$1,000,000 Each Occurrence. Coverage shall include liability for Owned, Non-Owned & Hired automobiles. In the event Company does not own automobiles, Company agrees to maintain coverage for Hired & Non-Owned Auto Liability, which may be satisfied by way of endorsement to the Commercial General Liability policy or separate Business Auto Liability policy.
- d. Company may satisfy the minimum liability limits required for Commercial General Liability or Business Auto Liability under an Umbrella or Excess Liability policy. There is

no minimum per occurrence limit of liability under the Umbrella or Excess Liability; however, the Annual Aggregate limit shall not be less than the highest "Each Occurrence" limit for either Commercial General Liability or Business Auto Liability. Company agrees to endorse the Customer as an Additional Insured on the Umbrella or Excess Liability, unless the Certificate of Insurance state the Umbrella or Excess Liability provides coverage on a "Follow-Form" basis.

- e. The Customer of Columbia, its elected officials and employees are to be Additional Insured with respect to the project to which these insurance requirements pertain. A certificate of insurance evidencing all coverage required is to be provided at least 10 days prior to the Effective Date of the Agreement between the Company and the Customer. Company is required to maintain coverages as stated and required to notify the Customer of a Carrier Change or cancellation within two (2) business days. The Customer reserves the right to request a copy of the policy.
- f. The Parties hereto understand and agree that the Customer is relying on, and does not waive or intend to waive by any provision of this Agreement, any monetary limitations or any other rights, immunities, and protections provided by the State of Missouri, as from time to time amended, or otherwise available to the Customer, or its elected officials or employees.
- g. Failure to maintain the required insurance in force may be cause for termination of the Agreement. In the event Company fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the Customer shall have the right to cancel and terminate the Agreement

without notice.

- h. The insurance required by the provisions of this article is required in the public interest and the Customer does not assume any liability for acts of the Company and/or their employees and/or their subcontractors in the performance of this Agreement.

8.14 Contract Documents. This Agreement includes the following exhibits, which are incorporated herein by reference:

Exhibit	Description
A	Services Statement of Work
B	Service Level Terms
C	Implementation Services Statement of Work
D	Per User Pricing
E	Performance Requirements
F	Company's Insurance Policy Summary
G	City's Red Flag Policy

In the event of a conflict between the terms of an exhibit and the terms of this Agreement, the terms of this Agreement controls.

[SIGNATURE PAGE FOLLOWS]

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized officials and officers on the day and year written below.

CITY OF COLUMBIA, MISSOURI

By: _____
Mike Matthes, City Manager

Date: _____

ATTEST:

By: _____
Sheela Amin, City Clerk

APPROVED AS TO FORM:

By: _____
Nancy Thompson, City Counselor

BENEVATE, INC.

By: g. gordon Russek

Date: 10/25/17

ATTEST:

By: Karlee Young
Name: Karlee Young

EXHIBIT A

Services Statement of Work

1. SaaS Services Description. Company will provide Customer with hosted software for the enrollment, qualification, administration and reporting of the following programs:
 - a. Grant Management
 - b. Property Acquisition/Demolition
 - c. Owner-Occupied Rehabilitation Program
 - d. Minor Home Repair
 - e. Down Payment Assistance Program
 - f. Columbia Community Land Trust Homeowners

Company will make available to Customer all updates, and any documentation for such updates, to the Services. Company will ensure that (i) new features or enhancements to existing features are synchronized with the previous version, and (ii) updates will not degrade the performance, functionality, or operation of the Services.

2. Training Services. Company will conduct one (1) four (4) hour training session, which may be recorded by Customer. The purpose of the training sessions is to familiarize administrator personnel with the workflow and functionality of hosted software.
3. Technical Support. Company will provide Technical Support to Customer via electronic mail on weekdays during the hours of 9:00 am through 5:00 pm Eastern time, with the exclusion of Federal Holidays (“Support Hours”). Customer may initiate a helpdesk ticket during Support Hours by emailing support@neighborlysoftware.com. Company will use commercially reasonable efforts to respond to all Helpdesk tickets within one (1) business day.
4. Data Storage. Company affirms that any and all Customer data will be stored, processed, and maintained solely in data centers located in the United States.
5. Backup and Recovery of Customer Data. As a part of the Services, Company is responsible for maintaining a backup of Customer Data and for an orderly and timely recovery of such data in the event that the Services may be interrupted. Company shall maintain a contemporaneous backup of Customer Data that can be recovered within four (4) hours at any point in time.
6. Loss of Data. In the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Customer Data or the physical, technical, administrative, or organizational safeguards put in place by Company that relate to the protection of the security, confidentiality, or integrity of Customer Data, Company shall, as applicable: (a) notify Customer as soon as practicable but no later than twenty-four (24) hours of becoming aware of such occurrence; (b) cooperate with Customer in investigating the occurrence, including making available all relevant records, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by Customer; (c) in the case of PII, at Customer’s sole election, (i) notify the affected individuals who comprise the PII as soon as practicable but no later than is required to comply with applicable law, or, in the absence of any legally required notification period, within five (5) calendar days of the occurrence; (d) in the case of PII, provide third-party credit and identity monitoring services to each of the affected individuals who comprise the PII for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for six (6) months following the date of notification to such individuals; (e) perform or take any other actions required to comply with applicable law as a result of the occurrence; Notification to affected individuals, as described above, shall comply with applicable law, be written in plain language, and contain, at a minimum: name and contact information of Company’s representative; a description of the nature of the loss; a list of the types of data involved; the known or approximate date of the loss; how such loss may affect the affected individual; what steps Company has taken to protect the affected individual; what steps the affected individual can take to protect himself or herself; contact information for major credit card reporting agencies; and, information regarding the credit and identity monitoring services to be provided by Company. This Section shall survive the termination of this Agreement.

EXHIBIT B

Service Level Terms

The Services shall be available 99.5%, measured monthly, excluding holidays and scheduled downtime. Further, any downtime resulting from outages of third party connections or utilities or other reasons beyond Company's control will also be excluded from any such calculation.

1) Definitions.

(a) "Actual Uptime" shall mean the total minutes in the reporting month that the Services were actually available for normal use.

(b) "Maintenance Window" shall mean the total minutes in the reporting month represented by the following day(s) and time(s) during which Service Provider shall maintain the Services: Tuesday, Thursday, Saturday 11pm-3am ET.

(c) "Scheduled Downtime" shall mean the total minutes in the reporting month represented by the Maintenance Window.

(d) "Scheduled Uptime" shall mean the total minutes in the reporting month less the total minutes represented by the Scheduled Downtime.

2) Calculation. $(\text{Actual Uptime} / \text{Scheduled Uptime}) * 100 = \text{Percentage Uptime}$ (as calculated by rounding to the second decimal point)

3) Performance Credit. Performance credits may not be redeemed for cash and will only apply a credit to the month in which the incident occurred. Company shall apply the credits to Customer's next payment.

(a) Where Percentage Uptime is equal to or greater than 99.5%, no Performance Credit will be due to Customer.

(b) Where Percentage Uptime is less than 99.5%, Customer shall be due a Performance Credit in the amount of 5% of the Services Fees (as calculated on a monthly basis for the reporting month)

EXHIBIT C

Implementation Services Statement of Work

This Implementation Services Statement of Work describes the Services to be performed, and Deliverables to be provided, by Company in completion and satisfaction of the Implementation Services.

- 1) **Company Key Roles.** Company will assign an Engagement Manager who will be Customer's primary contact person and who will coordinate all the activities of the Implementation team.
- 2) **Customer Key Roles.** Customer will assign a person to be the focal point to coordinate the user and technical support and resources needed for the implementation, and to be responsible for approvals and decisions. This person will coordinate data collection and reconciliation, review each stage of the implementation process, and provide end user involvement with systems and user acceptance training. Schedule and cost estimates assume that personnel acting in the roles noted above to be reasonably and readily available to the Company team as needed throughout the project. Additionally, all approvals and decisions are made within a reasonable time period.
- 3) **Implementation Steps.** The following are the general steps which make up the implementation process:
 - Kickoff meeting
 - Program Design and Documentation
 - System Configuration and Signoff
 - Data Review and Validation
 - Administrator Training
 - Historical Data Collection (if applicable)
- 4) **Implementation Deliverables.** The following are the items that will be delivered as part of implementation:
 - a. Program Design and Documentation
 - List of all documents to be uploaded into the system as part of the Program
 - List of all documents to be generated by the system as part of the Program
 - b. System Configuration
 - Create Administrator accounts in the system
 - Configure Customer enrollment application in the system
 - Configure Customer specific approvals and workflow in the system, including up to thirty (30) documents/images to be uploaded
 - Configure up to (15) program documents to be generated by system
 - c. Data Review and Validation
 - Provide up to five (5) business days for Customer to test and validate system data and configuration
 - d. Administrator Training
 - Conduct one (1) four (4) hour training session, which may be recorded by Customer.
 - e. Historical data conversion
 - Upload up to five (5) years of Customer historical data, to be provided by Customer in an electronic format specified by Company
- 5) **Customer Responsibilities**
 - a. Design and approve data elements, program workflow, and eligibility criteria
 - b. Identify all program documents required to be stored in the system
 - c. Identify all program documents to be generated by the system
 - d. Provide historical data in electronic format specified by Company
 - e. Test and approve system configuration
 - f. Provide final sign off that the system meets all requirements ("Go Live")
 - g. Participate in administrator training session

EXHIBIT D

Per User Pricing

Additional user licenses may be purchased, pro-rata to the Initial Service Term, based on the pricing table below. For purposes of licensing, a user is defined as an employee of Customer who uses the software and services of Company. Customer's applicants and other users of the software and services do not require licenses.

Per User Description	Number of User Licenses included in Order Form	Per User Per Month Pricing
1. Full User License – Ability to create and edit data records, run reports, and generate program documents.	4	\$135.00

Item #	Application Requirements	Pri r ty	Vendor Offers	Included or @ Add'l Cost (please list)	Comments
Conversions: Expectation of moving current data to new software					
	Format type-Excel Spreadsheet-Entire loan module				
	Can software easily accomodate an excel upload of data?				
	If customizable fields are used can data be converted through and upload or import process?				
Data: Expectations of how you plan to use the data and data types					
	Customizable fields to City application and workflow processes of the following programs: Rehabilitation, Minor Home Repair, Homebuyer Assistance, Acquisition/Demolition, CCLT, Subgrantees and RFP Process.				
	Fields should match with attached Housing Programs Application, Acquisition Demolition Application and annual RFP.				
	The ability to input all participant demogrpahic data, grant/funding source and expenditure data by program.				
Users and licensing: How many administrators, users and gra t recipie ts wil eed software					
	Four City Users - login and ability to access software from any device (mobile, ipad, laptop, desk top)-Yes.				
	Cost per City user: \$135/month				
	\$0 dollar cost for program applicants and organizations submitting a a proposal through the City's annual RFP process.				
Reports:					
	Need Expenditure Report: 1) Amount expended by grant/fund source, program and activity. 2) Demographic Report: demographic data of households served by activity and program including income (0-30% AMI, 30-50% AMI, 50-80% AMI, <80% AMI), race and ethnicity.				
Implementation:					
	Expectation of implementation: Be fully live within 60 days of approval to move forward including staff training, data conversion and user access.				
Training:					
	Expection of training: Online training of examples projects for each of the program areas, followed by onsite training with similar objective. On-site training of lenders on utilizing the system as an applicant.				

	<p>On-site training fo lenders: 1-hour training session for local lenders participating in Homebuyer Assistance Program. Training should ensure that local lenders understand how to access the system, enter data, upload documents and submit a completed applicaiton on behalf of the participant.</p>					
Timing:						
	<p>Within 60 days of Council approval to proceed.</p>					



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY)

10/24/2017

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER FounderShield, LLC 119 W 24th St, 3rd Floor New York, NY, 10010		CONTACT NAME: PHONE (A/C, No, Ext) 646-854-1058 FAX (A/C, No) E-MAIL ADDRESS: coi@foundershield.com	
INSURED Benevate 3423 Piedmont Rd NE - Suite 373 atlanta, Georgia, 30305		INSURER(S) AFFORDING COVERAGE	
		INSURER A: TWIN CITY FIRE INSURANCE CO	NAIC # 29459
		INSURER B: ACE FIRE UNDERWRITERS INS CO	20702
		INSURER C:	
		INSURER D:	
		INSURER E:	
		INSURER F:	

COVERAGES **CERTIFICATE NUMBER:** **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	LIMITS
A	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input type="checkbox"/> POLICY <input type="checkbox"/> PROJECT <input checked="" type="checkbox"/> LOC <input type="checkbox"/> OTHER:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	10SBMIS4695	01/18/2017	01/18/2018	EACH OCCURRENCE \$1,000,000.00
			DAMAGE TO RENTED PREMISES (Ea occurrence) \$1,000,000.00				
			MED EXP (Any one person) \$10,000.00				
			PERSONAL & ADV INJURY \$1,000,000.00				
			GENERAL AGGREGATE \$2,000,000.00				
			PRODUCTS - COMP/OP AGG \$2,000,000.00				
A	<input type="checkbox"/> AUTOMOBILE LIABILITY <input type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS <input checked="" type="checkbox"/> HIRED AUTOS <input type="checkbox"/> SCHEDULED AUTOS <input checked="" type="checkbox"/> NON-OWNED AUTOS	<input type="checkbox"/>	<input type="checkbox"/>	10SBMIS4695	01/18/2017	01/18/2018	COMBINED SINGLE LIMIT (Ea accident)
			BODILY INJURY (Per person)				
			BODILY INJURY (Per accident)				
			PROPERTY DAMAGE (Per accident)				
		Hired & Non Owned Auto \$1,000,000.00					
	<input type="checkbox"/> UMBRELLA LIAB <input type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE <input type="checkbox"/> DED <input type="checkbox"/> RETENTION	<input type="checkbox"/>	<input type="checkbox"/>				EACH OCCURRENCE
							AGGREGATE
	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR/PARTNER/EXECUTIVE OFFICER/MEMBER EXCLUDED? (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	<input type="checkbox"/>	<input type="checkbox"/>				<input type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER
		N/A					E.L. EACH ACCIDENT
							E.L. DISEASE - EA EMPLOYEE
							E.L. DISEASE - POLICY LIMIT
B	Cyber Liability, Errors & Omissions	<input type="checkbox"/>	<input type="checkbox"/>	EONGAF113209712	01/18/2017	01/18/2018	\$1,000,000.00 per occ \$1,000,000.00 in agg

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

The Certificate Holder is included as an Additional Insured on the above referenced policy as required by written contract.

CERTIFICATE HOLDER

**City of Columbia, Missouri
701 E Broadway
Columbia, MO 65201**

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Red Flag Rule

City of Columbia Identity Theft Prevention Program

Effective December, 2010

City Council Adopted and Effective Date: _____

This document is intended to give guidance to the City in their understanding of the FTC Red Flag Rule. It is not intended to be used in place of compliance, in whole or any part, of the FTC Rule.

08/02/10 Final

11/10/10 Reviewed/Updated

Table of Contents

	Pages
Introduction.....	3-4
Identification of Red Flags.....	5-8
Detection of Red Flags.....	9
Preventing and Mitigating Identity Theft.....	10-11
Updating the Program and the Red Flags.....	12
Program Administration and Training.....	13

Appendix A	Finance Department Internal Identity Theft Policies.....	14-19
Appendix B	Parks & Recreation Department Internal Identity Theft Policy.....	20
Appendix C	Information Systems Department Internal Identity Theft Policy.....	21-26
Appendix D	Law Enforcement Identity Theft Notification Steps.....	27-30
Appendix E	Identity Theft Training Protocol.....	31
Appendix F	Needs Assessment	32-36

INTRODUCTION

The City of Columbia (the "City") has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's ("FTC") Red Flag Rule, which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. §681.2. This Program is designed to detect, prevent and mitigate identity theft not only in connection with the opening and maintenance of City utility accounts but other city accounts, applications, registrations or other transactions, referred to as "Record" or "Records" throughout this Program, where identity theft might occur.

Why did FTC make this rule?

The intent is to protect consumers from identity theft. It is targeted at entities that **obtain** and **hold** consumer identification such as billing addresses, Social Security Numbers, dates of birth, passports or immigration documents, or other information.

Who must comply?

Entities such as Columbia that obtain and hold identification often targeted by identity thieves must comply.

What is a "Red Flag?"

A "Red Flag" is a term the FTC has coined to identify possible identity theft. It is a pattern or particular specific activity that indicates the possible risk of identity theft. The FTC has identified thirty-one "Red Flags" that entities, especially utilities, should watch for. Such entities are required to have a written plan to help employees identify these "Red Flags" and how to respond when a possible identity theft has occurred.

How does Columbia have to comply with this rule?

We have a duty to:

1. Identity Red Flags
2. Detect Red Flags; and
3. Respond to Red Flags

Who within City operations has to comply with the rule?

All City Departments which obtain and hold any of the consumer identification mentioned above must comply with the rule.

For purposes of this Program, "Identity Theft" is considered to be "fraud committed using the identifying information of another person." The Program "Record" is defined as:

1. A continuing relationship the City has with an individual through a Record the City offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and
2. Any other account, registration, application or record the City offers or maintains for which there is a reasonable foreseeable risk to customers or to the safety and soundness of the City from Identify Theft

This Program was developed with oversight and approval of the Columbia City Council. After consideration of the size and complexity of the City's operations and various systems, and the nature and scope of these activities, the Columbia City Council determined that this Program was appropriate for the City and therefore approved this Program on December 15, 2008.

The Red Flag Rule-City of Columbia Identity Theft Prevention Program was reviewed and amended December, 2010.

IDENTIFICATION OF RED FLAGS

A “Red Flag” is a pattern, practice, or specific activity that indicates the possible existence of Identity Theft. In order to identify relevant Red Flags, the City of Columbia considered risk factors such as the types of Records it offers and maintains, the methods it provides to open or establish these Records, the methods it provides to access its Records, and its previous experiences with Identity Theft. The City identified the following Red Flags in each of the listed Categories:

1. Notifications and Warnings from Consumer Reporting Agencies

- 1) A fraud or activity alert that is included with a consumer report;
- 2) Receiving a report or notice from a consumer reporting agency of a credit freeze;
- 3) Receiving a report of fraud with a consumer report; and
- 4) Receiving indication from a consumer report of activity that is inconsistent with a customer’s usual pattern or activity.

2. Suspicious Documents (see below) used in such a way (items 1-13)

- Lease
 - Death certificate
 - Driver’s license
 - Immigration Papers or Work Card
 - Passport
 - Birth certificate
 - Student Identifications
 - Government Issued Identification
 - Military Identification
 - Non-Driver’s License Identification
 - Credit and Debit Cards
- 1) Receiving documents that are provided for identification that appear to be forged or altered;
 - 2) Receiving documentation on which a person’s photograph or physical description is not consistent with the person presenting the documentation;
 - 3) Receiving other information on the identification not consistent with information provided by the person opening a new Record or customer presenting the identification;

- 4) Receiving other documentation with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged);
- 5) Receiving an application for service that appears to have been altered, forged or gives the appearance of having been destroyed and reassembled;
- 6) Personal identifying information provided is inconsistent when compared against external information sources used by the Department (such as the address does not match any address in the Consumer Report or the Social Security Number has not been issued, or is listed on the Social Security Death's Master File);
- 7) Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal knowledge and/or external third party sources (telephone number or address on an application is the same as the telephone number or address provided on a fraudulent application);
- 8) Receiving verbal, written, or internet based information where the same person with the same billing information requests utility service at more than one location;
- 9) The Social Security Number provided is the same as that submitted by other person(s) opening a Record;
- 10) The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening Records;
- 11) The person opening a Record fails to provide all required personal identifying information (incomplete application);
- 12) The person opening a Record cannot provide authenticating information if requested to do so;
- 13) The Department is notified by a customer (s) with information that another customer may have opened a fraudulent Record.

3. Suspicious Personal Identifying Information

- 1) A person's identifying information is inconsistent with other sources of information (such as an address not matching an address on a Consumer Report or a Social Security Number that was never issued);
- 2) A person's identifying information is inconsistent with other information the customer provides (such as inconsistent Social Security Numbers, billing addresses or birth dates);

- 3) A person's identifying information is the same as shown on other applications found to be fraudulent;
- 4) A person's identifying information is consistent with fraudulent activity (such as an invalid phone number or a fictitious billing address);
- 5) A person's Social Security Number is the same as another customer's Social Security Number;
- 6) A person's address or phone number is the same as that of another person;
- 7) A person fails to provide complete personal identifying information on an application when reminded to do so; and
- 8) A person's identifying information is not consistent with the information that is on file for the customer.
- 9) The physical appearance of a customer does not match with other sources of information (such as driver's license, passport or immigration work card).
- 10) A person does not know the last 4 digits of his/her Social Security Number.
- 11) A new customer requests new service and a routine Social Security Number check locates an account with delinquent or a collection balance that is proved not to be the responsibility of the customer requesting new service.

4. Unusual Use Of or Suspicious Activity Related to a Record

- 1) A change of address for a Record followed by a request to change the Record holder's name or add other parties;
- 2) A new Record used in a manner consistent with fraud (such as the customer failing to make the first payment, or making the initial payment and no other payments);
- 3) A Record being used in a way that is not consistent with prior use (such as late or no payments when the Record has been timely in the past);
- 4) Mail sent to the Record holder is repeatedly returned as undeliverable;

- 5) The Department receives notice that a customer is not receiving his paper statements; and
- 6) The Department receives notice that a Record has unauthorized activity.
- 7) A Record is designated for shut-off due to non-payment and the customer at the location does not match the customer on file.
- 8) Unauthorized access to or use of customer records information such as log on or authentication failures.

5. Notice Regarding Possible Identity Theft

The City receives notice from a customer, an identity theft victim, law enforcement or any other person that it has opened or is maintaining a fraudulent Account for a person engaged in Identity Theft.

DETECTION OF RED FLAGS.

1. In order to detect any of the Red Flags identified above with the opening of a new Record, City personnel will take the following steps and verify the identity of the person opening the Record:

- 1) Requiring certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, Social Security Number, driver's license or other identification;
- 2) Verifying the customer's identity in person, such as by copying and reviewing a driver's license or other identification card;
- 3) Reviewing documentation showing the existence of a business entity (in person process);
- 4) Independently contacting the customer; and
- 5) Requesting the customer to appear in person with appropriate information or documentation.

2. In order to detect any of the Red Flags identified above for an existing Record, City personnel will take the following steps to monitor transactions with such information:

- 1) Verifying the identification of customers if they request information (in person, via telephone, via facsimile, via email);
- 2) Verifying the validity of requests to change billing addresses;
- 3) Verifying changes in banking information given for billing and payment purposes; and
- 4) Verifying the last 4 digits of his/her Social Security Number.

PREVENTING AND MITIGATING IDENTITY THEFT

1. In the event City personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending on the degree of risk posed by the Red Flag:

- 1) Continuing to monitor a Record for evidence of Identity Theft;
- 2) Person who may be or is suspected to be the possible victim of identity theft;
- 3) Changing any passwords or other security devices that permit access to Records;
- 4) Reopening a Record with a new number;
- 5) Not opening a new Record;
- 6) Closing an existing Record;
- 7) Notifying law enforcement; See **Appendix D**.

Example: If the City receives notice that its system has been compromised such that a customer's personal information has become accessible, at a minimum the City will notify the customer and change passwords.

Example: If the City receives notice that a person has provided inaccurate identification information, the Record will be closed immediately and notify Law Enforcement.

- 8) Determining that no response is warranted under the particular circumstances; or

Example: If the City notices late payments on a Record regularly paid and determines the resident has been incapacitated, no action may be necessary.

- 9) Notifying the Program Administrator for determination of the appropriate step (s) to take.

2. In order to further prevent the likelihood of identity theft occurring with respect to Records the City will take the following steps with respect to its internal operating procedures:

- 1) Providing a secure website or clear notice that a website is not secure;

- 2) Ensuring complete and secure destruction of paper documents and computer files containing customer information. Paper documents and computer files containing customer information should be retained for the minimum retention required by law, unless there is a significant business purpose to retain the record for a longer period of time.
- 3) Requiring certain provisions included in city contracts with vendors. If the storage or destruction of paper documents and computer files are contracted to a private vendor, contracts must include a provision that requires the private vendor to store the documents and files in a secure manner so as to be accessible only by approved city personnel. Upon appropriate authorization by an approved city official, the vendor shall destroy the documents and computer files in a secure fashion. The storage and destruction of paper documents and computer files which contain sensitive information must be performed by either a city employee or a private vendor under contract.
- 4) Ensuring that office computers are password protected and that computer screens lock after a set period of time;
- 5) Requiring only the last 4 digits of Social Security Numbers on customer Records;
- 6) Requiring each Department review, no less than once a year, employee's access to Record information to determine if the employee's duties require such access and if the employee is complying with the provisions of the City Identity Theft Prevention Program. The Department shall restrict access as much as feasible and maintain an up to date list of those employees required to have access along with the date access was last reviewed. If the employee's access involves computer files, access shall be documented in the City Security Tracking System.
- 7) Prohibiting Record information to be written on sticky pads or note pads;
- 8) Ensuring that computer screens are only visible to the employee accessing the Record;
- 9) Requiring customers to authenticate addresses and personal information, rather than account representatives asking if the information is correct;
- 10) Maintaining secure office location;
- 11) Maintaining cameras in timely and good working order and providing for property destruction of tapes and other recording media;
- 12) Periodically (each Department) reviewing and maintaining a complete, accurate, and current internal list of authorized personnel and procedures with respect to the appropriate responses should a red flag occur or should the Department be aware of actual identity theft. Each Department with

access to such records shall provide periodic reports to the Red Flag Committee and Program Administrator. The report shall include red flags they have detected, their response, and any recommendations for changes in their Department internal policies and procedures and the City Identity Theft Prevention Program.

- 13) Should vendors have access to personal identifying information, Departments shall also include in contracts with vendors provisions for either the reporting of red flags to the Department or to require the vendor to prevent and mitigate the crime themselves. If the contract provides for the vendor to prevent and mitigate, the contract should also include a provision for periodic reports about the Red Flags the vendor detected and their response.
- 14) Each city department involved in the opening of new Records or maintenance of existing Records: Utility Customer Services, Parks and Recreation, and Information Systems shall maintain a complete, accurate, and current internal list of authorized personnel with respect to the appropriate responses in the event of a Red Flag occurring, having occurred or an actual Identity Theft; and
- 14) Because the City cannot predict all particular circumstances that may arise, City Personnel are requested to be diligent while not compromising customer service in the detection of other possible Red Flags.

UPDATING THE PROGRAM AND THE RED FLAGS

- 1) This Program will be reviewed and updated annually, or as needed, to reflect changes in risks to customers and the soundness of City Records from Identity Theft. An Assistant City Manager will be designated the Program Administrator and work with the **Red Flag Committee**, an internal City working group to consider the City's experiences with Identity Theft, changes in Identity Theft methods, changes in Identity Theft detection and prevention methods, changes in types of Records, and changes in the City's business arrangements with other entities. To do so, the Red Flag Committee and Program Administrator shall evaluate the effectiveness of the City Identity Theft Prevention Program, effectiveness of the monitoring of the practices of service providers, and will analyze significant incidents of identity theft and city response.
- 2) After considering these factors and recommendations from the Committee, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted. If warranted, the Program Administrator will present the Program and recommended changes to the City Council who will make a determination of whether to accept, modify or reject those changes to the Program.
- 3) **Note: Each City Department included in the Program shall conduct an annual Needs Assessment to ensure that their operation is current in identifying Red Flags and response protocol. See Appendix F.**

PROGRAM ADMINISTRATION AND TRAINING

1. Oversight.

The City's Program will be overseen by an Assistant City Manager and the Red Flag Committee. Committee members shall consist of the representatives of the City Manager's Office, and all other city Departments that obtain and hold personal identifying information. The Program Administrator will be responsible for the Program's administration, for ensuring appropriate training of staff on the Program, for reviewing any staff reports regarding the detection of Red Flags and the steps for preventing and mitigating Identity Theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and, if necessary, approving changes to the Program.

2. Staff Training and Reports.

City staff responsible for implementing the Program shall be trained under the direction of the Program Administrator, the appropriate Department Head, the Police Department and/or a combination of the above in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected. **See Appendix E.** Such training will be sufficient to effectively implement the Program. All training shall be conducted annually and documented. Vendors are required to either report any red flags to the Program Administrator or respond appropriately to prevent and mitigate the crime themselves.

3. Service Provider Arrangements.

The City will take the following steps to ensure the service provider performs its activity in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft.

- 1) Requiring, by contract, that service providers have such policies and procedures in place;
- 2) Requiring, by contract, that service providers review the City's Program and report any Red Flags to the Program Administrator; and,
- 3) Each Department is required to maintain an up-to-date written internal policy as it pertains to their internal security and identity theft.



Patricia Bollmann, Manager
City of Columbia, Utilities and Billing
PO Box 1676
Columbia MO 65205-1676
Phone 573-874-7458
Fax 573-874-7763
E-Mail PAB@gocolumbiamo.com

Appendix A

Finance Department Internal Identity Theft Policy Utility Customer Services Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Ordinance

POLICY: Any person or agency requesting information regarding a customer's account must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Customers must identify themselves by the last 4 digits of their SS# before any information may be given on their account. If they can not give the last 4 digits of their SS# no information can be given.

- Telephone requests from the public for phone or social security numbers are always declined
- Persons requesting any information of a personal nature must come in person with picture ID and speak to the Manager/Supervisor.
- Faxed requests for personal information are not acceptable.
- For Realtors or prospective tenants/new homeowners it is acceptable to give information regarding high and low or average utility bills. It is not acceptable to disseminate any personal information in the notes, master file, or payment history.
- Requests for billing information from the file should only be given to the spouse, the significant other, or roommates listed in the master file or notes after they have provided the correct Social Security as verification.
- Governmental agencies; police or prosecutors requesting information should properly identify themselves. These calls should be handled by the Manager or Supervisor or the Collection staff.
- Any discussion of the details of customer's accounts outside of the office is never acceptable for any reason.
- When there is a confidential flag on an account, follow the instructions on the notes

Customer information on master file is password protected.

- Customers are not allowed in CSR Area
- Customer payment agreements are kept in the secure area.
- No paper documents may be left on desks



Janice W. Finley, Business Services Administrator
City of Columbia, Business License Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7747
Fax: 573-874-7761
E-Mail: Janice@GoColumbiaMo.com

Appendix A (cont'd)

Finance Department Internal Identity Theft Policy

Business License Division

Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code-4 of Ordinances

POLICY: Any person or agency requesting information regarding a business license customer's confidential information in their license file must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

Identification of Red Flags

- Mail sent to the license applicant is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the license applicant.
- Receiving information from American DataBank Inc., the company that provides criminal background check services, concerning the inconsistency of a social security number and date of birth of a license applicant.
- The license applicant fails to provide the required personal identifying information (incomplete application).
- Receiving verbal or written information concerning an applicant submitting fraudulent documents.
- Applicant's driver's license photo is inconsistent with the person presenting the documentation.

- Owner of company listed on license application inconsistent with the Missouri Secretary of State records.

Detection of Red Flags

- Require identifying information from all license applicants.
- Verify the applicant's identity in person.
- Review documentation showing the existence of a business entity.
- Verify the identity of applicants, if they request information.

Preventing and Mitigating Identity Theft

- American Databank, Inc. monitors identifying information for inconsistencies in social security number, name, date of birth, and relays this information to the Business License Office.
- The invoices received from American Databank include only the last four digits of the applicants' social security number.
- Applicants' social security number and business gross receipts information are always deleted/blacked out on documents requested from a licensee's file.
- Social security and gross receipts information are never released unless requested by the applicant in person upon providing identification.
- Requests for confidential licensing information from City Police Department staff, Law Department staff, representatives from governmental agencies, etc., are required to obtain this information from the Business Services Administrator after providing identification.
- Inactive business license files are stored in a locked area.
- All Business License staff computers are password protected.
- Computer screens are only visible to the Business License employee when accessing licensing records.
- File cabinets that contain business license records, as well as hotel/motel and cigarette tax records, are locked at the end of each business day. The Business License area is never left unattended during office hours and access to this area is restricted to Business License staff and management.

- Always obtain copy of applicant's driver's license or other picture ID when applying for a license or permit.
- Check immigration papers to ensure validity.
- If an applicant fails to provide the requested personal identifying information, the license or permit application is denied.
- The appearance of altered or forged documents prompts further investigation.
- Double check with Missouri Secretary of State's Office to confirm members of a corporation are consistent with those listed on the application.
- Obtain criminal background check from previous state in which the applicant resided if the applicant has lived in Missouri for less than one year.
- Computer screen darkens or fades out when staff is away from their desks.
- The Business Services Administrator is the only person who can grant access to the business license system.

Ron Barrett, Comptroller
City of Columbia, Accounting Division
PO Box 6015
Columbia MO 65205
Phone: 573-874-7371
Fax: 573-874-7686
E-Mail: Ron@GoColumbiaMo.com



Appendix A (cont'd)

Finance Department Internal Identity Theft Policy

Miscellaneous Receivables Accounting Division

Effective October 25, 2008

PURPOSE: Establish guidelines consistent with City of Columbia Code of Ordinances

POLICY: Any person or agency requesting information regarding a miscellaneous receivables customer's confidential information in their miscellaneous receivables file must have a demonstrated right to know

PROCEDURE:

Identification of Red Flags

- Mail sent to the miscellaneous receivable customer is repeatedly returned as undeliverable.
- Suspicious immigration papers, criminal background check documents and other identification documents that appear to be forged/altered or are not consistent with information provided by the miscellaneous receivable customer.
- Receiving verbal or written information concerning a miscellaneous receivable customer submitting fraudulent documents.
- Owner of company listed on miscellaneous receivable customer inconsistent with the MO Secretary of State records.

Detection of Red Flags

- Review documentation showing the existence of a business entity.
- Verify the identity of miscellaneous receivable customer if they request information.

Preventing and Mitigating Identity Theft

- Social security numbers are never requested, used, or stored, in the miscellaneous receivable customer information system
- Requests for confidential miscellaneous receivable customer information files are provided only to city staff that are working with the miscellaneous receivable customer information as required for their department
- Customers' bank account information which is stored in the miscellaneous receivable system is maintained in a secure manner. This information is not disclosed to parties outside the miscellaneous receivable system staff.
- Inactive miscellaneous receivable customer files are stored in a locked area.
- All miscellaneous receivable customer system records are password protected.
- The appearance of altered or forged documents prompts further investigation.
- Computer screen darkens or fades out when miscellaneous receivable staff is away from their desk.
- The Accounting Assistant for miscellaneous receivables is designated as the only person who can grant access to the miscellaneous receivable system

APPENDIX B

Parks and Recreation Records Internal Identity Theft Policy Effective October 20, 2008

PURPOSE: Establish guidelines consistent with the City of Columbia's Identity Theft Prevention Program.

POLICY: Any person or agency requesting information regarding customer's personal information must have a demonstrated right to know and present themselves in person with the proper identification.

PROCEDURE:

- All credit card and ACH banking information stored in RecTrac database is encrypted throughout the database and cannot be obtained by any user or staff.
- WebTrac (online registration) user name and passwords are set by customer. If customer forgets this information, they must know their security features they set up in order to access such information.
- E-mail and phone requests requesting customer's PIN # for online registration must confirm their mailing address, phone number and security features.
- Faxed requests are not acceptable.
- Refunds and payments are only allowed by the actual customer. There shall be no refunds or transfers of programs by individuals outside the customer's household.
- Governmental agencies; police or prosecutors requesting information must properly identify themselves. These requests should be handled by the Manager or Supervisor.
- Any discussion of the details of customer's personal information outside of the office is never acceptable for any reason.
- Scholarship assistance information shall be stored in a lockable file cabinet. Access to scholarship information shall be limited to those employees requiring access.
- The Department shall maintain an up-to-date list of those employees that are required to have access to personal records.
- Any photocopies made by Manager or Supervisor must have sensitive information (social security number, driver license number) blacked out.

APPENDIX C

Information Systems Internal Identity Theft Policy Effective April 3, 2008

Relevant excerpts from the
City of Columbia Comprehensive Security Policy
(entire policy may be found online at
<http://www.columbia.mo.gov/is/documents/security-policies.pdf>)

1.3 Identification and Authentication

1.3.1 Passwords

Passwords confirm that a person is who they claim to be. As such, passwords are extremely important to the security of the City of Columbia Information System. In general, city password policy encourages a balance between complexity, rotation, and user needs. Both lenient and strict policies are generally counter productive to security. This policy instead strives to set standards that, when used together, strike an appropriate balance.

1.3.1.1 Complexity

Passwords should be greater than 8 characters, mix upper and lower case characters, and use symbols. Alternatively, passphrases can be used in the absence of passwords. For example, “AskNotForWhomTheBellTolls” is a very long password and is therefore more difficult to break. Passwords should not be easily guessed. Phone numbers, names of friends, relatives, and pets, and other personal information are generally very easy to guess.

PCI DSS 8.5.10

1.3.1.2 Rotation

Passwords should not resemble previous passwords. For example, “Password12” should not be used if “Password11” has been used before. Where possible, systems and

applications should be set to “remember” old passwords and disallow use of passwords that match or are similar to a previous password. Where possible, systems should be set to store the last 10 passwords.

PCI DSS 8.5.12

1.3.1.3 Password Responsibilities of Users

Users are responsible for choosing passwords that are reasonably complex as defined in 1.3.1.1. Users must be able to use their passwords day to day and are therefore responsible for choosing passwords that will be meaningful enough for them to remember. Users are allowed to write down their password if they are unable to remember it. If a user chooses to write down his/her password, he/she must follow these rules:

- a) Their user id must not accompany the password
- b) The written password must be stored in a locked location to which ONLY the user has access. The written password must never be hidden in an unlocked location.
- c) The password should not be disposed of until it is no longer valid. If possible, the user should shred the password.

Users must recognize the importance of password privacy. Users must never share their password with anyone. Users must never ask each other for their passwords.

Departments must make sure that business operations are such that users never need to share credentials. IT staff must never ask users for their passwords and users must understand that IT staff will never do so.

1.3.1.4 Creating and resetting passwords

Temporary passwords, whether created due to account creation or password reset, are subject to section 1.3.1.1. A temporary password created for one user should not be the same as a temporary password created for another user. Instead, temporary passwords should be random and unique.

Users should call the Helpdesk to have passwords reset for every system and application. The Helpdesk should generate a temporary password, set the password to expired, and give the user the new password. The Helpdesk should encourage the user to immediately change the password. When passwords are reset the password should never be available to the user in an electronic form. The Helpdesk shall reset the password then give the new password to the user over the phone.

When a user requests a password reset, a work order shall be immediately created before continuing. The technician resetting the passwords shall check the SecTrack application to ensure the user is allowed to use the system for which he/she is requesting the password change. If the user is not authorized to use the system for which he/she is requesting access, the technician shall inform the user that he/she needs access through the SecTrack system and he/she should speak to his/her supervisor. The success or failure of the password reset will be documented in the work order. The temporary password should not be put in the content of the work order.

Users should never be allowed to reset their password without sufficiently proving that they are who they claim to be. Systems and applications that have “Forgot Password” links should direct users to the Helpdesk instead of providing a password reset method. Helpdesk employees must take responsibility for ensuring that the person requesting a password change is who they claim to be.

If the helpdesk employee cannot verify the user's identity, the Helpdesk employee may require the user to provide "cognitive passwords," or answers to questions that only the user is likely to know. A list of questions and their corresponding answers will be maintained by the IT department, and when a user calls with a password reset request, three questions will be chosen at random. The user must be able to answer the cognitive password questions before the password is reset.

PCI DSS 8.5.2, PCI DSS 8.5.3

1.3.1.5 Password expire

Passwords shall expire every 90 days. Once a password is expired, the user shall be required to change it. All systems and applications that support password expiration should enforce this policy.

PCI DSS 8.5.9

1.3.1.6 Password Transmission and Storage

Passwords should be encrypted using hash algorithms whenever stored or transmitted. The password hash algorithm used should be evaluated in accordance with the cryptography policy.

PCI DSS 8.4

1.4.3 User privilege audits

Each system and application should have a user privilege audit at least annually. The audit should consist of two parts:

- 1) Department confirmation that the requested access on file in SecTrack matches the access the department wishes the user to have.

- 2) The access given matches the access requested in SecTrack.

Satisfies NERC CIP-003-1 R5.2

1.4.4 Account audits

Each system and application should have an account audit at least annually. The audit may be done in concert with the user privilege audit in 1.4.3. The audit should consist of two parts:

- 1) Enumeration of all user accounts.
- 2) Determination that each user account has a valid SecTrack request and that the user is still employed by the city.

NERC CIP-003-1 R5.2

1.5 Accountability and risk mitigation measures

1.5.1 Accountability

Every system and application has an accountability mechanism that differs in some way from the mechanisms of other systems and applications. Each system and applications should be evaluated and accountability mechanisms should be enabled and configured according to risk. The following are general guidelines to implementing accountability across multiple independent systems and applications.

1.5.2 Authentication logging

Systems and applications should, where possible, create log entries for authentication attempts, both successful and failed. Log entries should include user identification, date/time stamp, and the device (machine name and/or IP address) from which the attempt originated.

1.5.3 Review of authentication events

Every system and application should have its logs reviewed regularly for possible security breaches. The frequency and content of the log audits may be different for each system and should be risk based.

1.5.4 Last login information

On systems and applications where capability exists, the user should be presented with details about their last successful login. Details should include time, date, place and any other pertinent information specific to the system or application.

1.6 Administration

1.6.1 Clipping level

Accounts should not allow an infinite number of “tries” until the correct password is used. Instead systems and applications should implement a “clipping level” that locks out accounts once a certain number of failed attempts has occurred for a user id. Systems and applications that have an enforcement mechanism for this policy shall have this value set to no more than 6. If possible, the user should not be aware that their account is disabled, only that their login attempt failed. Systems and applications should lock accounts for no less than 30 minutes.

PCI DSS 8.5.13, PCI DSS 8.5.14



APPENDIX D

Columbia Police Department Notification Procedures

Effective October 24, 2008

City of Columbia Employees will routinely be exposed to situations where Identity theft is a concern. It is imperative that staff follow notification procedures to ensure that the interests of both the City of Columbia and potential victims are protected.

Employees will consistently be discussing account and customer information over the phone or in person. It is imperative that the customer identity be established prior to any account services being provided. Employees, at times, will be given conflicting or false customer information. If the information can not be clarified or substantiated by staff to a reasonable degree, the customer will be required to respond in person and show a valid form of photo I.D. Once employees are reasonably satisfied there are no identity theft concerns, services can be provided.

Employees who continue to suspect the customer of identity theft can request the assistance of the Columbia Police Department. Employees should obtain a detailed description of the suspect and be able to provide a short synopsis of the incident. Officers will respond to investigate, determine if a crime occurred and take appropriate action.

Staff will potentially discover instances of identity theft or will be notified by a customer of the crime. Employees will assist victims of identity theft with necessary information and also assist with the investigation. Employees will provide an "Identity Theft Victim Information" sheet to all potential victims. Any victims who suffer a monetary loss and are seeking potential reimbursement from the city of Columbia will be required to file a police report and assist with prosecution.

Employees will call the Columbia Police Department and an officer will respond to investigate. Staff should be prepared to provide the officer copies of original documents or any other pertinent information that can be used for the investigation. If the City of Columbia suffers a loss from the identity theft incident the officer needs to note this in the police report for potential restitution.

Employees discovering incidents of internal theft should obtain enough information for a preliminary police report. Staff should be prepared to work with investigators and gather the following information:

Case preparation guideline for embezzlement or internal theft cases

Major Crimes Division, Columbia Police Department

No one is more familiar with your bookkeeping methods than you or your accountant. Therefore, it is important that you convey that information in a manner that is easy to understand and follow. In order to assist in the investigation and prosecution of your case, it is requested that you provide documentation in the following format.

Document preparation:

When preparing your documentation, place all of the pertinent information into a three-ringed binder that is designed to hold your information secure. Original documents should be used when compiling your initial folder. Once your original binder has been completed, make three copies. Please retain one copy for your records. The original and **two** copies should be submitted to the police. Once your case has been completed, the original documents will be returned to you. **Please remember that a neat and professional product is very important.**

Overview sheet:

The overview is a “brief” narrative that provides enough details of the case that the reader can obtain a clear understanding of the incident. The following information must be included, but is not limited to:

- A. Who discovered the theft and how it was uncovered.
- B. Who the suspect is.
- C. The dates of when the theft started and ended.
- D. The theft amount.
- E. How the theft was performed.
- F. The names of anyone the suspect made statements to about the theft and what was said.

Narrative sheet:

Please provide a “detailed” explanation of the theft. Please include the same information from the Overview Sheet section, plus an explanation of the supporting evidence, i.e. documents, ledgers, receipts, etc. Note: This section should read like a novel, covering every aspect of the case from beginning to end. Your information may be returned for revision, if this section is not thorough. It is vital that you explain all the supporting documents in this section, so it is clear and easy to understand. All documents must be numbered. Numbering each document makes it easier for the reader to locate information, when you refer to specific figures and page numbers. You may also consider using a highlighter to aid in quick location of figures.

Itemized list

This section is composed of an itemized list of each loss, date of the loss and the supporting document page number. A total loss dollar amount should be included at the bottom of this list.

Supporting Documents:

Include all documents relating to this case, which were explained in the “Narrative” section. **If you have any questions; do not hesitate to call the detective handling your case. The investigative office can be reached at (573) 874-7423.**

Finally, employees discovering incidents of computer related crimes (hacking or similar offenses) or where customer information or employee identity theft is at risk should immediately call the Columbia Police Department to file a report and initiate an investigation. (**Emergency 911; Non-Emergency 442-6131**)

The following Identity Theft Victim Information is what responding police officers provide Identity Theft Victims:

Identity Theft Victim Information

The City of Columbia requires a Police report and cooperation in the prosecution of the person or persons responsible before any reimbursement of losses will be discussed/determined.

Place a fraud alert on your credit reports and review your credit reports:

Equifax	1-800-525-6285 P.O. Box 740241 Atlanta, GA 30374-0241
Experian	1-888-EXPERIAN (397-3742) P.O. Box 9532 Allen, TX 75013
TransUnion	1-800-680-7289 Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790

When you report to one of these bureaus, they will report to the other two for you, and send you free reports. When you receive your reports, review them carefully. If there are any errors, report that to the credit bureaus by phone and in writing.

Close any accounts that have been tampered with or opened fraudulently, such as credit cards, bank accounts, phone and cell phone accounts, utility accounts, and internet service providers. Either use an Identity Theft Affidavit or ask the company to send you fraud dispute forms if they prefer, if there are fraudulent charges or debits.

The ID Theft Affidavit is to make sure you do not become responsible for debts incurred by the ID thief, so you must provide proof you did not create the debt. You can use the affidavit where a NEW account was opened in your name. Use it ASAP. For EXISTING accounts, your credit company will provide you with their own Dispute forms. The ID Theft Affidavit can be found at www.consumer.gov/idtheft.

If your ATM card is lost, stolen, or otherwise compromised, cancel it. Get a new card and PIN.

If your checks were stolen or misused, close that account and open a new one. Contact the three major check verification companies, and ask that retailers who use their databases not accept your checks.

TeleCheck 1-800-710-9898 or 927-0188

Certegy, Inc. 1-800-437-5120
International Check Services 1-800-631-9656

Call SCAN at 1-800-262-7771 to see if bad checks are being passed in your name.

- **File a complaint with the FTC.**

FTC Toll-free 1-877-IDTHEFT (438-4338), www.consumer.gov/idtheft TDD 202-326-2502

Identity Theft Clearinghouse
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580

- Document everything: Keep originals of all correspondence and documents; send copies as necessary
- Keep a record of everyone you talk to (names, dates, etc.)
- Keep all your files FOREVER! If something happens at a later date, you will be glad you did
- If you believe someone has filed for bankruptcy in your name, write to the U.S. Trustee in the region where it was filed. A list is available on the UST website at www.usdoj.gov/ust/
- If wrongful criminal violations are attributed to your name, contact that law enforcement agency
- Contact the Department of Motor Vehicles at www.dor.mo.gov/ and ask that your files be flagged
- If theft of mail was involved, contact the U.S. Postal Inspection Service at www.usps.gov/websites/depart/inspect
- If phone fraud was involved, contact the Public Utility Commission. If cell phone or long distance service was involved, contact the FCC at www.fcc.gov
- If your social security number was involved, contact the Social Security Administration at www.socialsecurity.gov
- If tax fraud was involved, contact the IRS at www.treas.gov/irs/ci
- **You can find much more information about Identity Theft, with more help and guidance, at the FTC's website at www.consumer.gov/idtheft**
- *Information provided comes directly from the FTC's website at www.consumer.gov/idtheft*

Appendix E

Identity Theft Training Program

Effective December 1, 2008

Training Protocol

- I. Introduction
 - a. What is Identity Theft?
- II. Red Flag Legislation
 - a. The Federal Trade Commission's Red Flag Rule (Implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003, pursuant to 16 C.F.R. 681.2.
 - b. Complying with the Red Flag Rule
 - c. How flexible is the Red Flag Rule?
- III. The City's Identity Theft Prevention Program
 - a. Departments who must comply
 - b. Examples of Red Flags
 - c. What is your role and responsibility?
- IV. Identity Theft
 - a. What is Identity Theft?
 - b. How does it happen?
 - c. How do you protect yourself from it?
 - d. What do you do if you're a victim?
- V. How to Report
 - a. Your expectations
 - b. Notifying Law Enforcement
 - c. Your Assistance if investigation involved
 - d. What to do if a Law Enforcement response is not necessary
- VI. Resources

Appendix F
Needs Assessment
Effective December 1, 2008

Conducting a Needs Assessment

Opening a New Record

Identify the steps in establishing a new record for a customer.

- 1) What identification is required? How do you obtain identifying information and verify identity? _____

- 2) Do they need to make the application in person or can they send in the information in an alternate form? Telephone or other? _____

- 3) Does the Department use consumer reports in the application process? How? Establish deposit? Approve or deny services? _____

- 4) Does the Department have policies and procedures that define red flags for identity theft and actions for mitigation? _____

- 5) What happens to the hand written notes made by the Department Representative in the application process? _____

- 6) Is the computer screen visible to others during the application process? _____

- 7) Who has access to data once entered? Does the Department Representative lock computer when not at desk? _____

- 8) If applicant gives address, bank account, date of birth or social security number verbally to Department Representative, what precautions are taken from others hearing? _____

- 9) Once personal identification information is entered by Department Representative, where and how can it later be retrieved? _____

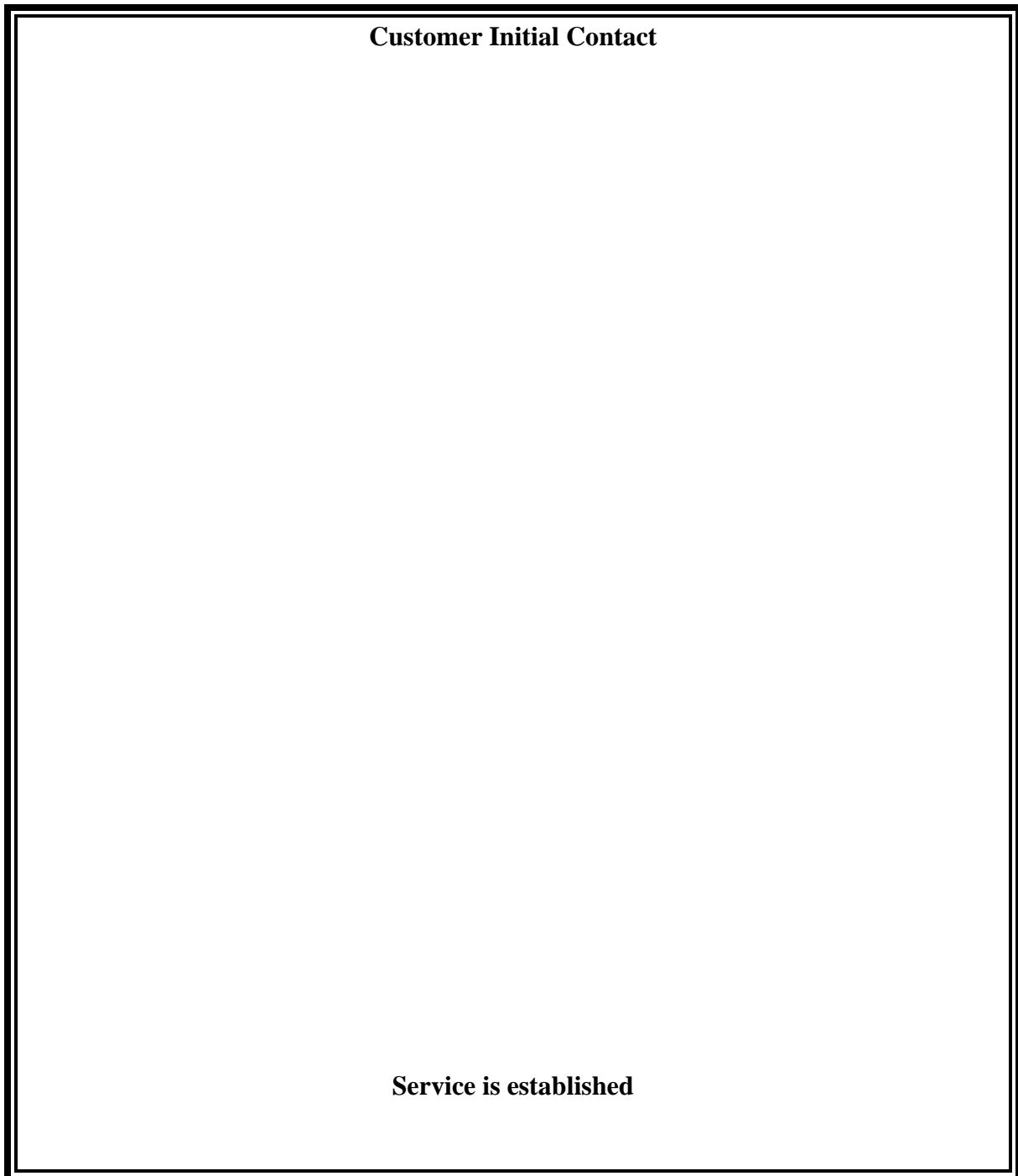
- 10) What safeguards are currently built into the application process? _____

- 11) What safeguards would you like to implement? _____

- 12) Which employees have access to information – is it on a “need to know” basis? _____

- 13) Is any customer personal information carried into the field on a laptop? _____

Map out the steps that occur when opening a new account. Is customer identification validated? Is so, how? Trace the flow of secured information.



Needs Assessment continued

Monitoring an Existing Record

Identify the possible red flags that may exist in the following procedures:

- ✓ Authenticating transactions for existing customers
- ✓ Monitoring activity/transaction of customers
- ✓ Verifying the validity of change of billing address
- ✓ Does the Department have policies and procedures that define red flags for identity theft and action for mitigation for existing records?

Does your Department use passwords or some form of security access?

Describe your process for verifying validating the following:

Check by phone _____

Credit Card Number _____

Are receipts ever printed? If so, what part of number is exposed? _____

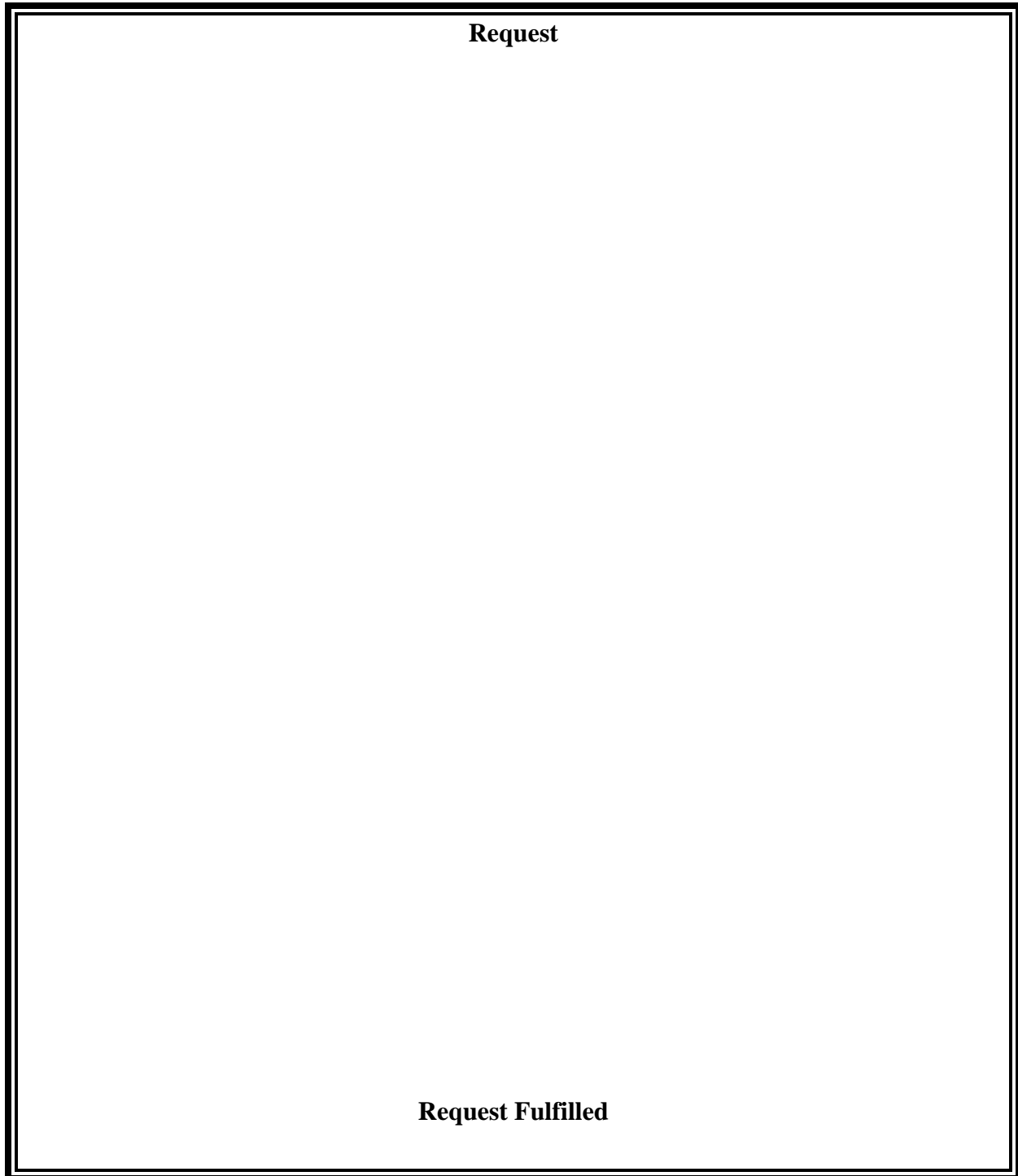
In what manner have customers attempted to fraudulently represent themselves as someone else in a transaction in an existing account?

What safeguards are currently built into monitoring existing record(s)?

What safeguards would you like to implement?

Map out the ways customers, 3rd parties and others access existing Records.

How do you authenticate transactions for existing Records?



After you have mapped out the flow of information, identify possible areas where the protection of secured information could be improved.