

# City of Columbia

701 East Broadway, Columbia, Missouri 65201



**Agenda Item Number:** R 96-15

**Department Source:** Public Works

**To:** City Council

**From:** City Manager & Staff

**Council Meeting Date:** 6/1/2015

**Re:** Authorizing a First Amendment to the Parking Services Agreement with Parkmobile USA, Inc.

## Documents Included With This Agenda Item

Council memo, Resolution/Ordinance, Exhibit to Resolution/Ordinance

**Supporting documentation includes:** None

## Executive Summary

Authorizing the City Manager to execute a first amendment to the Parking Services Agreement with Parkmobile USA, Inc. The amendment includes increasing the customer transaction fee from .35 cents to .45 cents and eliminates the credit card transaction fees currently paid by the City.

## Discussion

A successful 2012 pilot project allowed customers to pay for meters using their mobile phones. Staff found public response highly favorable, and feedback indicated that those who utilized the application appreciated the convenience of paying with a credit card over a mobile app. The mobile app provides customers with text reminders of expiring meter time and options to extend meter time.

In December of 2014, Council approved a Parking Services agreement with Parkmobile to implement their mobile application. This app will also allow easy implementation of a proposed downtown employee parking permit program. While reviewing the license agreement for the permit program, staff found several ways to reduce costs and risks to the City for credit card usage. The original agreement with Parkmobile was structured for customers to pay .35 cents per transaction to Parkmobile for use of the app, and the City paid all credit card transaction fees. With the proposed amended agreement, customers will pay .45 cents per transaction to Parkmobile for use of the app, and the City will no longer be responsible for the credit card transaction fees.

## Fiscal Impact

**Short-Term Impact:** This amendment eliminates credit card transaction fees currently paid by the City.  
**Long-Term Impact:** None

## Vision, Strategic & Comprehensive Plan Impact

Vision Impact: Downtown

Strategic Plan Impact: Financial Health

Comprehensive Plan Impact: Mobility, Connectivity, and Accessibility

# City of Columbia

701 East Broadway, Columbia, Missouri 65201



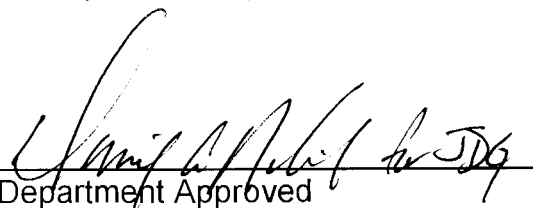
## Suggested Council Action


Authorize the City Manager to sign the first amended agreement with Parkmobile USA, Inc.

## Legislative History

12/1/14 (R225-14) Authorizing a Parking Services Agreement with Parkmobile

2/4/13 (REP 18-13) Purchase of Single-space Credit Card Capable Parking Meters

  
Department Approved

  
City Manager Approved

Introduced by \_\_\_\_\_ Council Bill No. \_\_\_\_\_ R 96-15

**A RESOLUTION**

authorizing a First Amendment to Parking Services Agreement with Parkmobile USA, Inc. to allow for the activation and payment of parking transactions using mobile technology.

BE IT RESOLVED BY THE COUNCIL OF THE CITY OF COLUMBIA, MISSOURI, AS FOLLOWS:

SECTION 1. The City Manager is hereby authorized to execute a First Amendment to Parking Services Agreement with Parkmobile USA, Inc. to allow for the activation and payment of parking transactions using mobile technology. The form and content of the agreement shall be substantially as set forth in "Attachment A" attached hereto and made a part hereof.

ADOPTED this \_\_\_\_\_ day of \_\_\_\_\_, 2015.

ATTEST:

\_\_\_\_\_  
City Clerk

\_\_\_\_\_  
Mayor and Presiding Officer

APPROVED AS TO FORM:

\_\_\_\_\_  
City Counselor

Copy

**First Amendment to Parking Services Agreement**

This First Amendment to Parking Services Agreement (hereinafter "Agreement") is made and entered into as of this \_\_\_\_\_ day of \_\_\_\_\_, 2015 by and between Parkmobile USA, Inc., a Georgia corporation f/k/a Parkmobile North America, Inc. (hereafter "Parkmobile") and the City of Columbia, a Missouri municipal corporation, (hereinafter "Client").

**RECITALS:**

WHEREAS the parties hereto entered into a Parking Services Agreement dated September 2, 2014, and

WHEREAS the parties desire to modify and amend certain provisions of that Agreement relating to fees charged by Parkmobile to end users per transaction and merchant processing and/or other third party processing and transfer fees, and

WHEREAS the parties desire to add certain general provisions further defining the obligations of the parties,

NOW THEREFORE, in consideration of the good and valuable consideration and the mutual covenants herein, the receipt and sufficiency of which are hereby acknowledged by the parties, the parties agree as follows:

1. Schedule 3 FEES, which is attached to and incorporated into the Agreement shall be amended as follows:

a. The amount of user convenience fee shall be increased from thirty-five cents (\$0.35) up to forty-five cents (\$0.45) per card transaction which shall include all costs associated with the acceptance of the card and electronic payments including but not limited to, merchant processing fees, third party processing fees, interchange fees, etc. and shall be borne by Parkmobile. There will be no fees charged to Client for card processing fees.

b. In the event Parkmobile elects to increase the user fees Parkmobile shall give ninety (90) days advance written notice to Client (increased from sixty (60) days in the original Agreement) and Client shall have the right to terminate this Agreement by providing sixty (60) days written notice to Parkmobile.

2. General Provisions

a. Requirements as Safeguards for Data

The Client has certain requirements and safeguards for the use and storage of data, external cloud regulations and red flag policies as set forth below and Parkmobile agrees to comply with these terms and provisions:

i. Data Ownership and Security. Parkmobile and its software shall comply with the requirements of this Section. Parkmobile shall require its subcontractors or third party software providers to at all times comply with the requirements of this section. Parkmobile covenants that any data from the City, its employees or customers or derived there from (hereinafter "City Data") shall be stored in the United States of America. City Data or any information derived there from shall not be transferred, moved, or stored to or at any location outside the United States of America. All such City Data and any information derived there from shall be confidential and proprietary information belonging to either the City or its customers or the users of the Software. Parkmobile covenants that Parkmobile, its subsidiaries or subcontractors shall not sell or give away any such City Data or information derived there from. Parkmobile shall maintain the security of City Data and that of City'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 City 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 forty-eight (48) hours.

ii. Binding Subcontractors and Subsidiaries to Data Security Standards. Parkmobile shall include similar provisions in Parkmobile's agreement(s) with subcontractors and subsidiaries who perform work or services related to these Software Products and or the City's Data contained therein or in the cloud storage.

iii. No Harmful Code. Parkmobile 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. Parkmobile shall include in contracts with any subcontractors a provision which prohibits the use of Harmful Code. Parkmobile shall include a similar provision in its contract with subcontractor.

iv. Software Upgrades. If, during the Term or any extended Maintenance Term of this Agreement, Parkmobile upgrades its software, City at its option, shall receive the upgrades at no additional charge.

v. Cloud Storage. Parkmobile shall comply with the City's Cloud Computing Requirements contained in Exhibit A.

vi. Red Flag Compliance. Parkmobile's Software shall at all times comply with the terms of this Agreement, the Contract Documents, Good

Financial Industry and Accounting Practices, Applicable Laws, City's Red Flag Policy, SAS70 auditing standards, and the City's Cloud Computing Requirements. Parkmobile shall comply with the City's Red Flag policy, attached as Exhibit B and timely report any Red Flags to the City's Program Administrator. Said report shall include Red Flags detected by Parkmobile or its subcontractors or subsidiaries and Parkmobile's response to the Red Flags so detected. Parkmobile shall provide City with a copy of its existing Red Flag policies and procedures, and shall promptly provide copies of any changes to its Red Flag policies and procedures.

vii. Compliance with Applicable Regulations and Standards for the use, storage or processing of Credit and Debit Cards. If any Software module or Software upgrade includes the storage, processing, or use of credit cards and/or debit cards, Parkmobile shall comply and shall warrant that the Parkmobile's software and services (including any modifications, customizations or interfaces) comply with the Payment Card Industry (PCI) Data Security Standards and the rules and regulations of payment card industry organizations including Visa, Mastercard, Discover, and any other applicable payment card industry organizations. Parkmobile shall further warrant that such software and/or modules be in compliance with Good Financial Industry and Accounting Practices; SAS70 auditing standards; NACHA (The Electronic Payments Association) Operating Rules; and the City's Red Flag Policy as applicable. Parkmobile shall further require that any subcontractor's software, modules, or upgrades be in compliance with this section in its contracts with those subcontractors or third party software providers. Compliance is required to be maintained with all listed applicable regulations, standards, etc. as they are updated and modified over the time period of the contracts.

Parkmobile shall notify City promptly of their failure or subcontractor's failure to maintain such compliance. In addition to Parkmobile's hold harmless agreement, Parkmobile shall be required to bear the cost of any fees, penalties, or costs accrued to City because of such failure to maintain such compliance.

Parkmobile shall provide annually to the City a copy of its PCI compliance audit certification.

b. Minimum Insurance Requirements.  
Parkmobile agrees to maintain the following minimum insurance requirements:

i. Insurance. Parkmobile 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 City's review or

acceptance of insurance maintained by Parkmobile is not intended to, and shall not in any manner limit or qualify the liabilities or obligations assumed by Parkmobile under the Agreement. Coverage to be provided as follows by a carrier with A.M. Best minimum rating of A- VIII:

1. Workers' Compensation & Employers Liability. Contractor 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 each accident, disease each employee and disease policy limit.
2. Commercial General Liability. Parkmobile shall maintain Commercial General Liability at a limit of not less than \$2,000,000 Each Occurrence, \$3,000,000 Annual, 3,000,000 Annual Aggregate. Coverage shall not contain any endorsement(s) excluding nor limiting Product/Completed Operations, Contractual Liability or Cross Liability.
3. Business Auto Liability. Parkmobile shall maintain Business Automobile Liability at a limit not less than \$2,000,000 Each Occurrence. Coverage shall include liability for Owned, Non-Owned & Hired automobiles. In the event Contractor does not own automobiles; Contractor 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.
4. Parkmobile 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. Contractor agrees to endorse the City 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.
5. The City 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 contractor and the City. Parkmobile is required to maintain coverages as stated and required to notify the City of a Carrier Change or

cancellation within two (2) business days. The City reserves the right to request a copy of the policy.

6. The Parties hereto understand and agree that the City 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 City, or its elected officials or employees.

7. Failure to maintain the required insurance in force may be cause for termination of the Agreement. In the event Parkmobile fails to maintain and keep in force the required insurance or to obtain coverage from its subcontractors, the City shall have the right to cancel and terminate the Agreement without notice.

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

c. Confidentiality.

The parties agree to abide by the terms and provisions as set forth in the confidentiality requirement:

i. The City of Columbia is subject to the Missouri Sunshine Law, See Section 610.021 RSMo and Section 2-25.3 of the City Code. Therefore, this agreement and any other related documentation are subject to the provisions of the Missouri Sunshine law.

ii. Each party acknowledges that all information and trade secrets relating to any of the other party's products and the services hereunder, including, without limitation, software, ("Confidential Information"). Except as otherwise set out herein, neither party shall disclose any Confidential Information of the other party to any third party or use it for its own benefit or the benefit of a third party, and each party shall take all commercially reasonable measures to protect the confidentiality of Confidential Information of the other party and prevent its disclosure to others.

iii. Each party may disclose the Confidential Information of the disclosing party to its affiliates and their respective employees and agents who are directly involved in the performance of this Agreement, who have a need to know and who are obligated to honor the restrictions on disclosure and use of such Confidential Information set forth in this Agreement (the persons to whom such disclosure is permissible being collectively known as "Representatives"). Each party shall be responsible



for any breach of this Section 5.2 by its Representatives. The parties shall not disclose, without the prior written consent of the disclosing party, any of such disclosing party's Confidential Information that it has learned either during the course of this Agreement or in discussions and proposals leading up to this Agreement, except as may be required by Law. The parties shall not use the Confidential Information of a disclosing party for any purpose other than that for which it was disclosed.

iv. All Confidential Information of Parkmobile and Client shall remain the property of each respective party. Upon any termination or expiration of this Agreement, each party shall return to the other party the other party's original version of all Confidential Information of such other party in document form, including any electronic media version, such as CD-ROM or computer disk, and shall confirm to such other party in writing that all such documents and things have been so provided and that all copies thereof have been destroyed subject to compliance with applicable Law. The foregoing shall not apply to any Confidential Information that is in the public domain without breach of this Agreement, Confidential Information that a party can demonstrate was known prior to receipt from the other party or Confidential Information that was subsequently received from a third party without any obligation of confidentiality to the other party.

v. To the extent any party determines it necessary or advisable to file a copy of this Agreement with a governmental agency, including the United States Securities and Exchange Commission, or otherwise in accordance with Law, that party and its counsel shall work with the non-disclosing party and its counsel to obtain confidential treatment of relevant portions of this Agreement, including, without limitation, product and service specifications and pricing information.

vi. Each party agrees that irreparable damage would occur, and that monetary damages would be an insufficient remedy at Law, in the event that any of the provisions of this confidentiality agreement were not performed by the other party in accordance with the terms hereof and that the each party shall be entitled to specific performance of the terms hereof, in addition to any other remedy at Law or equity.

vii. Each party's obligation with respect to the Confidential Information of a disclosing party shall expire three (3) years after the termination or expiration of this Agreement; provided, however, that each party's obligations with respect to the trade secrets of a disclosing party shall remain in effect throughout the Term and at all times thereafter, but only for so long as such information remains a trade secret.

d. Limitation of Liability.

The parties agree to the following provision for limitation of liability:

To the fullest extent permitted by law, the aggregate liability of Parkmobile for any and all losses and damages arising out of any cause whatsoever (whether such cause be based in contract, negligence, strict liability, other tort or otherwise) under this agreement shall in no event exceed an amount equal to the total amount paid for the services purchased hereunder; provided, however that the foregoing limitation of liability shall not apply in the event that the damages arise (a) from a data security breach of Parkmobile's system; (b) fraud or willful misconduct from Parkmobile or its employees, representatives, and agents, (c) intellectual property infringements or (d) violation of the confidentiality provisions of this agreement. Each party hereto agrees that the other party shall not be liable to such party of anyone acting through such party under any legal theory (including, without limitation, breach of contract, strict liability, negligence or any other legal theory) for incidental, consequential, indirect, special or exemplary damages arising out of or relating to this agreement.

3. Except as specifically set forth in this First Amendment to the Parking Services Agreement, the original Agreement is otherwise unmodified and remains in full force and effect and is hereby ratified and reaffirmed. In the event of any inconsistencies between the Agreement and this First Amendment the terms of this First Amendment shall take precedence.

[SIGNATURE PAGES FOLLOW]



Parkmobile USA, Inc. a Georgia  
Corporation f/k/a Parkmobile North  
America, Inc.:

BY: Cherie M. Suggs

Title: CEO

ATTEST: (if corporation)

[Signature]

STATE OF Georgia )  
COUNTY OF Fulton ) ss.

On this 18 day of May, 2015, before me, a notary public,  
appeared Cherie Fazzell, to me personally known, who being by me duly  
sworn did say that they are the CEO of Parkmobile USA, Inc. a  
Georgia corporation, f/k/a Parkmobile North America, Inc. and that this instrument was  
signed on behalf of said limited liability company and further acknowledged that they  
executed the same as their free act and deed for the purpose therein stated and that  
they have been duly granted the authority by said limited liability company to execute  
the same.

[Signature]  
Notary Public

My commission expires:

Cynthia Duos  
NOTARY PUBLIC  
Fulton County, GEORGIA  
My Comm. Expires  
12/06/2016

Exhibit **A**  
External Cloud Policies

When the City of Columbia purchases services from an external cloud provider, as defined in this cloud strategy, the following policies must be followed:

1.0 Responsibilities of the City of Columbia

The City of Columbia will carry out the following tasks for every external cloud deployment as defined in this cloud strategy:

- A. The City of Columbia will establish a written agreement with the cloud vendor. This agreement will explicitly state the responsibilities of the vendor.
- B. Prior to deployment, the City of Columbia will identify the regulations and standards that in force over the data or systems that may be moved to an external cloud. The City of Columbia will develop procedures and agreements with the cloud vendors to ensure compliance with all applicable regulations and standards.
- C. The City of Columbia will establish an acceptable time frame for the vendor to respond to open records request.
- D. The City of Columbia will establish a plan for the lifecycle of the service. The plan for the end of the service shall include what data will be extracted from the service, how data will be delivered, how the vendor will destroy data, and the price for these services. Data extracted from any system shall include transactional metadata, such as when data was added or changed and by whom.
- E. The City of Columbia will calculate the anticipated load that will be placed on the City of Columbia internet connection. If the internet connection cannot handle the load a load management plan will be created and implemented prior to service implementation.
- F. The City of Columbia will establish a business continuity plan that can be put into effect if the service ever becomes unavailable.
- G. The City of Columbia shall manage all user accounts for the service. User accounts shall be managed through the existing security track procedures.

2.0 Responsibilities of the Vendors

All external cloud vendors, defined as vendors providing any cloud services as defined in this strategy to the City of Columbia must adhere to the following policies.

2.1 Records Requests

- A. The vendor will respond to records request within the timeframe stated in the agreement. The vendor will accept liability if the records request is not fulfilled in the agreed upon timeframe.

## 2.2 Using City of Columbia Domain Names

- A. All cloud deployments that are intended to perform a service for our customers will be deployed using the gocolumbiamo.com domain name.
- B. The City of Columbia IT Department will be the sole entity responsible for the gocolumbiamo.com domain name. The cloud vendor shall not expect to maintain DNS records belonging to the City of Columbia.
  - a. The cloud vendor will provide the IP addresses used for the service prior to deployment. The City of Columbia IT Department will update the gocolumbiamo.com domain records accordingly.
  - b. The cloud vendor shall not change the addresses used with a frequency of greater than once per year.
  - c. The cloud vendor shall notify the City of Columbia IT department in writing on official letterhead 30 days in advance of any IP address changes.
  - d. The cloud vendor will use the gocolumbiamo.com only for the business purposes authorized by this agreement.
- C. Email from gocolumbiamo.com

When sending email from the service using the gocolumbiamo.com domain name, the following additional policies will be in effect:

- a. The cloud vendor will provide the IP addresses from which email will be sent. The City of Columbia IT Department will use this information to update the gocolumbiamo.com SPF record.
- b. The addresses provided to the City of Columbia as required in 3.2.3.1 shall be only those IP addresses that are used to send email using the gocolumbiamo.com domain name.
- c. The City of Columbia will update the gocolumbiamo.com SPF records according to the same policies and timelines as defined in 3.2.2 of this policy.
- d. The cloud vendor will take all reasonable precautions to ensure that SPAM is not sent using the gocolumbiamo.com domain or from any IP address under cloud vendor control that has been associated with the gocolumbiamo.com domain.
- e. The cloud vendor will react to email abuse reports in a timely manner.

### 2.3 Standards and Regulations

- A. The cloud vendor will adhere to relevant standards. For example, SaaS vendors deploying products over the web shall adhere to OWASP or similar standards.
- B. The cloud vendor shall take responsibility for all regulatory compliance.
- C. The cloud vendor shall conduct regular security audits of their systems. The security audits shall include internal and external review of system security and the security of all code used by the vendor. The vendor shall react promptly to mitigate the vulnerabilities identified by security audits.

### 2.4 System Integration

When an external cloud deployment requires access to existing information system infrastructure the following policies must be followed:

- A. Software should run with least possible privilege. For example, if database access needs to be given, the system account should have the least possible privilege; it should not run as a user that has access to schema outside of its need.
- B. System account names should not be easily guessed. Passwords for these accounts should not be easily guessed and should be different from other customers with the same product. Connections from system accounts should be, where appropriate and possible, controlled via access lists.

### 2.5 Deployment and Customization

- A. The cloud vendor shall disclose any authentication information that exists by default. The cloud vendor shall work with the City of Columbia to remove or change these accounts from their default values. The vendor shall not deploy services to the City of Columbia where system accounts are shared with other entities.

### 2.6 Encryption

- A. Cloud vendor shall establish a suitable data encryption scheme for data in transit between the City of Columbia, its customers, and the vendor. The City of Columbia will determine the suitability of the encryption scheme.
- B. Cloud vendor shall establish a suitable encryption for City of Columbia data while in storage for both live and backup media. The City of Columbia will determine the suitability of the encryption scheme.
- C. No encryption scheme will be considered suitable if City of Columbia data can be recovered using the same decryption key as that of another customer of the cloud vendor.

## 2.7 Incident Preparation

- A. The cloud vendor will take responsibility for keeping their system software up to date. Vendors should monitor relevant discussion boards and mailing lists for security problems with products they use.
- B. The cloud vendors shall have a method for customers and others to report security problems. This method should be well publicized and accessible. Vendors should have a method for prioritizing and acting on reports of security problems.
- C. The cloud vendors shall have a method for correcting discovered vulnerabilities. Vulnerabilities should be prioritized and corrected based on the risk vulnerability exploitation would pose to its customers. Vulnerability mitigation efforts should be tested by the vendor, as appropriate, prior to their release.

## 2.7 Incident Response

- A. The cloud vendor will take responsibility for security incident handling if their system is compromised.
- B. The cloud vendor shall immediately notify the City of Columbia of any breaches and will advise what information has been compromised. If this information is later found to be inaccurate the cloud vendor will immediately notify the City of Columbia with the correct information.
- C. If investigation, containment, and eradication efforts by the City of Columbia incur costs while fault lies with the cloud vendor, the cloud vendor will assume the costs.
- D. The cloud vendor will provide a rapid contact method for reporting suspected abuse, 24x7x365. The cloud vendor will react in a timely manner to abuse reports from the City of Columbia.
- E. The cloud vendor will provide their incident response plans. Response plans will include procedures for both security incident and disaster incident response.



exh. b7B

## **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

<b>Appendix A</b>	Finance Department Internal Identity Theft Policies.....	14-19
<b>Appendix B</b>	Parks & Recreation Department Internal Identity Theft Policy.....	20
<b>Appendix C</b>	Information Systems Department Internal Identity Theft Policy.....	21-26
<b>Appendix D</b>	Law Enforcement Identity Theft Notification Steps.....	27-30
<b>Appendix E</b>	Identity Theft Training Protocol.....	31
<b>Appendix F</b>	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. Identify 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.