City of Bloomington
Common Council

Legislative Packet

Committee of the Whole

23 September 2009

Please consult the Legislative Packet issued in interest of the 16 September 2009 Regular Session for additional legislation and background material.

Office of the Common Council
P.O. Box 100
401 North Morton Street
Bloomington, Indiana 47402

812.349.3409

council@bloomington.in.gov
http://www.bloomington.in.gov/council

City of Bloomington Indiana

City Hall
401 N. Morton St.
Post Office Box 100
Bloomington, Indiana 47402

Office of the Common Council
(812) 349-3409
Fax: (812) 349-3570
email: council@bloomington.in.gov

To: Council Members
From: Council Office
Re: Weekly Packet Memo
Date: September 18, 2009

Packet Related Material

Memo
Agenda
Calendar
Notices and Agendas:
None

Legislation for Discussion at Committee of the Whole:

- **App Ord 09-08** To Specially Appropriate from the Electronic Map Generation Fund Expenditures Not Otherwise Appropriated (Appropriating Funds to Retain Consultant for the City's Geographic Information System)
  Contact: Rick Dietz at dietzr@bloomington.in.gov

- **App Ord 09-09** To Specially Appropriate from the General Fund Expenditures Not Otherwise Appropriated (Appropriating a PetSmart Charities Grant for Use by the Animal Care and Control Department)
  Contact: Mike Trexler at 349-3412 or trexlerm@bloomington.in.gov

- **Res 09-08** Approving the City of Bloomington Utility Identity Theft Protection Program
  - Memo to Council from Vickie Renfrow, Assistant City Attorney; Identity Theft Prevention Program
  Contact: Vickie Renfrow at 349-3426 or renfrowv@bloomington.in.gov

- **Ord 09-17** To Vacate Four Public Parcels - Re: A Portion of North Madison Street, West 12th Street and Two Alleys Located Between North Rogers Street, the Indiana Railroad, 350 West 11th Street and West 11th Street (Doug Dayhoff, Upland Brewing Company, Inc., and Middle Court Real Estate, LLC (together "Upland"), Petitioners)
  Contact: Lynne Darland at 349-3529 or darlandl@bloomington.in.gov

Please see the September 16th Legislative Packet for the legislation, background materials and summaries regarding App Ord 09-08, App Ord 09-09, and Ord 09-17.

Memo

Four Items Ready for Discussion at the Committee of the Whole on Wednesday, September 23rd

There are four items ready for discussion at the Committee of the Whole next Wednesday. The information regarding the three ordinances can be found in last week's packet (see above for a link to that packet) and the information regarding the resolution is contained in this packet.

Item Three – Res 09-08 – Approving the City Utilities' Identity Theft Prevention Program as Required by the Federal "Red Flag Rule"

Res 09-08 approves the City Utilities' Identity Theft Prevention Program as required by the federal "Red Flag Rule." According to the memo from Vickie Renfrow, Assistant City Attorney, the "Red Flag Rule" is a set of regulations issued by a group of federal entities in order to implement the Fair and Accurate Credit Transactions (FACT) Act of 2003. As her memo says,

> The regulations require a "creditor" (which includes utility companies) who handles "covered accounts" (which includes utility accounts) to adopt a written program for the identification, detection, prevention and mitigation of identity theft. In particular, the program must identify practices or specific activities (known as "red flags") that could indicate identity theft and articulate responses to these red flags. The program must be approved by the "governing body" for the utility, which for our Utility is the Common Council. The accounts that must be monitored are utility accounts which are maintained primarily for personal, family, and household purposes and involve multiple, recurring transactions. If identify theft is suspected, the policy articulates specific steps that Utility personnel will follow for prevention and mitigation, including monitoring the account for suspicious activity, contacting the customer, closing an account, or contacting law enforcement.

The Identity Theft Prevention Program must be in writing (it is attached to the resolution), customized to address the circumstance of each applicable entity, and contain five measures. These measures [1] include:

Identifying "red flags"

The program must identify "red flags" for our "covered (customer) accounts." For the Utilities Department, these "red flags" comprise:

- Suspicious documents – which, for example, include:
  - altered or forged IDs; or
  - information on identification that is inconsistent with other facts (like the physical appearance of the applicant) which are known by, or readily available to, the Utility;
- Suspicious personal identifying information – which, for example, include personal identifying information that is:
  - not consistent with other information provided by the customer or used by the Utility, or
  - associated with known fraudulent activity or
- Unusual use of, or other suspicious activity related to, covered accounts – which, for example, include:
  - an account that is used in an unusual manner, or
  - a long dormant account that is used, or
  - instances where mail to an account is repeatedly returned even though transactions with the customer continue or
- Notices of fraudulent accounts – which, for example, occur when:
  - a customer, victim of identity theft, law enforcement official or other person notifies the Utility of a fraudulent account opened for a person engaged in identity theft

Detecting "red flags" when they arise

The program must establish procedures to detect the "red flags" by verifying the identity of persons opening an account, authenticating customers, monitoring transactions and verifying requests for change of address. The proposed program does this for both new and existing accounts and acknowledges that information may be obtained "in person, by telephone, fax, mail or email of scanned documents."

[1] This summary was borrowed from the following presentation: Red Flag Rules – Compliance for Municipalities, Indiana Municipal Law Association Seminar XXVI (6/12/09), Jeremy L. Fetty of Parr, Richey, Obremskey, Frandsen & Patterson, Attorneys at Law

Responding to "red flags" in order to prevent and mitigate identity theft

In the event "red flags" are detected, the program must establish procedures to respond to them in a manner to prevent or mitigate identity theft. In that regard, along with taking all reasonable steps in regard to internal procedures to forestall the problem, the proposed program directs staff to do one or more of the following depending on the level of risk involved:

- monitor the account;
- contact the customer;
- change passwords;
- perhaps close the existing account and, perhaps, not open a new one
- notify the Program Administrator and/or law enforcement; and
- determine that the particular circumstances warrant no response.

Administering the program

The program must provide for the oversight, development, implementation and administration of this initiative, the training of staff, and the oversight of service providers. In this regard, the proposed program:

- designates the Bloomington Utility Assistant Director of Finance (Michael Horstman) as Program Administrator with responsibility for oversight, development, implementation and administration of the program and creates an Identity Theft Prevention Committee consisting of the Utility Accounts Receivable Coordinator, Utility Customer Service Coordinator, Technology Support Manager and Technology Support Specialist to assist the Administrator;
- provides for the Program Administrator to train staff who implement this program; and
- requires all 3rd party service providers to comply with the "red flag rule" as well.

Periodically update the procedures

The program must provide for a periodic review of procedures to address changes in risks associated with identity theft for customers as well as the Utility. The proposed program calls for an annual review with any changes to be approved by the Utility Services Board.

NOTICE AND AGENDA
BLOOMINGTON COMMON COUNCIL COMMITTEE OF THE WHOLE
7:30 P.M., WEDNESDAY, SEPTEMBER 23, 2009
COUNCIL CHAMBERS
SHOWERS CENTER, 401 N. MORTON ST.

Chair: Susan Sandberg

1. Appropriation Ordinance 09-08 To Specially Appropriate from the Electronic Map Generation Fund Expenditures Not Otherwise Appropriated (Appropriating Funds to Retain Consultant for the City's Geographic Information System)

Asked to Attend: Rick Dietz, Director of Information Technology Services
Mike Trexler, Controller

2. Appropriation Ordinance 09-09 To Specially Appropriate from the General Fund Expenditures Not Otherwise Appropriated (Appropriating a PetSmart Charities Grant for Use by the Animal Care and Control Department)

Asked to Attend: Laurie Ringquist, Director of Public Works
Mike Trexler, Controller

3. Resolution 09-08 Approving the City of Bloomington Utility Identity Theft Protection Program

Asked to Attend: Vickie Renfrow, Assistant City Attorney

4. Ordinance 09-17 To Vacate Four Public Parcels - Re: A Portion of North Madison Street, West 12th Street and Two Alleys Located Between North Rogers Street, the Indiana Railroad, 350 West 11th Street and West 11th Street. (Doug Dayhoff, Upland Brewing Company, Inc., and Middle Court Real Estate, LLC [together "Upland"], Petitioners)

Asked to Attend: Lynne Darland, Zoning and Enforcement Manager

Posted & Distributed: Friday, September 18, 2009

City of Bloomington
Office of the Common Council

To: Council Members
From: Council Office
Re: Calendar for the Week of September 21-26, 2009

Monday, September 21, 2009

12:00 pm Bloomington Entertainment and Arts District Advisory Meeting, McCloskey
4:00 pm Council for Community Accessibility, McCloskey
5:30 pm Bicycle and Pedestrian Safety Commission, Hooker Room

Tuesday, September 22, 2009

4:00 pm Bloomington Community Farmers' Market, Madison St, Between 6th & 7th St
4:00 pm Board of Park Commissioners, Council Chambers
5:15 pm Solid Waste Management District Citizens Advisory Committee, McCloskey
5:30 pm Bloomington Public Transportation Corporation, Public Transportation Center, 130 W Grimes Lane
7:00 pm Public Forum: *Imagine a City of Peace*, Council Chambers

Wednesday, September 23, 2009

10:00 am Metropolitan Planning Organization Technical Advisory Committee, McCloskey
4:00 pm Dr. Martin Luther King, Jr., Birthday Commission, McCloskey
6:30 pm Metropolitan Planning Organization Citizens Advisory Committee, McCloskey
7:30 pm Common Council Committee of the Whole, Council Chambers

Thursday, September 24, 2009

10:30 am County Address Coordination, McCloskey
5:30 pm Board of Zoning Appeals, Council Chambers

Friday, September 25, 2009

12:00 pm Economic Development Commission, Hooker Room
1:00 pm Commission on Hispanic and Latino Affairs Open Forum, Council Chambers

Saturday, September 26, 2009

8:00 am Bloomington Community Farmers' Market, Showers Common, 401 N. Morton
10:00 am Latino Dance Demonstration at Farmers' Market, Showers Common, 401 N. Morton

Posted and Distributed: Friday, September 18, 2009

RESOLUTION 09-08
APPROVING THE CITY OF BLOOMINGTON UTILITY
IDENTITY THEFT PROTECTION PROGRAM

WHEREAS, the "Red Flag Rule" refers to regulations that were issued jointly by the Federal Trade Commission, the National Credit Union Administration, and the federal bank regulatory agencies, to implement the Fair and Accurate Credit Transactions (FACT) Act of 2003, and said regulations implement Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 681.2; and

WHEREAS, said regulations require that a "creditor" (which includes utility companies) who handles "covered accounts" (which includes utility accounts) to adopt a written policy or program for the identification, detection, prevention and mitigation of identity theft; and,

WHEREAS, said policy or program must identify practices or specific activities (known as "red flags") that could indicate identity theft and articulate responses to these red flags; and,

WHEREAS, said policy or program must be approved by the "governing body" for the utility, which for the City of Bloomington Utility is the Common Council; and,

WHEREAS, the City of Bloomington Utility has developed an Identity Theft Prevention Program, a copy of which is attached to this Resolution, and requests the Common Council's approval of said policy so as to come into compliance with the Red Flag Rule.

NOW, THEREFORE, BE IT RESOLVED BY THE COMMON COUNCIL OF THE CITY OF BLOOMINGTON, INDIANA, THAT:

SECTION 1: The Common Council of the City of Bloomington hereby approves the City of Bloomington Utility Identity Theft Program as set out in the attachment to this Resolution.

SECTION 2. This resolution shall be in full force and effect from and after its passage by the Council and approval of the Mayor of the City.

PASSED AND ADOPTED by the Common Council of the City of Bloomington, Monroe County, Indiana, upon this _____ day of _____, 2009.

_____
ANDY RUFF, President
Bloomington Common Council

ATTEST:

_____
REGINA MOORE, Clerk
City of Bloomington

PRESENTED by me to the Mayor of the City of Bloomington, Monroe County, Indiana, upon this _____ day of _____, 2009.

_____
REGINA MOORE, Clerk
City of Bloomington

SIGNED and APPROVED by me upon this _____ of _____, 2009.

_____
MARK KRUZAN, Mayor
City of Bloomington

SYNOPSIS

This Resolution approves the City of Bloomington Utility Identity Theft Program which was developed pursuant to the Federal Trade Commission's Red Flags Rule ("Rule") and is required by said Rule. The Program identifies the "red flags" which will be detected and give rise to responses which will prevent and mitigate Identity Theft associated with City of Bloomington Utility accounts.

CITY OF BLOOMINGTON
LEGAL DEPARTMENT
MEMORANDUM

TO: **Common Council Members**
FROM: **Vickie Renfrow, Assistant City Attorney**
RE: **Red Flag Rule Compliance – Resolution 09-08**
DATE: **September 15, 2009**

The "Red Flag Rule" refers to regulations that were issued jointly by the Federal Trade Commission, the National Credit Union Administration, and the federal bank regulatory agencies, to implement the Fair and Accurate Credit Transactions (FACT) Act of 2003. The regulations require a "creditor" (which includes utility companies) who handles "covered accounts" (which includes utility accounts) to adopt a written program for the identification, detection, prevention and mitigation of identity theft. In particular, the program must identify practices or specific activities (known as "red flags") that could indicate identity theft and articulate responses to these red flags. The program must be approved by the "governing body" for the utility, which for our Utility is the Common Council. The accounts that must be monitored are utility accounts which are maintained primarily for personal, family, and household purposes and involve multiple, recurring transactions. If identify theft is suspected, the policy articulates specific steps that Utility personnel will follow for prevention and mitigation, including monitoring the account for suspicious activity, contacting the customer, closing an account, or contacting law enforcement.

The Red Flag Rules only require that a program be approved by the governing body but do not dictate what the program should contain. There are suggestions as to what should be considered a "red flag", but the substance of the program to be adopted is up to the utility and its governing body. The program attached to Resolution was developed by City Utilities, Legal and ITS staff after reviewing samples of Red Flag programs from other Indiana cities and other material. The program was approved by the USB and adheres closely to the suggestions set out in the Federal Register. By and large this really involves formalizing policies and practices which are already in place. Please let me know if you have any questions regarding this matter.

CITY OF BLOOMINGTON UITLITY
IDENTITY THEFT PREVENTION PROGRAM

The City of Bloomington Utility has developed this Identity Theft Prevention Program ("Program") pursuant to the Federal Trade Commission's Red Flags Rule ("Rule"), which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003, 16 C.F.R. § 681.2. The law applies to "Creditors" which includes "utility companies", and relates to "covered accounts" which includes "an account that a . . . creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a . . . utility account, and any other account that the . . . creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the . . . creditor from identity theft . . . ." The law defines "Identity Theft" as "fraud committed using the identifying information of another person. The law defines "Red Flag" as "a pattern, practice or specific activity that indicates the possible existence of identity theft". 16 C.F.R. § 681.2(b)(8) & (9). The Program is intended to identify red flags and detect, prevent, and mitigate identity theft in connection with the opening or accessing of an account.

I. IDENTIFICATION OF RED FLAGS.

The Utility identifies the following red flags in each of the listed categories:

A. Suspicious Documents:
   1. Documents provided for identification appear to have been altered or forged;
   2. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification;
   3. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification;
   4. Other information on the identification is not consistent with readily accessible information that is on file with the Utility;
   5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

B. Suspicious Personal Identifying Information:
   1. Personal identifying information provided is inconsistent when compared against external information sources used by the Utility;
   2. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer;
   3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Utility, for example:
      a. The address on an application is the same as the address provided on a fraudulent application, or

b. The phone number on an application is the same as the number provided on a fraudulent application;

4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Utility, for example:
   a. The address on an application is fictitious, a mail drop, or a prison; or
   b. The phone number is invalid, or is associated with a pager or answering service;
5. The SSN provided is the same as that submitted by other persons opening an account or other customers;
6. 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 accounts or other customers;
7. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete;
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the Utility;

C. Unusual Use of, or Suspicious Activity Related to, the Covered Account:
1. A covered account is used in a manner that is not consistent with established patterns of activity on the account;
2. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors);
3. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account;
4. The Utility is notified that the customer is not receiving paper account statements;
5. The Utility is notified of unauthorized charges or transactions in connection with a customer's covered account.

D. The Utility is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

II. DETECTING RED FLAGS

A. New Accounts – New accounts can be opened in person, by fax, by mail or by email of scanned documents. In order to detect any of the Red Flags identified above associated with the opening of a new account, Utility personnel will take the following steps to obtain and verify the identity of the person opening the account:

1. Require identifying information including name, date of birth, residential or business address, principal place of business or an entity, driver's license or other identification;
2. Verify the customer's identity with photo identification
3. Review documentation showing the existence of a business entity; and
4 Contact the customer if necessary to clarify information

B. Existing Accounts – Information regarding existing accounts and changes of billing address can be obtained in person, by telephone, fax, mail or email of scanned documents. Requests to discontinue service or changes in banking information must be made in writing either in person, by fax, mail or email of scanned documents. In order to detect any of the Red Flags identified above associated with activity related to an existing account, Utility personnel will take the following steps to monitor transactions with an account:

1. Verify the identification of customers if they request information
2. Verify the validity of request to discontinue service, change billing address, etc.; and
3. Verify changes in banking information given for billing and payment purposes.

III. RESPONSE TO RED FLAGS–PREVENTING AND MITIGATING IDENTITY THEFT

A. Response to Red Flags – In the event Utility personnel detect any identified Red Flags, such personnel shall take one or more of the following steps, depending upon the degree of risk posed by the Red Flag:

1. Continue to monitor an account for evidence of Identity Theft;
2. Contact the customer;
3. Change any passwords or other security devices that permit access to accounts;
4. Not open a new account;
5. Close an existing account;
6. Reopen an account with a new number
7. Notify the Program Administrator for determination of the appropriate steps to take;
8. Notify law enforcement; or
9. Determine that no response is warranted under the particular circumstances.

B. Further Protection of Identifying Information – In order to further prevent the likelihood of Identity Theft occurring with respect to Utility accounts, the Utility will take all other reasonable steps with respect to it internal operating procedures to protect customer identifying information.

IV. PROGRAM ADMINISTRATION AND UPDATING

The City of Bloomington Utility Assistant Director of Finance shall be the Program Administrator and shall be responsible for the oversight, development, implementation and administration of the Program. The Program Administrator shall administer the Program with the assistance of the Utility Accounts Receivable Coordinator, the Utility Customer Service Coordinator, and the Technology Support Manager and the Utility Technology Support Specialist from the City of Bloomington Information and Technology Services Department, which shall constitute the City of Bloomington Utility Identity Theft Program Committee. The Program shall be reviewed on an annual basis to determine whether modifications are necessary and to review its effectiveness. Any modifications to the Program shall be subject to the approval of the Utility Service Board. Utility personnel responsible for implementing the Program shall be trained by the Program Administrator. In addition, the Utility will, as part of its contracts with third party service providers, require as part of the contract that these providers have policies, procedures and programs that comply with the "Red Flag Rule".