SOUTH WEBER CITY COUNCIL
AGENDA

PUBLIC NOTICE is hereby given that the City Council of SOUTH WEBER, Davis County, Utah will meet in a PUBLIC WORK MEETING on

TUESDAY, 3 NOVEMBER 2009

in the City Planning Room, 1600 E South Weber Dr, South Weber, UT

The Public Work Meeting is held for discussion purposes only.
Any items requiring action by Resolution or Ordinance will be placed on the agenda of a Regular Public Meeting or Public Hearing for deliberation and action as required.

PUBLIC WORK MEETING

5:30 P.M. **DISCUSSION: RESOLUTION 09-47 ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM IN COMPLIANCE WITH FEDERAL AND STATE LEGISLATION AND REGULATION**

5:45 P.M. **DISCUSSION WITH STAKER PARSONS – DIGITAL SIGN, RELOCATION OF DETENTION BASIN, DEW TOUR PARKING**

6:15 P.M. **REVIEW OF UPCOMING AGENDA**

- *Canvass 2009 Municipal General Election*
- *Resolution 09-47: A Resolution Establishing an Identity Theft Prevention Program*
- *Final Acceptance of S & S Estates Subdivision*

CLOSED EXECUTIVE SESSION

CLOSED EXECUTIVE SESSION: *IN ACCORDANCE WITH UTAH CODE 52-4-205*

- **FOR STRATEGY SESSION TO DISCUSS THE PURCHASE, EXCHANGE, OR LEASE OF REAL PROPERTY**

THE UNDERSIGNED DULY APPOINTED CITY RECORDER FOR THE MUNICIPALITY OF SOUTH WEBER CITY HEREBY CERTIFIES THAT A COPY OF THE FOREGOING NOTICE WAS MAILED, EMAILED OR POSTED TO:

CITY OFFICE BUILDING
CITY WEBSITE www.southwebercity.com
UT PUBLIC NOTICE WEBSITE ww.utah.gov/pmn
THOSE LISTED ON THE AGENDA

SOUTH WEBER ELEMENTARY SCHOOL
RAY'S VALLEY SERVICE
SOUTH WEBER FAMILY ACTIVITY CENTER UT
EACH MEMBER OF GOVERNING BODY

DAVIS COUNTY CLIPPER
STANDARD-EXAMINER
SALT LAKE TRIBUNE
DESERET NEWS

DATE: October 30, 2009 **CITY RECORDER: Erika J. Ahlstrom**

IN COMPLIANCE WITH THE AMERICANS WITH DISABILITIES ACT, INDIVIDUALS NEEDING SPECIAL ACCOMMODATIONS DURING THIS MEETING SHOULD NOTIFY ERIKA AHLSTROM, 1600 EAST SOUTH WEBER DRIVE, SOUTH WEBER, UTAH 84405 (479-3177).

Agenda times are approximate and may be moved in order, sequence and time to meet the needs of the Council.

SOUTH WEBER CITY COUNCIL

Staff Backup Report

Date of City Council Meeting: **3 Nov Work Mtg; 10 Nov 2009**

Title: **RES 09-47: Adoption of Identity Theft Prevention Policy**

RECOMMENDATION

Adopt an Identity Theft Prevention Policy as required by the Federal Trade Commission.

BACKGROUND

The Federal Trade Commission issued a regulation for all financial institutions and creditors to adopt and implement a program to respond to the increasing problem of identity theft; known as "Red Flag Rules". To be in compliance, municipalities must create a program that explains how it will implement the new regulations and approve a resolution adopting the program by November 1, 2009.

Governmental agencies will be audited for compliance with these regulations along with their annual comprehensive financial audits. By adopting these regulations the city will also reduce the likelihood of liabilities related to fraudulent acts. (For information on the Federal Trade Commission's Investigative And Law Enforcement Authority, go to http://ftc.gov/ogc/brfovrvw.shtm)

Staff became aware of this new regulation and attended the session for Red Flags Rules at ULCT conference in September. After review of the Red Flag Rules (for more information on the Rules http://www.redflagrules.net/General_Requirements.html), staff assessed steps currently taken to protect covered accounts and found that much of the program is already in use but that several improvements could be made.

Staff used guidelines provided by the Federal Trade Commission to develop this policy.

CONCLUSION

By adopting the Identity Theft Prevention Policy the City will fulfill the requirements of the Red Flag Rules. The goal is to be aware of the Red Flags, remain alert in detecting those Red Flags and respond. This program is to be updated annually to be in compliance to help ensure the safety and security of the residents and the City.

RESOLUTION 09-47

A RESOLUTION ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM IN COMPLIANCE WITH FEDERAL AND STATE LEGISLATION AND REGULATION

WHEREAS, on October 31, 2007 the Federal Trade Commission passed Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the "Red Flag Rules," which requires creditors that hold consumer accounts to develop and implement a written identity theft prevention program providing for the identification, detection and response to patterns, practices or specific activities known as "Red Flags" that could indicate identity theft; and

WHEREAS, the compliance of these "Red Flags Rules" is required by November 1, 2009; and

WHEREAS, the General Assembly of State of Utah approved the Protection of Personal Information Act (the "Act"), effective January 1, 2007; and

WHEREAS, the implementation of both the "Red Flag Rules" and the "Act" require the City to establish policies limiting and managing the collection and dissemination of personal identifying and financial information, and the diligent pursuit of "Red Flags" which are indicators that identity theft is about to happen or has happened in the past in relation to covered accounts.

BE IT THEREFORE RESOLVED by the South Weber City Council that:

1. The attached "Identity Theft Prevention Policy" (the "Policy") is hereby adopted with an effective date of November 1, 2009.
2. The City Manager is hereby authorized to make changes to this policy as necessary to achieve and maintain compliance with the letter and the spirit of these requirements.

PASSED AND ADOPTED by the City Council of South Weber this **10th day of November 2009.**

APPROVED

_____

Brent V. Petersen, Mayor

Attest:

_____

Erika J. Ahlstrom, City Recorder

SOUTH WEBER CITY

Identity Theft Prevention Program

Protection of Consumer Information and Detection, Prevention and Mitigation of Identity Theft for Covered Accounts

FACTA Section 114 Red Flag Plan
and
Utah Protection of Personal Information Act

Adopted by South Weber City Council
Resolution 09-47; (Date)

Purpose

On October 31, 2007, the Federal Trade Commission passed Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA), also known as the RED FLAG RULES.

Under the Red Flag Rule, every financial institution and creditor is required to establish an "Identity Theft Prevention Program" to detect, prevent and mitigate identity theft in connection with the opening of certain new and certain existing accounts. The Program shall be tailored to the size, complexity and nature of its operation. Each program must contain reasonable policies and procedures to:

1. Identify relevant red flags for new and existing covered accounts and incorporate those red flags into the program;
2. Detect red flags that have been incorporated into the program;
3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
4. Ensure the program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the creditor from identity theft.

Designation of Committee(s)

1. RED FLAG IMPLEMENTATION COMMITTEE

This group is charged with the responsibility of performing the initial gap analysis, prioritizing deficiencies, performing market studies on solutions available, selecting and contracting for specific solution components, developing specific solution requirements, delivering training appropriate to deploy and maintain solutions, and documenting all of the above in the written Identity Theft Prevention Program document to be submitted to the City Council. At this time the committee consists of the Utility Billing Clerk and the City Treasurer.

2. RED FLAG OVERSIGHT COMMITTEE

The members of this committee are charged with the responsibility of keeping the Identity Theft Prevention Program up to date and in compliance with FACTA Section 114 requirements, and ensuring employees are trained to effectively execute the duties under the plan. This committee will report the Council annually to review the effectiveness of the Program on the covered accounts and to make recommendations for any material changes to the Plan. At this time the committee consists of the City Manager and the City Recorder.

Definitions

Creditor: An entity that regularly extends, renews, continues credit or arranges for extension of credit.

Covered Account: A consumer account designed to permit multiple payments or transactions, or any other account for which there is a reasonably foreseeable risk of identity theft (e.g. residential files, billing records, payment records).

Identity Theft: Occurs when a person wholly takes over another individual's indentifying information to obtain goods or services.

Identifying Information: Any indentifying information which may be used to identify a person, such as a date of birth, Social Security Number , state issued drivers license, government identification, passport, etc.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft.

Risk Assessment

The Red Flag Implementation Committee has conducted a Risk Assessment based on the requirements of FACTA Section 114, and has determined that there is a need to implement an Identity Theft Prevention

Program for South Weber City. The Committee assessed which accounts should be included, based on the definitions for "Covered Accounts" as shown under 'Definitions'.

During the risk assessment, the following were considered:

- The methods used to open accounts;
- The methods used to access accounts; and
- Previous experiences with identity theft.

Under the definition of "Creditor" the Committee also considered Covered Accounts as any account for which the city provides a product or service and does not collect payment in advance or at the time of service, and any account where a consumer may default in payment after obtaining the product or service.

In addition, the Risk Assessment Committee we considered the potential for both new and existing account fraud based on the following threats that may result in the unauthorized access of personal information that can lead to identity theft:

- Technology intrusion (hacking, spyware, bots, etc.)
- Consumer deception (phishing, pharming, vishing, etc.)
- Employee theft of consumer information
- Social engineering – cons perpetrated against employees/customers
- Physical intrusion (break-in)
- Compromise of postal mail – both internal and at mailbox
- Loss/theft of laptop computers –unencrypted
- Other accidental loss – improper disposal of information, loss in transport, etc.

List of Red Flags

Following is a list of the Red Flags shown in FACTA Section 114, Subpart J, Appendix A, and an indication of "Applicable" if the Red Flag will be included in this Identity Theft Prevention Program, and "Not Applicable" if the Red Flag will NOT be included as part of this Program, and the reason for excluding the sample Red Flag.

Category: Alerts, notifications, or other warnings received from customer reporting agencies or service providers, such as fraud detection services.

1. A fraud alert included with a consumer report. *Not applicable - currently the city does not check credit reports.*

2. Notice of credit freeze in response to request for a consumer report. *Not applicable - currently the city does not check credit reports.*

3. A consumer reporting agency providing notice of address discrepancy. *Applicable.*

4. Unusual credit activity, such as an increased number of accounts or inquiries. *Not applicable - currently the city does not check credit reports.*

Category: The Presentation of Suspicious Documents.

5. Documents provided for identification appearing altered or forged. *Applicable.*

6. Photograph on identification inconsistent with appearance of customer. *Applicable.*

7. Information on identification inconsistent with information proved by person opening account. *Applicable.*

8. Information on identification, such as signature, inconsistent with information on file at financial institute. *Applicable*.

9. Application appearing forged or altered or destroyed and reassembled. *Applicable*.

Category: Suspicious Personal Identifying Information.

10. Information on identification not matching addresses in the consumer report, Social Security number has not been issued or appears on the Social Security Administration's Death Master File, a file of information associated with Social Security numbers of those who are deceased. *Not applicable - currently the city does not confirm SSN's with an outside source.*

11. Lack of correlation between Social Security number range and date of birth. *Applicable*.

12. Personal Identifying information associated with known fraud activity. *Applicable.*

13. Suspicious addresses supplied, such as mail drop or prison, or phone numbers associated with pagers or answering service. *Applicable*.

14. Social Security number provided matching that submitted by another person opening an account or other customers. *Applicable*.

15. An address or phone number matching that supplied by a large number of applicants. *Applicable*.

16. The person opening the account unable to supply identifying information in response to notification that the application is incomplete. *Applicable*.

17. Personal information inconsistent with information already on file at financial institute or creditor. *Applicable*.

18. Person opening account or customer unable to correctly answer challenging questions. *Applicable.*

Category: Unusual Use of, or Suspicious Activity Related to, the Covered Account.

19. Shortly after change of address, creditor receiving request for additional users of account. *Applicable*.

20. Most of available credit used for cash advances, jewelry or electronics; customer fails to make first payment or makes an initial payment but no subsequent payments. *Applicable*.

21. Drastic change in payment patterns such as:

    a. Non-payment when there is no history of late or missed payments
    b. A material increase in use of available credit
    c. A material change in purchasing or spending patterns
    d. A material change in electronic fund transfer patterns in connection with a deposit account
    e. A material change in telephone call patterns in connection with a cellular phone account

    Applicable.

22. An account that has been inactive for a lengthy time suddenly exhibiting unusual activity. *Applicable*.

23. Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account. *Applicable*.

24. Financial institution or creditor notified that customer is not receiving paper account statements. *Applicable.*

25. Financial institution or creditor notified of unauthorized charges or transactions on customers account. *Applicable.*

Category: Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institute or Creditor.

26. Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft. *Applicable.*

Detection and Response to Red Flags

1. New Residential Accounts
    - Require and verify identifying information when setting up new utility account
    - Compare photo identification carefully to resident presenting identification
    - Compare physical description to resident presenting identification (e.g. DOB, height, etc.)
    - Check expiration date of identification
    - Compare signature on identification to utility application
    - Review identification for evidence of tampering

2. Existing Residential Accounts
    - Verify identification of resident or legal representative before disclosing any personal identifying information.
    - Verify identification of resident or legal representative before accommodating requests for changes of billing address or name changes.

Prevention and Mitigation of Identity Theft

If identity theft is suspected for any reason, immediate action is required. Notify a committee member or the City Manager. One of the following actions will immediately be put into place:

- Monitor the covered account for evidence of identity theft
- Contact the resident
- Re-open a covered account with a new account number
- Do not open a new covered account
- Closing an existing covered account
- Notify law enforcement

Administration of the Identity Theft Prevention Program

Periodic Risk Assessment

In accordance with the administrative requirements of FACTA Section 114, a risk assessment should be performed annually to determine if procedures are being followed to correctly include the necessary accounts as indicated in the Risk Assessment section of this Identity Theft Prevention Program

Updating with New Red Flags

In accordance with FACTA Section 114, the Identity Theft Prevention Program should be updated annually. New Red Flags may be identified based on the following considerations:

- **Experiences with ID Theft**
  At this time South Weber City has not experienced ID theft.

- **Changes in the methods of ID Theft at large**

- **Changes in methods to detect, prevent and mitigate ID Theft**

- **Changes in business arrangements, i.e. mergers, acquisitions, alliances, joint ventures, service providers, etc.**

Annual Report to the City Council

The Red Flag Oversight Committee should provide a report to the City Council on an annual basis that will include the following:

Significant Incidents – a list of Red Flags found and any other significant identity theft/information breach issues that occurred within the organization or reported by customers or employees.

Response to Significant Incidents – an indication of how each situation was handled and ultimately resolved.

Effectiveness on Covered Accounts – a summary of the effectiveness of the plan based on how the incidents above were handled.

Service Provider Oversight – a list of any new service providers and a description of the evaluation process conducted to assure compliance with Section 114 service provider oversight requirements.

Recommendations for Updating/Amending Program – a recommendation for deletions, amendments or additions to the Identity Theft Prevention Program.

Compliance with the Utah Code Title 13, Chapter 44

Protection of Personal Information Act

Overview:

Utah Code 13-44-101 et seq., effective January 1, 2007, as amended.

The Protection of Personal Information Act requires notice of a breach of the security of computerized personal information that is not protected by a method that makes the information unusable. Entities covered by another state or federal law are exempt if the person notifies each affected Utah resident in accordance with the applicable law.

Consistent with federal laws the Utah Protection of Personal Information Act is intended to tackle the critical problem of identity theft by requiring entities collecting personal information to take steps to secure it. The Act also requires that leaked information be immediately disclosed to the consumer to prevent further loss.

While the federal Red Flag Rule applies mainly to utilities operated by municipalities, state legislation can affect other areas of cities and towns based on the information collected and stored. All municipalities should evaluate their situation to ensure compliance with these laws.

Effective Date – January 1, 2007

Following pages are the requirements that the municipality must follow.

Compliance with Utah Code Title 13, Chapter 44
"Protection of Personal Information Act"

13.44.102	Definitions
	13-44-102. Definitions. As used in this chapter: (1) (a) "Breach of system security" means an unauthorized acquisition of computerized data maintained by a person that compromises the security, confidentiality, or integrity of personal information. (b) "Breach of system security" does not include the acquisition of personal information by an employee or agent of the person possessing unencrypted computerized data unless the personal information is used for an unlawful purpose or disclosed in an unauthorized manner. (2) "Consumer" means a natural person. (3) (a) "Personal information" means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii) (A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number. (b) "Personal information" does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public. (4) "Record" includes materials maintained in any form, including paper and electronic.
13-44-201	**Protection of Personal Information**
	13-44-201. Protection of personal information. (1) Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person. (2) The destruction of records under Subsection (1)(b) shall be by: (a) shredding; (b) erasing; or (c) otherwise modifying the personal information to make the information indecipherable.

13-44-202	Disclosure of System Security Breach
	13-44-202. Personal information -- Disclosure of system security breach. (1) (a) A person who owns or licenses computerized data that includes personal information concerning a Utah resident shall, when the person becomes aware of a breach of system security, conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be misused for identity theft or fraud purposes. (b) If an investigation under Subsection (1)(a) reveals that the misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur, the person shall provide notification to each affected Utah resident. (2) A person required to provide notification under Subsection (1) shall provide the notification in the most expedient time possible without unreasonable delay: (a) considering legitimate investigative needs of law enforcement, as provided in Subsection (4)(a); (b) after determining the scope of the breach of system security; and (c) after restoring the reasonable integrity of the system. (3) (a) A person who maintains computerized data that includes personal information that the person does not own or license shall notify and cooperate with the owner or licensee of the information of any breach of system security immediately following the person's discovery of the breach if misuse of the personal information occurs or is reasonably likely to occur. (b) Cooperation under Subsection (3)(a) includes sharing information relevant to the breach with the owner or licensee of the information. (4) (a) Notwithstanding Subsection (2), a person may delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation. (b) A person who delays providing notification under Subsection (4)(a) shall provide notification in good faith without unreasonable delay in the most expedient time possible after the law enforcement agency informs the person that notification will no longer impede the criminal investigation. (5) (a) A notification required by this section may be provided: (i) in writing by first-class mail to the most recent address the person has for the resident; (ii) electronically, if the person's primary method of communication with the resident is by electronic means, or if provided in accordance with the consumer disclosure provisions of 15 U.S.C. Section 7001; (iii) by telephone, including through the use of automatic dialing technology not prohibited by other law; or (iv) by publishing notice of the breach of system security: (A) in a newspaper of general circulation; and (B) as required in Section **45-1-101**. (b) If a person maintains the person's own notification procedures as part of an information security policy for the treatment of personal information the person is considered to be in compliance with this chapter's notification requirements if the procedures are otherwise consistent with this chapter's timing requirements and the person notifies each affected Utah resident in accordance with the person's information security policy in the event of a breach. (c) A person who is regulated by state or federal law and maintains procedures for a breach of system security under applicable law established by the primary state or federal regulator is considered to be in compliance with this part if the person notifies each affected Utah resident in accordance with the other applicable law in the event of a breach. (6) A waiver of this section is contrary to public policy and is void and unenforceable. Amended by Chapter 388, 2009 General Session

13-44-301	Enforcement
	13-44-301. Enforcement. (1) The attorney general may enforce this chapter's provisions. (2) (a) Nothing in this chapter creates a private right of action. (b) Nothing in this chapter affects any private right of action existing under other law, including contract or tort. (3) A person who violates this chapter's provisions is subject to a civil fine of: (a) no greater than $2,500 for a violation or series of violations concerning a specific consumer; and (b) no greater than $100,000 in the aggregate for related violations concerning more than one consumer. (4) In addition to the penalties provided in Subsection (3), the attorney general may seek injunctive relief to prevent future violations of this chapter in: (a) the district court located in Salt Lake City; or (b) the district court for the district in which resides a consumer who is affected by the violation. (5) In enforcing this chapter, the attorney general may: (a) investigate the actions of any person alleged to violate Section **13-44-201** or **13-44-202**; (b) subpoena a witness; (c) subpoena a document or other evidence; (d) require the production of books, papers, contracts, records, or other information relevant to an investigation; and (e) conduct an adjudication in accordance with Title 63G, Chapter 4, Administrative Procedures Act, to enforce a civil provision under this chapter. (6) A subpoena issued under Subsection (5) may be served by certified mail. (7) A person's failure to respond to a request or subpoena from the attorney general under Subsection (5)(b), (c), or (d) is a violation of this chapter. (8) (a) The attorney general may inspect and copy all records related to the business conducted by the person alleged to have violated this chapter, including records located outside the state. (b) For records located outside of the state, the person who is found to have violated this chapter shall pay the attorney general's expenses to inspect the records, including travel costs. (c) Upon notification from the attorney general of the attorney general's intent to inspect records located outside of the state, the person who is found to have violated this chapter shall pay the attorney general $500, or a higher amount if $500 is estimated to be insufficient, to cover the attorney general's expenses to inspect the records. (d) The attorney general shall deposit any amounts received under this Subsection (8) in the Attorney General Litigation Fund established in Section **76-10-922**. (e) To the extent an amount paid to the attorney general by a person who is found to have violated this chapter is not expended by the attorney general, the amount shall be refunded to the person who is found to have violated this chapter. (f) The Division of Corporations and Commercial Code or any other relevant entity shall revoke any authorization to do business in this state of a person who fails to pay any amount required under this Subsection (8). Amended by Chapter 29, 2008 General Session