

ORDINANCE NO. 2008-11

AN ORDINANCE BY THE CITY OF INGLESIDE ON THE BAY TEXAS, ESTABLISHING AN IDENTITY THEFT PREVENTION PROGRAM, SETTING OUT DEFINITIONS, POLICIES AND PROCEDURES FOR IMPLEMENTATION OF THE IDENTITY THEFT PREVENTION PROGRAM; PROVIDING A REPEALING CLAUSE, PROVIDING A SAVINGS AND SEVERABILITY CLAUSE AND PROVIDING FOR AN EFFECTIVE DATE.

WHEREAS, Federal Trade Commission adopted rules pertaining to an Identity Theft Prevention pursuant to the Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 which requires that creditors adopt an Identity Theft Prevention Program on or before November 1, 2008; and

WHEREAS, the Red Flags Rule defines creditor to include all utility companies and the City owns and provides utility services and/or accepts payments for municipal utility services and is therefore classified as a creditor; and

WHEREAS, the City Council has reviewed the Program and believes it fulfills, complies and implements the Red Flags Rule and other requirements outlined by the Federal Trade Commission; and

WHEREAS, the City Council finds that it is in the public interest to approve the Program.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF INGLESIDE ON THE BAY, TEXAS, THAT:

Section 1. Findings. The foregoing recitals are hereby found to be true and correct and are hereby adopted by the City Council and made a part hereof for all purposes as findings of fact.

Section 2. Implementation. All procedures and requirements of The Identity Theft Prevention Program shall be implemented as outlined in the Exhibit A.

Section 3. All provisions of the Code of Ordinances of the City of Ingleside on the Bay in conflict with the provisions of this Ordinance are hereby repealed to the extent of such conflict, and all other provisions of the Ordinances of the Ingleside on the Bay not in conflict with the provisions of this Ordinance shall remain in full force and effect.

Section 4. Should any sentence, paragraph, subdivision, clause, phrase or section of this Ordinance be adjudged or held to be unconstitutional, illegal or invalid, the same shall not affect the validity of this Ordinance as a whole, or any part or provision thereof other than the part so decided to be invalid, illegal or unconstitutional, and shall not affect the validity of the Code of Ordinances as a whole.

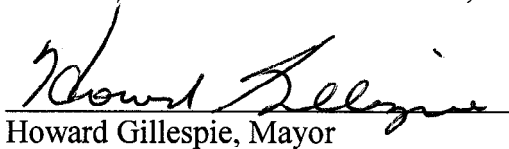
Ordinance 2008-11

Section 5. This Ordinance shall take effect immediately from and after its passage and the publication of the caption in the official newspaper as the law in such cases provide.

Section 6. Open Meetings. That it is hereby officially found and determined that the meeting at which this ordinance is passed was open to the public as required and that public notice of the time, place, and purpose of said meeting was given as required by the Open Meeting Act, Capt. 551, Loc. Gov't. Code.

PASSED AND APPROVED on this 21ST day of October, 2008.

CITY OF INGLESIDE ON THE BAY, TEXAS


Howard Gillespie, Mayor

ATTEST:


Diane Hosea, City Secretary

APPROVED AS TO FORM:


Hal George, City Attorney

EXHIBIT "A"

CITY OF INGLESIDE ON THE BAY
IDENTITY THEFT PREVENTION POLICY

SECTION 1: BACKGROUND

The risk to the City, its employees and customers from data loss and identity theft is of significant concern to the City and can be reduced only through the combined efforts of every employee and contractor.

SECTION 2: PURPOSE

The City adopts this sensitive information policy to help protect employees, customers, contractors and the City from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the City in compliance with state and federal law regarding identity theft protection.

This policy enables the City to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the City from fraudulent new accounts. The program will help the City:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

SECTION 3: SCOPE

This policy and protection program applies to employees, contractors, consultants,

temporary workers, and other workers at the City, including all personnel affiliated with third parties.

SECTION 4: POLICY

A. Sensitive Information Policy

1. Sensitive information includes the following items whether stored in electronic or printed format:

- a. Credit card information, including any of the following:
 - 1.) Credit card number (in part or whole)
 - 2.) Credit card expiration date
 - 3.) Cardholder name
 - 4.) Cardholder address
- b. Tax identification numbers, including:
 - 1.) Social Security number
 - 2.) Business identification number
 - 3.) Employer identification numbers
- c. Payroll information, including, among other information:
 - 1.) Paychecks
 - 2.) Pay stubs
- d. Cafeteria plan check requests and associated paperwork
- e. Medical information for any employee or customer, including but not limited to:
 - 1.) Doctor names and claims
 - 2.) Insurance claims
 - 3.) Prescriptions
 - 4.) Any related personal medical information
- f. Other personal information belonging to any customer, employee or contractor, examples of which include:
 - 1.) Date of birth
 - 2.) Address
 - 3.) Phone numbers
 - 4.) Maiden name
 - 5.) Names
 - 6.) Customer number

City personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Texas Open Records Act and the City's open records

policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. In the event that the City cannot resolve a conflict between this policy and the Texas Open Records Act, the City will contact the Texas Attorney General's Office for guidance.

B. Hard Copy Distribution

Each employee and contractor performing work for the City will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a suitable shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" City records, however, may only be destroyed in accordance with the City's Records Retention Policy.

C. Electronic Distribution

Each employee and contractor performing work for the City will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved municipal e-mail. All sensitive information must be encrypted when stored in an electronic format.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

“This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited.”

D. Red flags

1. The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.
 - a. Alerts, notifications or warnings from a consumer reporting agency;
 - b. A fraud or active duty alert included with a consumer report;
 - c. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
 - d. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

2. Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries
 - b. An unusual number of recently established credit relationships
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

3. **Suspicious documents**
 - a. Documents provided for identification that appear to have been altered or forged.
 - b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

- c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- d. Other information on the identification is not consistent with readily accessible information that is on file with the City, such as a signature card or a recent check.
- e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

4. Suspicious personal identifying information

- a. Personal identifying information provided is inconsistent when compared against external information sources used by the City. For example:
 - The address does not match any address in the consumer report;
 - The Social Security number (SSN) has not been issued or is listed on the Social Security Administration Death Master File; or,
 - Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
- b. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address on an application is the same as the address provided on a fraudulent application.
- c. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example:
 - The address on an application is fictitious, a mail drop, or a prison; or
 - The phone number is invalid or is associated with a pager or answering service.
- d. The SSN provided is the same as that submitted by other persons opening an account or other customers.

-
- e. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.
 - f. The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
 - g. Personal identifying information provided is not consistent with personal identifying information that is on file with the City.
 - h. When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

5. Unusual use of, or suspicious activity related to, the covered account

- a. Shortly following the notice of a change of address for a covered account, the City receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.
- b. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments
- c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:
 - Nonpayment when there is no history of late or missed payments;
 - A material change in purchasing or usage patterns
- d. 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).
- e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

-
- f. The City is notified that the customer is not receiving paper account statements.
 - g. The City is notified of unauthorized charges or transactions in connection with a customer's covered account.
 - h. The City receives 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 City
 - i. The City 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.

E. DETECTING RED FLAGS.

1. New Accounts

In order to detect any of the Red Flags identified above associated with the opening of a **new account**, utility billing employees will take the following steps to obtain and verify the identity of the person opening the account:

- a. Require certain identifying information such as name, date of birth, residential or business address, principal place of business for an entity, driver's license or other identification;
- b. Verify the customer's identity (for instance, review a driver's license or other identification card);
- c. Review documentation showing the existence of a business entity;
- d. Request additional documentation to establish identity; and
- e. Independently contact the customer or business.

2. Existing Accounts

In order to detect any of the Red Flags identified above for an **existing account**, utility billing employees will take the following steps to monitor transactions with an account:

- a. Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email);

- b. Verify the validity of requests to close accounts or change billing addresses; and
- c. Verify changes in banking information given for billing and payment purposes.

F. PREVENTING AND MITIGATING IDENTITY THEFT

1. Prevent and Mitigate

In the event utility billing employees 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:

- a. Continue to monitor an account for evidence of Identity Theft;
- b. Contact the customer, sometimes through multiple methods;
- c. Change any passwords or other security devices that permit access to accounts;
- d. Not open a new account;
- e. Close an existing account;
- f. Do not close the account, but monitor or contact authorities;
- g. Reopen an account with a new number;
- h. Notify the Program Administrator for determination of the appropriate step(s) to take;
- i. Notify law enforcement; or
- j. Determine that no response is warranted under the particular circumstances.

2. Protect customer identifying information

In order to further prevent the likelihood of identity theft occurring with respect to utility accounts, the City will take the following steps with respect to its internal operating procedures to protect customer identifying information:

- a. Ensure that its website is secure or provide clear notice that the website is not secure;
- b. Where and when allowed, ensure complete and secure destruction of paper documents and computer files containing customer information;
- c. Ensure that office computers are password protected and that computer screens lock after a set period of time;
- d. Change passwords on office computers on a regular basis;
- e. Ensure all computers are backed up properly and any backup information is secured;
- f. Keep offices clear of papers containing customer information;
- g. Request only the last 4 digits of social security numbers (if any);
- h. Ensure computer virus protection is up to date; and
- i. Require and keep only the kinds of customer information that are necessary for utility purposes.

F. PROGRAM ADMINISTRATION

1. The importance of this program warrants the highest level of attention by administration and staff. Appropriate staff shall be responsible for developing and implementing this program.
2. Staff training shall be conducted for any employee, official or contractor who may reasonably come into contact with accounts or personally identifiable information that it may constitute a risk to the City or its customers.
3. All service providers with access to sensitive information shall be required to show proof of adherence to reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

-
4. This policy may be amended by the City Council as needed to comply with changing laws, and to maintain consistency with the current state of the identity theft problem.

G. SPECIFIC PROGRAM ELEMENTS AND CONFIDENTIALITY

For the effectiveness of Identity Theft prevention Programs, the Red Flag Rule envisions a degree of confidentiality regarding the City's specific practices relating to Identity Theft detection, prevention and mitigation. Therefore, under this program, knowledge of such specific practices is limited to employees who need to know them for purposes of preventing Identity Theft. Because this program is to be adopted by a public body and thus publicly available, it would be counterproductive to list these specific practices here. Therefore, only the program's general red flag detection, implementation and prevention practices are listed in this document.

**ORDINANCE NO
2008-11**
**AN ORDINANCE BY
 THE CITY OF INGLE-
 SIDE ON THE BAY
 TEXAS ESTABLISHING
 AN IDENTITY THEFT
 PREVENTION PRO-
 GRAM, SETTING OUT
 DEFINITIONS, POLI-
 CIES AND PROCE-
 DURES FOR IMPLI-
 MENTATION OF THE
 IDENTITY THEFT PRE-
 VENTION PROGRAM,
 PROVIDING A REPEAL-
 ING CLAUSE, PROVID-
 ING A SAVING AND
 SEVERABILITY
 CLAUSE AND PROVID-
 ING FOR AN EFFEC-
 TIVE DATE.
 PUBLISHED IN THE
 INGLESIDE INDEX,
 OCTOBER 29, 2008.**

THE STATE OF TEXAS
 COUNTY OF SAN PATRICIO:

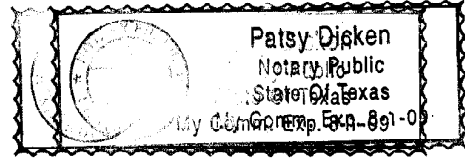
Before me, the undersigned authority, personally appeared
Clay Morgan of The Ingleside Index, who after being
 by me duly sworn, on his oath deposes and said:

1. That (he) (she) is Publisher of The Ingleside Index a weekly newspaper
 published in San Patricio County, Texas.

2. That the City of Ingleside On Bay -
Ordinance - 2008-11
 hereto annexed, was published in the regular issues of said Ingleside Index once
 each week for One (1) week successive weeks said publications
 having been made on the October 29, 2008

3. That a printed copy of said Notice
 as the same appeared in said issues is attached hereto.

Clay Morgan



Sworn to and subscribed before me this 7th
 day of November, 2008
Patsy Dicken
 Notary Public, San Patricio County, Texas
 PUBLICATION FEE: \$ 44.50