City of Battle Ground Identity Theft Red Flag Policy

Policy

It is the policy of the City of Battle Ground to protect the identity of the City's customers from identity theft. This policy applies to any account the City offers or maintains that involves multiple payments or transactions. The City developed this Identity Theft Prevention Program pursuant to the Federal Trade Commission's Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

Program Purpose

The City of Battle Ground establishes an Identity Theft Prevention Program to detect, prevent and mitigate identity theft. The Program shall include reasonable policies and procedures to:

1. Identify relevant red flags for covered accounts it offers or maintains and incorporates 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 and to the safety and soundness of the creditor from identity theft.

The program shall, as appropriate, incorporate existing policies and procedures that control reasonably foreseeable risks.

Program Administration

The Finance and Information Services Director is responsible for oversight of the program implementation. The City Manager is responsible for reviewing reports prepared by staff regarding compliance with red flag requirements. The Finance and Information Services Director shall recommend material changes to the program to address changing identity theft risks and to identify new or discontinued types of covered accounts.

1. The Finance and Information Services Director will report to the City Manager at least annually, on compliance with the red flag requirements. The report will address material matters related to the program and evaluate issues such as:

    a. The effectiveness of the policies and procedures of the City in addressing the risk of identity theft in connection with opening of covered accounts and with respect to existing covered accounts;

    b. Service provider relationships;

    c. Significant incidents involving identity theft and management's response; and

    d. Recommendations for material changes to the Program.

2. The Finance and Information Services Director is responsible for providing training to all employees responsible for or involved in opening a new covered account or accepting payment for a covered account with respect to the implementation and requirements of the Identity Theft Prevention Program. The Finance and Information Services Director shall exercise his or her discretion in determining the amount and substance of training necessary.

Process of Establishing a Covered Account

As a precondition to opening a covered account in the City, each applicant shall provide the City either through the loan closing process at the Title Companies, a phone call or in person at the Finance Department, a Washington State driver's license or Washington identification number.

Access to Covered Account Information

The City staff will strive to protect utility account information through the following steps:

- Access to customer accounts shall be password protected and shall be limited to authorized City personnel.
- Any unauthorized access to or other breach of customer accounts is to be reported immediately to the Finance and Information Services Director.
- Personal identifying information included in customer accounts is considered confidential and any request or demand for such information shall be immediately forwarded to the Finance and Information Services Director.

Credit Card Payments

Credit card payments shall be processed in the following manner:

- In the event that credit card payments are made over the internet through the City's third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place that is applicable to such payments.

- All credit card payments made over the telephone or in person, shall be entered directly into the credit card processing software.

- Account statements and receipts for covered accounts shall include only the last four digits of the credit or debit card used for the payment of the covered account.

Sources and Types of Red Flags

All employees responsible for or involved in the process of opening a covered account or accepting payment for a covered account shall check for red flags as indicators of possible identity theft and such red flags may include:

1. Alerts from consumer reporting agencies, fraud detection agencies or service providers. Examples of alerts include but are not limited to:
    a. A fraud or active duty alert that is not included with a consumer report;
    b. A notice of credit freeze in response to a request for a consumer report;
    c. A notice of address discrepancy provided by a consumer reporting agency;
    d. Indications of a pattern of activity in a consumer report that is inconsistent with the history and usual pattern of activity of an applicant or customer such as:
        i. A recent and significant increase in the volume of inquiries;
        ii. An unusual number of recently established credit relationships;
        iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
        iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
2. Suspicious Documents. Examples of suspicious documents include:
    a. Documents provided for identification that appear to be altered or forged;
    b. Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer;
    c. Identification on which the information is inconsistent with information provided by the applicant or customer.
    d. Identification on which the information is inconsistent with readily accessible information that is on file with the creditor, such as the application for service; or
    e. An application that appears to be altered or forged, or appears to have been destroyed and reassembled.
3. Suspicious personal identification such as suspicious address change. Examples of suspicious identifying information include:
    a. Personal identifying information that is inconsistent with external information sources used by the City. For example:
        i. The address does not match any address in the consumer report; or
        ii. The Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File.

b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer such as a lack of correlation between the Social Security Number range and the date of birth.
c. Personal identifying information or a phone number or address, is associated with known fraudulent applications or activities as indicated by internal or third-party sources used by the City.
d. Other information provided, such as fictitious mailing address, mail drop addresses, jail addresses, invalid phone numbers, pager numbers or answering services, is associated with fraudulent activity.
e. The Social Security Number provided is the same as that submitted by other applicants or customers.
f. 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 applicants or customers.
g. The applicant or customer fails to provide all required personal information on an application or in response to notification that the application is incomplete.
h. Personal identifying information is not consistent with personal identifying information that is on file with the City.
i. The applicant or customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

4. Unusual use of or suspicious activity relating to a covered account. Examples of suspicious activity include:
    a. Shortly following the notice of change of address for an account, City receives a request 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:
        i. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
    c. An account is used in a matter that is not consistent with established patterns of activity on the account. There is, for example:
        i. Nonpayment when there is no history of late or missed payments;
        ii. A material change in purchasing or consumption patterns;
    d. An account that has been inactive for a long 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 the transactions continue to be conducted in connection with the customer's account.
    f. The City is notified that that customer is not receiving paper account statements.
    g. The City is notified of unauthorized charges or transactions in connection with a customer's account.
    h. The City is notified by a customer, law enforcement or another person that it has opened a fraudulent account for a person engaged in identity theft.

5. Notice from customers, law enforcement, victims or other reliable sources regarding possible identity theft or phishing relating to covered accounts.

Prevention and Mitigation of Identity Theft

In the event that any City employee responsible for or involved in restoring an existing covered account or accepting payment for a covered account becomes aware of red flags indicating possible identity theft with respect to existing covered accounts, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Finance and Information Services Director. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee shall convey this information to the Finance and Information Services Director, who may in his or her discretion determine that no further action is necessary. If the Finance and Information Services Director in his or her discretion determines further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate by the Finance and Information Services Director:

a. Contact the customer;
b. Make the following changes to the account if, after contacting the customer, it is apparent that someone other than the customer has accessed the customer's covered account:
    i. Change any account numbers or other security devices that permit access to an account; or
    ii. Close the account.
c. Cease attempts to collect additional charges from the customer in the event the customer's account has been accessed without authorization and such access has caused additional charges to accrue;
d. Notify law enforcement, in the event that someone other than the customer has accessed the customer's account causing additional charges to accrue or accessing personal identifying information; or
e. Take other appropriate action to prevent or mitigate identity theft.

In the event that any City employee is responsible for or involved in opening a new covered account becomes aware of red flags indicating possible identity theft with respect an application for a new account, such employee shall use his or her discretion to determine whether such red flag or combination of red flags suggests a threat of identity theft. If, in his or her discretion, such employee determines that identity theft or attempted identity theft is likely or probable, such employee shall immediately report such red flags to the Finance and Information Services Director. If, in his or her discretion, such employee deems that identity theft is unlikely or that reliable information is available to reconcile red flags, the employee

shall convey this information to the Finance and Information Services Director, who may in his or her discretion determine that no further action is necessary. If the Finance and Information Services Director determines that further action is necessary, a City employee shall perform one or more of the following responses, as determined to be appropriate by the Finance and Information Services Director:

a. Request additional identifying information from the applicant;
b. Deny the application for the new account;
c. Notify law enforcement of possible identity theft; or
d. Take other appropriate action to prevent or mitigate identity theft.

Updating the Program

The Finance and Information Services Director shall annually review and as deemed necessary, update the Identity Theft Prevention Program along with any relevant red flags in order to reflect changes in risks to customers or to the safety and soundness of the City and its covered accounts from identity theft. In so doing, the Finance and Information Service Director shall consider the following factors and exercise its discretion in amending the program:

a. The City's experience with identity theft;
b. Updates in methods of identity theft;
c. Updates in customary methods used to detect, prevent, and mitigate identity theft;
d. Updates in the types of accounts that the City offers or maintains; and
e. Updates in service provider arrangements.

Any recommended material changes to the program shall be submitted to the City Council for consideration by the Council.

Outside Service Providers

In the event that the City engages a service provider to perform an activity in connection with one or more covered accounts, the Finance and Information Services Director shall exercise his or her discretion in reviewing such arrangements in order to ensure, to the best of his or her ability, that the service provider's activities are conducted in accordance with policies and procedures, agreed upon by contract, that are designed to detect any red flags that may arise in the performance of the service provider's activities and take appropriate steps to prevent or mitigate identity theft.

Identity Theft Policy Adoption

The City of Battle Ground's Identity Theft Program Policy shall be adopted by resolution of the City Council.

GLOSSARY

CITY: means the City of Battle Ground.

COVERED ACCOUNT: An account that a financial institution or 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 credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account. It also means any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

CREDIT: means the right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment therefore.

CREDITOR: means any person who regularly extends, renews, or continues to credit; any person who regularly arranges for extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit and includes utility companies and telecommunication companies.

CUSTOMER: means a person that has a covered account with a creditor.

IDENTITY THEFT: means a fraud committed or attempted using identifying information of another person without authority.

PERSON: means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

PERONAL IDENTIFYING INFORMATION: means a person's credit card account information, debit card information, bank account information and drivers' license information and for a natural person includes their social security number, mother's birth name, and date of birth.

RED FLAG: means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

SERVICE PROVIDER: means a person that provides a service directly to the City.