## EXHIBIT G

## FACT ACT IDENTITY THEFT PROTECTION POLICY

It is the policy of High Plains Metropolitan District (the "District") to maintain maximum compliance with Federal Regulations (16 C.F.R. §681.2), known as the Fair and Accurate Credit Transaction (FACT) Act, its amendments, laws and regulations.

The Board of Directors designates the District Manager as FACT Act Officer (defined below). The FACT Act Officer is responsible for coordinating and monitoring day-to-day FACT Act compliance and managing all aspects of the FACT Act Identity Theft Prevention Compliance Program (the "Program"), including, but not limited to, adherence of FACT Act and its implementing regulations.

The Program includes:

1. Approval of the written Program from the Board of Directors, or an appropriate committee of the Board; that directs management to create and implement a system of internal controls designed to:

    a. Identify Red Flags the District is likely to encounter;
    b. Document how the financial District's employees are to detect these Red Flags;
    c. Respond appropriately (risk based) to these Red Flags; and
    d. Ensure the Program is updated periodically.

2. Involvement of the Board of Directors, an appropriate committee, or a designated senior level employee ("FACT Act Officer") in the oversight, development, implementation and administration (to include an annual report to the Board of Directors) of the Program;

3. Staff training; and,

4. Due diligence (oversight) of service provider arrangements.

The Board of Directors will be ultimately responsible for the District's FACT Act compliance and will ensure that the FACT Act Officer has sufficient authority and resources (monetary, physical and personnel) to administer an effective risk based Program.

# FACT Act Identity Theft Prevention Procedures



---

## I. Guidelines for Establishment/Access to Accounts

1. Establishing Covered Accounts.

(a) As a condition to opening a covered account, each applicant shall provide the District with the following information:

(i) name;

(ii) address;

(iii) date of birth, if the applicant is an individual;

(iv) if the applicant is an individual, or an agent on behalf of an entity, an unexpired government-issued identification including a photograph, such as a driver's license or passport;

(v) for customers that are not individuals, such as corporations or limited liability companies, articles of incorporation, articles of organization or similar documentation.

To the extent any of the required information cannot be provided, verification of identity through other reasonable means, such as a review of public records, shall be undertaken.

(b) Each covered account shall be assigned a unique account number. The District may utilize computer software to randomly generate and/or encrypt account numbers.

2. Access to Covered Account Information.

The District shall take reasonable precautions to limit access to information regarding covered accounts and personal identifying information. Such reasonable precautions shall include:

(a) For paper records, the same shall be stored in locked cabinets or other facilities. Access to such facilities shall be restricted to personnel authorized by the District's Board of Directors or Manager ("Authorized Personnel").

(b) Access to electronic records shall be password protected and shall be limited to Authorized Personnel. Such passwords shall be changed on a regular basis, shall be at least 8 characters in length and shall contain letters, numbers and symbols.

(c) Any unauthorized access to or other breach of covered accounts is to be reported immediately to the FACT Act Officer and the locks and/or passwords changed immediately.

(d) Personal identifying information associated with covered accounts is confidential and any request or demand for such information shall be immediately forwarded to the FACT Act Officer.

3. Credit and Debit Card Payments.

(a) In the event that credit or debit card payments made over the Internet are processed through a third party service provider, such third party service provider shall certify that it has an adequate identity theft prevention program in place.

(b) Customer account statements and payment receipts shall include only the last four digits of the credit or debit card or the bank account used for payment.

## II. Identifying Relevant Red Flags

The District will consider the following risk factors in identifying relevant Red Flags for covered accounts, as appropriate:

1. The types of covered accounts it offers or maintains;
2. The methods it provides to open its covered accounts;
3. The methods it provides to access its covered accounts; and
4. Its previous experiences with identity theft.

The District will incorporate Red Flags from sources such as;

1. Incidents of identity theft that the District has experienced;
2. Methods of identity theft that the District has identified that reflect changes in identity theft risks; and,
3. Applicable supervisory guidance.

The categories of Red Flags will include but are not limited to:

1. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
2. The presentation of suspicious documents;
3. The presentation of suspicious personal identifying information, such as a suspicious address change;
4. The unusual use of, or other suspicious activity related to, a covered account; and,
5. 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 District.

## III. Detecting Red Flags

The detection of Red Flags in connection with the opening of new and existing accounts by:

1. Obtaining identifying information about, and verifying the identity of, a person prior to opening an account, for example, using the policies and procedures regarding identification and verification set forth in the District's rules, regulations and policies.

2. Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the ease of existing covered accounts.

## IV. Responding to Red Flags

The District will document an appropriate response to each Red Flag the District or customer has detected, commensurate with the degree of risk posed. In determining an appropriate response, the District will consider factors that may heighten the risk of identity theft. Those factors include unauthorized access to a customer's account records or notification that a customer has provided information to someone fraudulently or to a fraudulent website. Appropriate responses may include the following:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the customer;
3. Changing any passwords, security codes, or other security devices that permit access to a covered account;
4. Reopening a covered account with a new account number;
5. Not opening a new covered account;
6. Closing an existing covered account;
7. Not attempting to collect on a covered account or not selling a covered account to a debt collector;
8. Notifying law enforcement; or
9. Determining that no response is warranted under the particular circumstances.

## V. Updating the Program

The Districts will update the Program (including the Red Flag determined to be relevant) periodically to reflect changes in risks to customers or to the safety and soundness of the District from identity theft, based on factors such as:

1. The experiences of the District or creditor with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the District offers or maintains; and,
5. Changes in the business arrangements of the District, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

## VI. Methods for Administering the Program

The Board of Directors is ultimately responsible for the Identity Theft Prevention compliance program. However, the FACT Act Officer is responsible for the day-to-day administration and oversight. The FACT Act Officer is expected to:

1. Assign specific responsibility for the Program's implementation;

2. Review, prepare and provide at least annually, reports on the District's compliance with the Identity Theft Prevention compliance program, the effectiveness of the policy and procedures, significant incidents involving identity theft and management's response; and recommendations for material changes to the Program;

3. Obtain management approval of changes to the procedures and Board approval of policy as necessary to address changing identity theft risks; and,

4. Whenever the District engages a service provider to perform an activity in connection with one or more accounts the FACT Act Officer will ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a District could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the District, or to take appropriate steps to prevent or mitigate identity theft.

## VII. Other Requirements

The Districts will be mindful of other related legal requirements that may be applicable, such as:

1. Implementing any requirements regarding the circumstances under which credit may be extended when the District detects a fraud or active duty alert;

2. Implementing any requirements for furnishers of information to consumer reporting agencies for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and,

3. Complying with the prohibitions on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

## VIII. Identity Theft Prevention Program Red Flags

The District's Identity Theft Prevention Program will include, but not be limited to, the following Red Flags:

**Alerts, Notifications or Warnings from a Consumer Reporting Agency**

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity 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,

**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 District, such as a signature card or a recent check.

5. An application that appears to have been altered or forged, or appears to have been destroyed and reassembled.

**Suspicious Personal Identifying Information**

1. Personal identifying information provided is inconsistent when compared against external information sources used by the District or creditor. For example:

   a. The address does not match any address in the consumer report; or,

   b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

2. 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.

3. Personal identifying information such as a phone number or address is associated with known fraudulent activity as indicated by internal or third-party sources used by the District.

4. Personal identifying information of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the District, is provided, such as fictitious mailing address, mail drop addresses, prison addresses, invalid phone numbers, pager numbers or answering services.

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 District or creditor.

9. For Districts that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would by available from a wallet or consumer report.

**Unusual Use of, or Suspicious Activity Related to, the Covered Account**

1. Shortly following the notice of a change of address for a covered account, the District receives a request for the addition of authorized users on the covered account and/or a return of a prepaid service fee or other deposit.

2. A new 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.

3. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

   a. Nonpayment when there is no history of late or missed payments;

   b. A material change in electronic fund transfer patterns in connection with a deposit account; or

4. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

5. The District is notified that the customer is not receiving paper account statements.

6. The District is notified of unauthorized charges or transactions in connection with a customer's covered account.

**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 District or Creditor**

1. The District 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.