**JOINT**

**RESOLUTION NO. 3267-2009**
**RESOLUTION OF THE FORT BRAGG CITY COUNCIL**

**RESOLUTION NO. R157-2009**
**RESOLUTION OF THE FORT BRAGG REDEVELOPMENT AGENCY**

**RESOLUTION NO. ID 317-2009**
**RESOLUTION OF THE FORT BRAGG MUNICIPAL IMPROVEMENT DISTRICT NO. 1**

**ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM PURSUANT TO THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT AND THE FEDERAL TRADE COMMISSION'S RED FLAG RULES**

**WHEREAS**, the Federal Trade Commission ("FTC") and other federal regulatory agencies have recently published rules and guidelines for regulating identity theft; and

**WHEREAS**, the new regulations implement the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), 15 U.S.C. sections 1681 *et seq.*; and

**WHEREAS**, the FTC's regulations are known as the "Red Flag Rules" ("Rules"), 16 C.F.R. Part 681; and

**WHEREAS**, the Rules require "creditors" that maintain "covered accounts" to develop and implement an identity theft prevention program; and

**WHEREAS**, local governmental entities are considered to be "creditors" if the entity provides goods or services for which payment by the customer is deferred; and

**WHEREAS**, local governmental entities maintain "covered accounts" if the entity maintains (1) accounts designed to permit multiple payments or transactions, such as utility accounts, or (2) other accounts where there is a continuing relationship between the entity and customer and a reasonably foreseeable risk to customers or entity of identity theft exists; and

**WHEREAS**, the Rules require creditors that maintain covered accounts to develop and implement a written identity theft prevention program designed to detect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account; and

**WHEREAS**, the identity theft prevention program must be appropriate to the size and complexity of the creditor and the nature and scope of its activities; and

**WHEREAS**, the term "City" as used herein also includes the Fort Bragg Redevelopment Agency and the Fort Bragg Municipal Improvement District No.1. The "City" is a "creditor" that maintains "covered accounts" because the City provides water, sewer and business licensing services to customers as well as residential and commercial grant related loans and occasional loans subject to a micro-loan program, and maintains ongoing accounts for such customers and loan recipients; and

**WHEREAS**, the City desires to adopt an identity theft prevention program in compliance with the Rules to detect, prevent and mitigate identity theft in connection with the services it provides and the customer accounts it maintains for these services.

**WHEREAS,** based on all the evidence presented, the City Council finds as follows:

1. The Identity Theft Prevention Program ("Program"), attached as Exhibit A and incorporated herein by reference, has been developed in compliance with FACTA and the Rules.
2. The Program is appropriate to the size and complexity of the City and the nature and scope of its activities.

**NOW, THEREFORE, BE IT RESOLVED** that the City Council of the City of Fort Bragg, Agency Board of the Fort Bragg Redevelopment Agency and District Board of the Fort Bragg Municipal Improvement District No. 1 do hereby approve and adopt the Identity Theft Prevention Program pursuant to the Fair and Accurate Credit Transactions Act and the Federal Trade Commission's Red Flag Rules, attached as Exhibit A.

**BE IT FURTHER RESOLVED** that the Program shall be immediately implemented by the City Staff in the manner described in the Program.

**The above and foregoing Resolution was introduced by Council/Agency/Board Member Turner, seconded by Council/Agency/Board Member Melo, and passed and adopted at a regular meeting of the City Council of the City of Fort Bragg, Agency Board of the Fort Bragg Redevelopment Agency, and District Board of the Fort Bragg Municipal Improvement District No. 1 held on the 27th day of April, 2009, by the following vote:**

| | |
|---|---|
| **AYES:** | **Council/Agency/Board Members Turner, Gjerde, Melo, and Mayor/Chair Hammerstrom.** |
| **NOES:** | **None.** |
| **ABSENT:** | **Council/Agency/Board Member Courtney.** |
| **ABSTAIN:** | **None.** |

**DOUG HAMMERSTROM,**
**Mayor**

**ATTEST:**

**Cynthia M. VanWormer, CMC**
**City Clerk**

Exhibit A

# City of Fort Bragg
# Identity Theft Prevention Program

## I. PROGRAM INTRODUCTION

This Identity Theft Prevention Program ("Program") is developed and implemented pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), 15 U.S.C. 1681 *et seq.*, and regulations of the Federal Trade Commission ("FTC") known as the "Red Flag Rules" ("Rules"), 16. C.F.R. Part 681, that were designed and adopted in compliance with FACTA. The Rules require the City of Fort Bragg ("City") to develop and implement a program to detect, prevent and mitigate identity theft. (The term "City" as used herein also includes the Fort Bragg Redevelopment Agency and the Fort Bragg Municipal Improvement District No. 1.) This Program is intended to memorialize and outline the identity protections and procedures of the City and to formalize their continued use and update, as required by law.

## II. PROGRAM PURPOSE

A. The City places the highest priority on protecting any confidential financial and personal information submitted to it in the course of providing City services. This Program applies to the City's "covered accounts", such as water and sewer service customer accounts, business license accounts, and all grant or micro-loan program related loan accounts that are offered and maintained by the City.

B. This Program has the following purposes:

1. Identity "red flags" applicable to the accounts offered and maintained by the City and incorporate those "red flags" into this Program;

2. Detect those "red flags" that have been incorporated into this Program as they occur;

3. Ensure that staff responds appropriately to detected "red flags" so as to prevent and mitigate identity theft; and

4. Ensure that staff manages the receipt of any notices of address discrepancy from consumer reporting agencies in accordance with the Rules.

5. Ensure that this Program is updated periodically to reflect changes in identity theft risk to City customers or to the City.

6. Ensure that all service providers' activities are conducted in accordance with reasonable policies and procedures to detect, prevent and mitigate the risk of identity theft.

## III. DEFINITIONS

A. For purposes of this Program, the words set forth below shall have the following meanings:

1. "Account" means the water and sewer service accounts, business license accounts and all grant or micro-loan program related loan accounts offered and maintained by the City. These accounts qualify as "accounts" and "covered accounts" as defined by the Rules under 16 C.F.R. section 681.2.

2. "Consumer report" means a consumer report as defined by 15 U.S.C. section 1681a(d), also known as a "credit report," which is requested from a consumer reporting agency.

3. "Consumer reporting agency" means a consumer reporting agency as defined by 15 U.S.C. section 1681a(f), also known as a "consumer credit reporting agency," from which the City requests consumer reports. Consumer reporting agencies include, but are not limited to, Equifax Credit Information Services, Inc., Trans Union LLC and Experian Information Solutions, Inc.

4. "Customer" means a person that is applying to open an account or a person that has an existing account with the City.

5. "Finance Director" means the Finance Director of the City or his/her designee.

6. "Identifying information" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

   (a) Name, Social Security Number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; unique electronic identification number, address, or routing code, or as otherwise provided in 16 C.F.R. section 603.2.

7. "Identity theft" means a fraud committed or attempted using the identifying information of another person without authority or as otherwise provided in 16 C.F.R. section 603.2.

8. "Person" means a natural person, a corporation, government or governmental subdivision or agency, trust, estate, partnership, cooperative, or association.

9. "Red flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

10. "Service Provider" means a person that provides a service directly to the City in connection with one or more accounts.

11. "Staff" means the City staff who has access to identifying information of customers during the opening and maintaining of the accounts.

## IV. IDENTIFICATION OF RED FLAGS

A. The City has completed an assessment of the accounts it offers and maintains to determine potential red flags that may arise in connection to the accounts. The City has assessed the following: (1) the type(s) of Accounts offered and maintained by the City; (2) the methods the City uses to open accounts; (3) the methods it provides to allow Staff and customers to access accounts; and (4) the City's previous experiences with identity theft.

B. Based on the foregoing assessment, the City has determined that the existence of any of the following red flags in connection with any account indicates the possible existence of identity theft:

1. **Alerts, Notifications, or Other Warnings Received From Consumer Reporting Agencies or Service Providers**

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

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

   (c) A consumer reporting agency provides a notice of address discrepancy in response to a request for a consumer report.

   (d) A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a customer, such as:

      (i) A recent 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 with a third-party that was closed for cause or identified for abuse of account privileges by the third-party.

2. **Suspicious Documents**

   (a) Documents provided by the customer for identification appear to have been altered or forged.

(b) The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification.

(c) Other information on the identification is not consistent with information provided by the customer.

(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.

3. **Suspicious Customer Identifying Information**

(a) The identifying information provided by the customer is inconsistent when compared against 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) The identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the Social Security Number range and date of birth.

(c) The identifying information provided by the customer is associated with known fraudulent activity as indicated by internal or third-party sources used by the City. For example, the address or phone number on an application is the same as the address or phone number provided on a fraudulent application.

(d) The identifying information provided by the customer is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the City. For example:

(i) The address on an application is fictitious, a mail drop, or a prison; or

(ii) The phone number is invalid, or is associated with a pager or answering service.

(e) The Social Security Number provided by the customer is the same as that submitted by other customers opening accounts or having existing accounts with the City.

(f) The address or telephone number provided by the customer is the same as or similar to the address or telephone number submitted by an unusually large number of other customers opening accounts or having existing accounts with the City.

(g) A customer opening an account or having an existing account fails to provide all required identifying information on an application or in response to notification that the application is incomplete.

(h) The customer identifying information is not consistent with identifying information that is on file with the City.

(i) A customer opening an account or having an existing account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report. For example, the customer cannot answer a challenge question.

4. **Suspicious Activity**

(a) Shortly following receipt of a notice of a change of address from a customer for their account, the City receives additional requests for changes to the account.

(b) An account is used in a manner that is not consistent with established patterns of activity on the account. For example, the customer misses a payment when there is no history of late or missed payments.

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

(d) The City is notified that the customer is not receiving paper account statements or billing statements.

(e) The City is notified of unauthorized transactions in connection with a customer's account.

5. **Notices From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other persons**

(a) The City is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that the City has opened a fraudulent account for a person engaged in identity theft.

## V. DETECTION OF RED FLAGS

A. In connection with the opening and maintaining of any account, staff shall take the steps set forth below to detect red flags.

B. **Opening New Accounts:**

1. Staff shall verify the identity of each customer to the extent reasonable and practicable.

2. Staff shall obtain certain identifying information to verify the identity of each customer such as the name of the customer, date of birth for individuals, address, social security number, taxpayer identification number, passport number, alien registration number, etc.)

3. Staff shall review the obtained identifying information for any red flags identified in Section IV of this Program.

4. Staff shall obtain a copy of any of the following documents verifying the identifying information submitted by each customer: driver's license, passport, articles of incorporation, a government-issued business license, a partnership agreement, a trust instrument, etc.)

5. Staff shall review the obtained copies of documents verifying the identifying information submitted by each customer for any red flags identified in Section IV of this Program.

6. Staff shall verify the customer's identity through the comparison of the identifying information and any other information provided by the customer with information contained in City files, information obtained from a consumer reporting agency, or information obtained from any other source.

7. If the customer is not an individual and staff cannot verify the customer's identity through the steps listed above, staff may, based on a risk assessment, obtain identifying information of and verify the identity of the individuals with authority or control over the account, including signatories, pursuant to the steps listed above.

C. **Maintaining Existing Accounts:**

1. Staff shall verify the identity of each customer that requests account information, other than a request for the outstanding balance owed, to the extent reasonable and practicable.

2. Staff shall monitor the transactions of the Accounts maintained by the City for any red flags identified in Section IV of this Program.

3. Staff shall verify the validity of any notice of change of address or notice of change of billing information by contacting the customer and/or through the comparison of the identifying information in the notice of change of address or notice of change of billing information and any other information provided by the customer with information contained in City files, information obtained from a consumer reporting agency, or information obtained from any other source.

## VI. PREVENTING AND MITIGATING IDENTITY THEFT

A. In the event that staff detects any red flags related to an Account, staff shall respond to the red flag by taking one or more of the responsive actions set forth below. In responding to a red flag, staff shall take into consideration which actions are appropriate for the degree of risk of identity theft posed by the red flag.

B. **Responses to Detected Red Flags**

1. Mark an account in the billing system and monitor it for evidence of identity theft.

2. Contact the customer.

3. Change any passwords, security codes or other security devices that permit access to an account.

4. Reopen an account with a new account number.

5. Refuse to open a new account.

6. Close an existing account.

7. Not attempt to collect on an account or not sell the account to a debt collector.

8. Notify law enforcement and/or prosecutorial agencies.

9. Determine that no response is warranted under the particular circumstances.

10. Notify the Finance Director for determination of the appropriate step(s) to take.

C. Each situation shall be evaluated on a case-by-case basis. In determining an appropriate response, Staff shall consider any aggravating factors that may heighten the risk of identity theft. For example, a data security incident that results in unauthorized access to a customer's Account records held by the City, receipt of notice that a data security incident has occurred that results in unauthorized access to a customer's account records held by a third-party, or

receipt of notice that a customer has provided information relating to an Account with the City to someone fraudulently claiming to represent the City or to a fraudulent website.

D. **Internal Protection of Customer Identifying Information**

1. In order to further prevent the likelihood of identity theft occurring with respect to Accounts offered and maintained by the City, Staff shall 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) Ensure that office computers from which customer identifying information may be accessed are password protected.

(c) Keep all desks, workstations, work areas, printers, fax machines and common shared work areas clear of documents containing customer identifying information when not in use.

(d) Ensure computer virus protection is up to date.

(e) Lock all file cabinets, desk drawers, overhead cabinets and any other storage space containing documents with customer identifying information when not in use.

(f) Lock storage rooms containing documents with customer identifying information at the end of each workday or when unsupervised.

## VII. NOTICE OF ADDRESS DISCREPANCY

A. A notice of address discrepancy is a notice sent to the City by a consumer reporting agency as required by FACTA to inform the City of a substantial difference between the address for the customer that staff provided to the consumer reporting agency to request the consumer report and the address(es) in the consumer reporting agency's file for the customer.

B. The receipt of a notice of address discrepancy is a red flag pursuant to Section IV(B)(1)(c) and shall be treated as any other red flag in accordance with the detection, prevention and mitigation procedures set forth in Sections V and VI of this Program. In addition, when the City receives a notice of address discrepancy, the procedures set forth in this Section VII of this Program shall be followed.

C. **Customer Verification**

1. When the City receives a notice of address discrepancy, staff shall take any necessary steps that are reasonable and practicable to form a reasonable belief

that the consumer report received relates to the customer about whom staff requested the consumer report. The steps, which shall be taken by staff, to form such a reasonable belief may include, but not be limited to:

(a) Comparing the information in the consumer report provided by the consumer reporting agency with information the City:

(i) Obtains and uses to verify the identity of customers pursuant to Section V of this Program.

(ii) Maintains in its own records, such as applications, change of address notifications and other customer account records.

(iii) Obtains from third-party sources.

(b) Verifying the information in the consumer report provided by the consumer reporting agency with the customer.

D. **Furnishing Confirmed Address to the Consumer Reporting Agency**

1. Staff shall furnish an address for the customer that the City has reasonably confirmed is accurate to the consumer reporting agency from whom the City received the notice of address discrepancy when all of the following conditions are satisfied:

(i) Staff can form a reasonable belief that the consumer report relates to the customer about whom staff requested the consumer report;

(ii) The City establishes a continuing relationship with the customer; and

(iii) Regularly and in the ordinary course of business, staff furnishes information to the consumer reporting agency from which the notice of address discrepancy was received.

2. A continuing relationship with the customer is not established, for purposes of satisfying the condition contained in Section VII(D)(1)(ii) of this Program, if:

(a) The consumer report was requested for purposes of opening a new account with the customer, but the new account is not opened; or

(b) The consumer report was requested for purposes relating to an existing account.

3. Staff shall reasonably confirm that the address provided by the customer is accurate, despite being different from the address(es) in the consumer

reporting agency's file for the customer, by taking one or more of the following steps:

(a) Verifying the address with the customer about whom it has requested the consumer report.

(b) Reviewing its own records to verify the address of the customer.

(c) Verifying the address through third-party sources.

(d) Using other reasonable means.

4. The confirmed address of the customer shall be furnished to the consumer reporting agency pursuant to the following:

(a) In writing.

(b) Upon the approval of the Finance Director.

(c) As part of the information the City regularly furnishes to the consumer reporting agency for the reporting period in which the City establishes a relationship with the customer.

## VIII. ADMINISTRATION AND UPDATING OF THIS PROGRAM

A. This Program shall be administered by the Finance.

1. The Finance Director shall be responsible for:

(a) Assigning the specific responsibility for this Program's implementation to the appropriate staff.

(b) Review annual reports prepared by staff regarding compliance by the City with FACTA and the Rules.

(c) Approve material changes to this Program as necessary to address changing identity theft risks.

B. **Annual Reports**

1. Staff shall provide annual reports to the Finance Director regarding compliance of this Program with the Rules.

2. The annual reports shall address any material matters related to this Program and evaluate any issues related to this Program, including:

(a) The effectiveness of this Program in addressing the risk of identity theft in connection with the opening and maintaining of accounts.

(b) Any arrangements with new service providers or any changes in the arrangements with existing service providers to detect, prevent and mitigate identity theft, if applicable.

(c) Any significant incidents involving identity theft and Staff's response to those incidents.

(d) Changes in methods of identity theft.

(e) Changes in methods to detect, prevent and mitigate identity theft.

(f) Changes in the types of accounts the City offers or maintains.

(g) Recommendations for material changes to this Program.

C. **Updating this Program**

1. Upon review of the annual reports submitted by staff and the recommendations contained therein, the Finance Director shall determine whether material changes to this Program are necessary to update this Program to better detect, prevent and mitigate identity theft related to the accounts offered and maintained by the City.

2. If the Finance Director determines that such an update to this Program is necessary, the Finance Director shall direct Staff to draft the recommended material changes to this Program, which shall be submitted to the Finance Director for approval.

D. **Staff Training**

1. The Finance Director shall ensure that Staff is trained as necessary to effectively implement this Program, which includes training regarding any approved material changes to this Program.

## IX. OVERSIGHT OF SERVICE PROVIDERS

A. The City shall take steps necessary to ensure that the activity of any service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

B. The Finance Director shall determine which steps are necessary to ensure the safety of any service providers activities related to the accounts. The Finance Director may, if he or she deems it appropriate, require a service provider by contract to design and implement policies and procedures to detect relevant red flags that may arise in the performance of the Service Provider's activities related to the accounts, and either report the red flags to the Finance Director or to take appropriate steps to prevent or mitigate identity theft.