AVE MARIA UTILITY COMPANY, LLLP

RED FLAG IDENTITY THEFT PREVENTION PROGRAM

AVE MARIA, FLORIDA

Prepared by

CH2M HILL OMI

May 1, 2009

Purpose Statement

The Ave Maria Utility Company, LLLP Red Flag Identity Theft Prevention Program ("Program") has been developed to safeguard against Identity Theft. This Program is intended to safeguard Covered Accounts and Covered Account Holders from Identity Theft and to identify Red Flags that may indicate a Covered Account Holder is attempting to commit a theft by fraud by means of using another's Personal Identifying Information.

The purpose of this policy is to identify patterns, practices, or specific activities that indicate the possible existence of Identity Theft and to take all reasonable steps to detect, prevent, and mitigate the Identity Theft of the Utility's Covered Account Holders.

Administration of the Program

The Ave Maria Utility Company, LLLP (hereafter "Utility") is responsible for the development, implementation, oversight and continued administration of the Program. The Utility shall train staff, as necessary, to effectively implement the Program; and shall exercise appropriate and effective oversight of service provider arrangements.

The Utility is responsible to include this Program for Identity Theft protection and Red Flag alerts as part of new employee orientation and shall document the review of its policies and concepts.

Department directors are responsible for being familiar with the Program and for meeting with their staff to assess current compliance with and effectiveness of the Program.

Employees are responsible for complying with the Program and any internal processes as directed by their director. Noncompliance may result in disciplinary action. Employees are encouraged to contact their supervisor if they have questions about compliance with this Program.

Definitions

Account means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes.

Covered Account means:

a. Any account the Utility offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions. Examples are credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts.

b. Any other account the Utility offers or maintains for which there is a reasonably foreseeable risk to Covered Account Holders or to the safety and soundness of the Utility from Identity Theft. Examples include small business accounts, sole proprietorship accounts, or single transaction consumer accounts that may be vulnerable to Identity Theft. Unlike consumer accounts designed to permit multiple payments or transactions – they always are “Covered accounts” under the Rule – other types of accounts are “Covered accounts” only if the risk of Identity Theft is reasonably foreseeable.

Covered Account Holder means a person or business entity that has a Covered account with the Utility.

Credit means the right granted by the Utility to a Covered Account Holder for payment of debt or to incur debts and defer its payment or to purchase Utility services or property and defer payment.

Creditor for the purpose of this program includes a person or entity that arranges for the extension, renewal or continuation of credit. A creditor includes businesses or organizations that regularly defer payment for goods or services or provide goods or services and bill Covered Account Holders later. By providing water and sewer utilities and billing based on Covered Account Holder usage the Utility is considered a Creditor.

Financial institution means a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a “transaction account” belonging to a Covered Account Holder.

FTC means the Federal Trade Commission.

Identity Theft means a fraud committed or attempted using Personal Identifying Information of another person without authority, or consent, to do so.

Personal 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 name, address, telephone number, social security number, date of birth, government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number or unique electronic identification number.

Red Flag means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Service Provider means a person or business entity that provides a service directly to the Utility relating to or connection with a Covered account.

I. Red Flags

Red Flags are potential patterns, practices, or specific activities that indicate the possibility of Identity Theft. As the Red Flag Identity Theft Prevention Program was developed, site-specific risk factors, probable sources of Red Flags and common Red Flag categories that could be of significance to the program were all considered.

Risk factors vary, depending on the types of accounts that are maintained. Red Flags for consumer accounts may not be the same as those for business accounts and Red Flags for accounts opened or accessed online or by phone may differ from those involving in-person contact. In developing this Program, consideration was given to the types of accounts we maintain; the methods used to open Covered Accounts; and how access to those Covered Accounts is provided. Sources of Red Flags have been reviewed and considered in the preparation of the Program. However, it is imperative that the Utility remain mindful that technology and criminal techniques change often. Therefore, the Utility shall review the Program periodically to address new threats.

Categories of common Red Flags have been outlined in guidance provided by the FTC. The guidance details five specific categories of warning signs, or Red Flags, to consider when developing a Program. The information provided for each category was taken into account as the Utility's Program developed. Guidance from the FTC includes:

1. Alerts, Notifications, and Warnings from a Credit Reporting Company.

Changes in a credit report or a consumer's credit activity may signal Identity Theft. These changes include:

- A fraud or active duty alert on a credit report;
- A notice of credit freeze in response to a request for a credit;
- The report of a notice of address discrepancy provided by a credit reporting agency; or
- A credit report indicating a pattern of activity inconsistent with the person's history – for example, an increase in the volume of inquiries or the use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account that was closed because of an abuse of account privileges.

2. Suspicious Documents.

Signs of Identity Theft in submitted paperwork may signal an Identity Theft. Examples of Red Flags involving documents include:

- Identification that looks altered or forged;
- The person presenting the identification doesn't look like the photo or match the physical description information on the identification;
- The person presenting the identification is providing information that doesn't match with other information, like a signature card or recent check
- An application that looks like it's been altered or forged; or
- A document that has been torn up and reassembled.

3. Suspicious Personal Identifying Information.

Identity thieves may use personally identifying information that doesn't appear accurate. Examples of Red Flags involving identifying information include:

- Inconsistencies with what else you know – for example, an address that doesn't match the credit report, the use of a Social Security number that's listed on the Social Security Administration Death Master File, or a number that hasn't been issued, according to the monthly issuance tables available from the Social Security Administration;
- Inconsistencies in the information the Covered Account Holder has given you – for example, a date of birth that doesn't correlate to the number range on the Social Security Administration's issuance tables;
- An address, phone number, or other personal information that's been used on an account you know to be fraudulent;
- A bogus address, an address for a mail drop or prison, a phone number that's invalid, or one that's associated with a pager or answering service;
- A Social Security number that's been used by someone else opening an account;
- An address or telephone number that's been used by many other people opening accounts;
- A person who omits required information on an application and doesn't respond to notices that the application is incomplete; or
- A person who can't provide authenticating information beyond what's generally available from a wallet or credit report – for example, a person who can't answer a challenge question.

4. Suspicious Account Activity.

Sometimes a sign of fraud is how the account is being used. Examples of Red Flags related to account activity include:

- Change of address for an account followed by a request to change the account holder's name;
- Account used in a way that is not consistent with prior use – for example, increased activity;
- Mail sent to the account holder is repeatedly returned as undeliverable;
- Notice to the Utility that a Covered Account Holder is not receiving mail sent by the Utility;
- Notice to the Utility that an account has unauthorized activity;
- Breach in the Utility's computer system security; or
- Unauthorized access to or use of Covered Account Holder account information.

5. Notice from Other Sources.

Sometimes a Red Flag that an account has been opened or used fraudulently comes from a Covered Account Holder, a victim of Identity Theft, a law enforcement authority, or another third party.

II. DETECTING RED FLAGS

The Utility collects a substantial amount of Personal Identifying Information regarding the Utility's Covered Account Holders through a variety of processes. For this reason, the Utility staff is required to assess and address risks associated with the collection of this information. Collecting Personal Identifying Information requires the Utility and its employees to make a good faith attempt to verify the identity of a person doing business with the Utility.

New Accounts

When opening a new account with the Utility, prospective Covered Account Holders must complete an application for service and as part of the application process will be required to submit the following information:

- Name to appear on the account;
- Address location where service shall be provided;
- Billing address;
- Contact information, including phone number and email address;
- Date of Birth;
- Last 4 digits of Social Security Number;
- Tax Identification Number (Business Accounts); and
- Valid government-issued photo identification as proof of identity.

When an application for a new account is received, the Utility will:

- Verify the Covered Account Holder's identity (for instance, review a driver's license or other identification card); or
- Verify through documentation or first-hand knowledge the existence of a business entity.

Existing Accounts

It is the responsibility of the Utility to maintain reasonable safeguards to prevent and mitigate Identity Theft for Covered Accounts and Covered Account Holders. The most common identifying information collected by the Utility is documentation that contains sensitive data such as:

- Security deposits;
- Permits;
- Credit card numbers; and

- Bank draft account information (bank routing and account number).

The Utility recognizes that there are a number of practices and specific activities that might indicate the possible existence of Identity Theft. Therefore the Utility has instituted reasonable procedures to authenticate Covered Account Holders, monitor transactions, and verify the validity of change-of-address requests.

Red Flags associated with Covered Account Holder accounts or for the establishment of a Covered Account Holder account includes:

- Inquiries inconsistent with the history and usual pattern of activity of a Covered Account Holder including:
    - A recent and significant increase in the volume of inquiries;
    - A material change in the use of services, or other unusual activity associated with the account;
    - An account with another municipal entity that was closed for cause or identified for abuse of account privileges; or
    - Documents provided for identification appear to have been altered or forged;
- A photograph or physical description on the identification is not consistent with the appearance of the applicant or Covered Account Holder presenting the identification;
- Information on the identification that is not consistent with information provided by the person opening a new account or Covered Account Holder presenting the identification;
- Information on the identification is not consistent with readily accessible information that is on file, such as a prior Covered Account Holder file;
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled; or
- Business account fees are not paid from a check matching the name of the business on the application.

Other potential Red Flags may include the presentation of suspicious information that may contain personal Identifying Information that is inconsistent when compared against external information sources such as:

- An address that does not match any address in the data file;
- Personal Identifying Information provided by the Covered Account Holder that is not consistent with other Personal Identifying Information provided by the Covered Account Holder;
- The Personal Identifying Information provided is associated with known fraudulent activity as indicated by internal or third-party sources;
- An address on an application is the same as the address provided on a fraudulent application;
- A phone number on an application is the same as the number provided on a fraudulent application;

- The Personal Identifying Information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources. For example:
    - The address on an application is fictitious, a mail drop, or a prison;
    - A phone number that is invalid, or is associated with a pager or answering service;
    - The Social Security number provided is the same as that submitted by other persons opening an account or another Covered Account Holder;
    - An address or telephone number that 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 Covered Account Holders;
    - The person opening the account fails to provide all required Personal Identifying Information on an application or in response to notification that the application is incomplete;
    - The Personal Identifying Information provided is not consistent with information that is on file with the Utility; or
    - The person or Covered Account Holder opening the account cannot provide authenticating information beyond that which generally would be available from a wallet.

Unusual or suspicious activity that may be an indicator of Identity Theft includes:

- A notice of a change of address for a Covered Account Holder account, followed by a request for the addition of authorized users on the account;
- Mail sent to the Covered Account Holder is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the Covered Account Holder's Covered account;
- The Utility is notified that the Covered Account Holder is not receiving their utility bill;
- The Utility is notified of unauthorized charges or transactions in connection with the Covered Account Holder's account;
- Payments are made in a manner associated with fraud;
- An existing account with a stable history shows irregularities;
- Alerts, notifications, or other warnings received from local law enforcement or other governmental organizations; or
- A fraud alert or the United States Post Office providing a notice of address discrepancy.

III. RESPONSES TO RED FLAGS

Appropriate responses to detected Red Flags shall be taken within 24 hours of discovery. The response shall be commensurate with the degree of risk posed. The FTC has outlined appropriate responses which include:

- The monitoring of a Covered account for evidence of Identity Theft;
- Contacting the Covered Account Holder;

- Changing any passwords, security codes or other security devices that permit access to a Covered account;
- Closing an existing Covered Account then reopening it with a new account number;
- Not opening a new Covered Account;
- Notifying a supervisor;
- Notifying law enforcement; or
- Making a determination that no response is warranted under the particular circumstances.

IV. PROCEDURES FOR SAFEGUARDING PERSONAL IDENTIFYING INFORMATION

The Utility shall implement and maintain reasonable safeguards to protect the security and confidentiality of Personal Identifying Information, including its proper disposal. Personal Identifying Information collected by the Utility includes:

- A Covered Account Holder's name in combination with other contact information and a driver's license or identification card; and
- Credit, or debit card numbers with security or access codes.

When indicated, an information discrepancy will be reported to the supervisor for further review and verification of the information. Verification may include a verification of identification in person at the Utility office.

An employee shall also report to her/his supervisor an appearance that account documents have been altered or forged when compared to other documents in a Covered Account Holder file. The employee shall immediately alert her/his supervisor of a situation where a Covered Account Holder or applicant presents an invalid identification or identification that appears forged for the purpose of obtaining access to account information.

The supervisor will investigate, and if appropriate, contact the Collier County Sheriff Department and request their assistance with an investigation.

Access to Account Information

Access to account information in person will be permitted by the Utility only after verifying the Covered Account Holder's identity through photo identification.

Access to account information can be obtained over the internet utilizing the Utility account number and a PIN number. Information available online is limited to basic contact information and history of payments. Bank draft information (bank name, routine number, and account information) are stored electronically in the database and accessible only through the application with approved credentials. Credit card information is not stored electronically or on the premises.

Access to Covered Account Holder account information via telephone requires the Covered Account Holder to verify his or her identity by providing the address, name on the account, account holder's date of birth and last 4 digits of the social security number on file.

Utility Responsibilities

When there is a lack of correlation between information provided by a Covered Account Holder and information contained on file the requested information the Utility will not disclose information without having first cleared any discrepancies with the information provided.

The Utility shall not print Tax Identification Numbers on any mailed materials unless masked; and are prohibited from publicly posting or displaying Tax Identification Numbers. Tax Identification Numbers **will not** be provided by Utility employees, either verbally or in writing, even when a Covered Account Holder is asking for his/her own information.

The Utility may not request sensitive data on certain forms if the data is not absolutely necessary for the Covered Account.

Employees shall note unusual use of accounts, or suspicious activities related to accounts and promptly notify a supervisor when there are an unusually high number of inquiries on an account, coupled with a lack of correlation in the information provided by the Covered Account Holder.

Utility will monitor transactions and verify the validity of change of address requests, in the case of existing accounts.

If the Utility discovers that any of its Covered Account Holders have become a victim of Identity Theft through personal information used by the organization in opening or maintaining an account, management shall take appropriate steps that it deems necessary to mitigate the impacts of such Identity Theft. These steps may include, but are not limited to the steps outlined above in **Section III. Responses to Red Flags**, and reiterated here:

- Monitoring an account for evidence of Identity Theft;
- Contacting the Covered Account Holder;
- Changing any passwords, security codes, or other security devices that permit access to an account;
- Closing an existing Covered account then reopening it with a new account number.
- Closing an existing or compromised account;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

Record Retention and Disposal

The improper disposal of old receipts, service applications, papers or CDs containing personally identifying information facilitates fraud and exposes Covered Account Holders to the risk of Identity Theft. The proper disposal of sensitive information ensures that it cannot be read or reconstructed. To minimize the risk of Identity Theft the Utility has instituted disposal practices that are reasonable and appropriate for the information on file.

The Staff shall purge and shred documents that have reached end of a required detention period. All documents containing sensitive information will be shredded prior to disposal.

When old computers and other electronic storage devices are disposed of, the hard drives are erased and software programs are uninstalled. Computers that are returned to leaser will be further erased so that the files are no longer recoverable.

Sensitive documents are stored in filing cabinets behind locked doors. Entry to the filing area is limited to Utility staff.

V. DATA SECURITY

Effective data security starts with assessing what information you have and identifying who has access to it. Understanding how personal information moves into, through, and out of your business and who has—or could have—access to it is essential to assessing security vulnerabilities. It is universally accepted that the most effective data security plans incorporates four key elements: physical security, electronic security, employee training, and the security practices of third party vendors and service providers.

1. Physical Security

Data compromises tend to happen the old-fashioned way—through lost or stolen paper documents and electronically — through computer data storage. To protect against Identity Theft from accrued documentation the Utility will:

- Store paper documents, files, and backup devices (CDs, floppy disks, zip drives, etc) containing personally identifiable information in a locked room.
- Limit access to employees with a legitimate business need, control who has a key, and restrict the number of keys.
- Require that files containing personally identifiable information be kept in filing cabinets except when an employee is working on the file.
- Train employees not to leave sensitive papers out on their desks when they are away from their workstations.
- Ensure the complete and secure destruction of paper documents and computer files containing Covered Account Holder information;
- Require employees to put files away, log off their computers, and lock office doors at the end of the day.
- Require all office computers to be password protected and that computer screens lock after a set period of idle time;
- Require and keep only the kinds of Covered Account Holder information that are necessary for utility purposes
- Ensure that website is secure or provide clear notice that the website is not secure
- Ensure that computer virus protection is up to date
- Implement appropriate access controls for Utility buildings. The Utility will also train employees what to do and whom to call if they see an unfamiliar person on the premises.
- Maintain secure offsite storage facilities only when necessary and limit employee access to those with a legitimate business need.

- If necessary, ship sensitive information using outside carriers or contractors that allow delivery tracking services. All shipped information will be encrypted and inventoried.

2. Electronic Security

Computer security is very important to the Utility. A vulnerable computer or unprotected Internet service provider can result in the fraudulent use of the confidential information of all Utility customers. To protect Covered Account Holders from electronic Identity Theft the Utility will:

- Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting utility business.
- Encrypt sensitive information sent to third parties over public networks and the internet. Email transmissions containing personal information will also be encrypted whenever possible.
- Regularly run up-to-date anti-virus and anti-spyware programs on individual computers and on network servers.
- Regularly check expert websites (such as www.sans.org) and Utility's software vendors' websites regularly for alerts about new vulnerabilities, and implement policies for installing vendor-approved patches to correct problems.
- Scan computers on Utility's network to identify and profile the operating system and open network services. Services that are not needed will be disabled to prevent hacks or other potential security problems.
- Received or transmitted credit card information or other sensitive financial data is encrypted through a secure connection that protects the information in transit.
- Periodically review the security of Utility's web applications. Web applications may be particularly vulnerable to a variety of hack attacks.

Password Management

Control access to sensitive information requires that Utility employees use "strong" passwords on their computers. Experts in the field of technological security agree that the longer the password, the better the security. The Utility requires employees to choose unique passwords that provide a combination of a mix of letters, numbers, and characters. The Utility also requires scheduled changes in passwords every 60 to 90 days. Access to billing software requires an additional user name and password, providing an additional layer of protection.

Wireless and Remote Access

The personal information of Covered Account Holders is transmitted via both cable and wireless devices. The Utility maintains a secure, password-protected, wireless network.

3. Employee Training

The Red Flag Identity Theft Prevention Program is only effective when properly implemented by the employees of the Utility. The Utility recognizes that well-trained employees are the best defense against Identity Theft and data breaches and therefore, their training emphasizes the importance of meaningful data security practices.

The Utility conducts background checks (national criminal check for felonies, state criminal check for misdemeanors, and motor vehicle check) for all employees before their hire. The Utility stresses to each employee their responsibility to follow the confidentiality and security standards for handling sensitive data. Adherence to the policies of this Program is not only part of their job duties but is also a legal requirement of them to keep Covered Account Holder information secure and confidential. Employees who leave the Utility's employ no longer have access to sensitive information. Upon termination passwords are deleted and keys and identification cards surrendered as part of the exit procedures.

Employees are trained in the Utility's policies regarding confidentiality and data security. Employees are advised to be suspicious of unknown callers claiming to need account information to process an order or asking for Covered Account Holder information. When a customer's identity is in doubt, information is verified by the Utility using contact information known to be genuine.

All employees are required to notify their supervisor immediately if there is evidence of a real or potential security breach.

4. Third Party Contractors

The Utility has several business relationships with third party contractors, including CSI (Collectors Solutions Incorporated) – through whom credit card payments are made online - and Harris – the utility software provider of InHance, a web application software. Within these business relationships, the third party contractor may require access to information regarding a Covered Account Holder. Although these requests are rare, the Utility will continue to verify that the third party contractor's Identity Theft practices are consistent with the Utility's Identity Theft policies by:

- Amending contractor agreements to incorporate these requirements; or
- Determining through written acknowledgment that the third party contractor has reasonable alternative safeguards that provide the same or a greater level of protection for customer information as provided by the Utility.

All third party Contractors and Service Providers are required to notify the Utility of any security incidents they experience, even if the incidents may not have led to an actual compromise of Utility data.

Responding to Data and Security Breaches

When a security compromise is discovered that could result in harm to a Covered Account Holder or business, local law enforcement will be contacted immediately. It has been demonstrated that the sooner law enforcement learns about the theft, the more effective they can be in mitigating damage. If the local authorities are not able to investigate the breach, the FTC, the local office of the Federal Bureau of Investigation, and the U.S. Secret Service will be contacted. Should an incident involve mail theft, the U.S. Postal Inspection Service will be notified. Contact Information for all parties is provided in **Section IV. Contact Information**.

Notifying Other Effected Financial Institutions

If account information (credit card or bank account numbers) is stolen for accounts that the Utility does not maintain, the Utility is required to notify the institution that manages the account so that they can monitor the breached account for fraudulent activity.

If names and Tax Identification Numbers are been stolen, the Utility will contact the major credit bureaus for additional information or advice. If the compromise involves a large group of people, Utility may need to provide Covered Account Holders with free access to a credit monitoring bureau to enable them to monitor their accounts for fraudulent activity. Contact information for the credit monitoring bureaus is provided in **Section IV. Contact Information**.

Notifying Individuals

Early notification to individuals whose personal information has been compromised allows them to take steps to mitigate the misuse of their information. To determine if notification is warranted, Utility will consider the nature of the compromise, the type of information taken, the likelihood of misuse, and the potential damage arising from misuse. For example, thieves who have stolen names and Tax Identification Numbers can use this information to cause significant damage to a victim's credit record. Individuals who are notified early can take steps to prevent or limit any harm.

When notifying individuals, The Utility will follow the recommendations of the FTC whereby they shall:

- Consult with law enforcement about the timing of the notification so it does not impede any ongoing investigation.
- Designate a contact person within the Utility to release information. That contact person will be given the latest information about the breach, the Utility's response, and how individuals should respond.

The FTC recommends that any communication with Utility's customers:

- Clearly describes what the Utility knows about the compromise. Utility's written notification will include information about how the breach happened, what information was taken, how the thieves have used the information (if known), and what actions the Utility has taken to remedy the situation. Customers who have additional questions will be provided with contact information. No information shall be included in any communication without prior consultation of law enforcement so that the notification does not hamper any ongoing investigation.
- Explains what responses may be appropriate for the type of information taken. For example, customers whose Tax Identification Numbers have been stolen should contact the credit bureaus to ask that fraud alerts be placed on their credit reports.
- Includes current information about Identity Theft. The FTC's internet site at www.ftc.gov/idtheft has information to help individuals guard against and deal with Identity Theft.
- Provides contact information for the law enforcement officer working on the case (as well as the case report number, if applicable) for victims to use. The Utility shall alert the law enforcement officer working the case that this information is being shared. Identity Theft victims often can provide important information to law enforcement. Victims should be advised to request a copy of the police report and make copies for creditors who have accepted unauthorized charges, as the report provides important evidence that can help absolve a victim of fraudulent debts.

- Encourages those who discover that their information has been misused to file a complaint with the FTC at www.ftc.gov/idtheft or at 1-877-ID-THEFT (877-438-4338). Information entered into the Identity Theft Data Clearinghouse, the FTC's database, is made available to law enforcement.

VI. UPDATING THE PROGRAM

The Red Flag Identity Theft Prevention Program shall be updated periodically to reflect changes in risks to Covered Account Holders or to the safety and soundness of the Utility from Identity Theft based on factors such as:

- The experiences of the organization with Identity Theft.
- Changes in methods of Identity Theft.
- Changes in methods to detect prevent and mitigate Identity Theft.
- Changes in the types of accounts that the organization offers or maintains.
- Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures and service provider arrangements.

This Program shall be reviewed on an annual basis and shall be amended as necessary to ensure compliance with the Red Flag Identity Theft Prevention Act.

VII. CONTACT INFORMATION

1. **LOCAL LAW ENFORCEMENT:**

   Collier County Sheriff Dept Main Number
   239.774.4434
   Immokalee Sheriff Station
   239.657.6168
   Orange Tree Sheriff Station
   239.657.2878

2. **UTILITY PROJECT MANAGER:**

   Jason Vogel
   239.289.3542

3. **FEDERAL TRADE COMMISSION:**

   Consumer Response Center, FTC
   600 Pennsylvania Avenue, N.W.
   Washington, DC 20580
   1 877 ID THEFT (877.438.4338)
   www.ftc.gov/bcp/edu/microsites/idtheft/

4. **FBI LOCAL OFFICE:**

   5525 West Gray Street
   Tampa, Florida 33609
   www.tampa.fbi.gov

813.253.1000

5. **US SECRET SERVICE LOCAL OFFICE:**

   Miami Office
   305.863.5000

6. **US POSTAL SERVICE:**

   To report scams or deceptive ads via the mail, or postage fraud:
   https://postalinspectors.uspis.gov/forms/MailFraudComplaint.aspx

   To report Identity Theft via us mail:
   https://postalinspectors.uspis.gov/forms/idtheft.aspx

7. **CREDIT MONITORING BUREAUS:**

   TransUnion
   P.O. Box 6790
   Fullerton, CA 92834
   Phone: 800.680.7289

   Equifax
   Equifax Information Services, LLC.
   PO Box 740250
   Atlanta GA 30374-0250
   Phone: 800.525.6285
   Email: businessrecordsecurity@equifax.com

   Experian
   Experian Security Assistance
   P.O. Box 1017
   Allen, TX 75013
   Phone: 888.397.3742
   Email: BusinessRecordsVictimAssistance@experian.com