Memorandum

MIAMI-DADE COUNTY

Date: May 18, 2010

To: Honorable Chairman Dennis C. Moss
and Members, Board of County Commissioners

Agenda Item No.12(A)(4)

From: George M. Burgess
County Manager

Subject: Resolution Approving the Miami-Dade County Identity Theft Prevention Program in Accordance with the Fair and Accurate Credit Transactions Act of 2003

RECOMMENDATION

It is recommended that the Board of County Commissioners (Board) approve the attached resolution adopting the Miami-Dade County Identity Theft Prevention Program (Program) designed to identify and respond to patterns, practices and activities known as "Red Flags" that could indicate identity theft. This program is a requirement of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

SCOPE OF AGENDA ITEM

This resolution will have a countywide impact.

FISCAL IMPACT/FUNDING SOURCE

This resolution will require a one-time expenditure of $16,160 to create and implement an electronic database to record and store data related to the Identity Theft program. Annual recurring costs of $4,160 for database maintenance and $8,100 to roll out and support a countywide online training program will also be needed. These will be funded through the FY2010-11 IT funding model which is supported by the General Fund and Proprietary Funds.

TRACK RECORD/MONITOR

This Program will be monitored by a Program Administrator to be appointed by the County Manager.

BACKGROUND

On November 9, 2007, the Federal Trade Commission (FTC) issued rules and regulations requiring financial institutions and creditors to develop and implement written identity theft prevention programs under Section 114 of the FACT Act. The FACT Act mandates that such creditors that hold "Covered Accounts" develop and implement an Identity Theft Prevention Program for both new and existing accounts.

A creditor is defined as an organization that provides goods and services to customers and allows customers to pay at a later date, arrange for and grants loans, extends credit or makes credit decisions.

A covered account is one for which the organization maintains accounts for personal, family and household purposes that permit multiple payments or transactions to be made on the account. Additionally, any account maintained by an organization for which identity theft is a reasonable foreseeable risk that may impact customers or the safety and soundness of the organization is

considered a covered account. Miami-Dade County meets both the above criteria and must therefore develop a Red Flags program and train its employee as mandated by the FACT Act.

Twenty-eight departments and the County Attorney's Office collaborated in developing the attached program. As required by the FACT Act, the program provides a mechanism to identify and respond to patterns, practices or specific activities that could indicate identity theft. The goal is to assist County departments with detecting, preventing and mitigating identity theft using Red Flag Rules. Red Flags include, for example, unusual account activity, fraud alerts on a consumer report or account application documents that seem suspicious. These rules are designed to ensure that staff stay alert for signs or indicators that an identity thief is actively misusing or attempting to misuse another individual's sensitive data, typically to obtain goods or services from the County. All County employees will receive mandatory training on identifying and detecting Red Flags, and the appropriate actions to be taken in the event identity theft is suspected. The training program will be implemented by the Human Resources and the Enterprise Technology Services Departments and overseen by the Program Administrator. Additionally, individual departments will be able to use this Red Flags policy to develop more detailed internal procedures to suit their individual needs.

The Program Administrator will be responsible for administration and oversight of the Program, and will coordinate preliminary investigations of suspected identity theft. Department Directors or their designees will report to the Program Administrator all instances of suspected identity theft within 48 hours of their discovery. The electronic database will be utilized to report, record and archive all incidents relating to identity theft.

The FTC requires that the Board adopt the Program on or before June 1, 2010.

Assistant County Manager

MEMORANDUM

(Revised)

TO: Honorable Chairman Dennis C. Moss and Members, Board of County Commissioners

DATE: May 18, 2010

FROM: R. A. Cuevas, Jr. County Attorney

SUBJECT: Agenda Item No. 12(A)(4)

Please note any items checked.

_____ **"3-Day Rule" for committees applicable if raised**

_____ **6 weeks required between first reading and public hearing**

_____ **4 weeks notification to municipal officials required prior to public hearing**

_____ **Decreases revenues or increases expenditures without balancing budget**

_____ **Budget required**

_____ **Statement of fiscal impact required**

_____ **Ordinance creating a new board requires detailed County Manager's report for public hearing**

_____ **No committee review**

_____ **Applicable legislation requires more than a majority vote (i.e., 2/3's ____, 3/5's ____, unanimous _____) to approve**

_____ **Current information regarding funding source, index code and available balance, and available capacity (if debt is contemplated) required**

Approved _____ Mayor

Veto _____

Override _____

Agenda Item No. 12(A)(4)
5-18-10

RESOLUTION NO. _____

RESOLUTION APPROVING THE MIAMI-DADE COUNTY IDENTITY THEFT PREVENTION PROGRAM IN ACCORDANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003

WHEREAS, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (the "FACT Act"), which requires certain financial institutions and creditors that maintain covered accounts to prepare, adopt, and implement an identity theft prevention program by June 1, 2010; and

WHEREAS, the Federal Trade Commission ("FTC") enacted regulations in 2007 to implement the FACT Act, codified at 16 C.F.R. section 681, which require such identity theft prevention programs to identify, detect, and respond to "Red Flags," defined as patterns, practices, or specific activities that indicate the possible existence of identity theft; and

WHEREAS, based on the definitions set forth by the United States Congress and the FTC, certain Miami-Dade County Departments qualify, or may qualify in the future, as creditors that maintain covered accounts, thereby necessitating the adoption of an identity theft prevention program for Miami-Dade County as mandated by the FACT Act; and

WHEREAS, to comply with FTC regulations, the Mayor and his staff have developed and prepared a Miami-Dade County Identity Theft Prevention Program in the form attached hereto as "Exhibit A" and incorporated herein by this reference (the "Program"), designed to be implemented by the County Mayor, that sets forth policies and procedures for detecting and responding to Red Flags, provides for the appropriate training of staff, includes comprehensive oversight of the Program, and ensures the annual review and updating of the Program; and

WHEREAS, pursuant to FTC regulations, the Mayor and his staff have recommended that the Program now be approved and adopted by the Board of County Commissioners,

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COUNTY COMMISSIONERS OF MIAMI-DADE COUNTY, FLORIDA, that the Miami-Dade County Identity Theft Prevention Program, in the form attached, is hereby approved and adopted effective the date set forth below. The Board of County Commissioners delegates to the Mayor or the Mayor's designee full authority to implement and administer the Program, to periodically amend and update the Program as necessary to reflect changes in identity theft risks to Miami-Dade County and its customers, and to take such other actions reasonably necessary to develop and execute the Program.

The foregoing resolution was offered by Commissioner , who moved its adoption. The motion was seconded by Commissioner and upon being put to a vote, the vote was as follows:

Dennis C. Moss, Chairman
Jose "Pepe" Diaz, Vice-Chairman

Bruno A. Barreiro	Audrey M. Edmonson
Carlos A. Gimenez	Sally A. Heyman
Barbara J. Jordan	Joe A. Martinez
Dorrin D. Rolle	Natacha Seijas
Katy Sorenson	Rebeca Sosa
Sen. Javier D. Souto	

The Chairperson thereupon declared the resolution duly passed and adopted this 18th day of May, 2010. This resolution shall become effective ten (10) days after the date of its adoption unless vetoed by the Mayor, and if vetoed, shall become effective only upon an override by this Board.

MIAMI-DADE COUNTY, FLORIDA
BY ITS BOARD OF COUNTY
COMMISSIONERS

HARVEY RUVIN, CLERK

Approved by County Attorney as
to form and legal sufficiency.

By:_____
Deputy Clerk

Rodolfo A. Ruiz

MIAMI-DADE COUNTY
IDENTITY THEFT PREVENTION PROGRAM

Approved by

Miami-Dade County Board of County Commissioners
_____ __, 2010

7

Program Review History

Date	Summary of Revision

Table of Contents

9

I. PURPOSE AND SCOPE

The Miami-Dade County Identity Theft Prevention Program (Program) was developed pursuant to the Federal Trade Commission's 2007 "Red Flags Rule", 16 C.F.R. Section 68.2, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The FACT Act requires all Financial Institutions and Creditors that hold "Covered Accounts" to develop and implement an Identity Theft Prevention Program for new and existing accounts. The program must provide a methodology to identify and respond to patterns, practices, or specific activities that could indicate Identity Theft, also known as Red Flags. Red Flags include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents.

Based on the definitions provided by the Federal Trade Commission (FTC) several departments within Miami-Dade County qualify, or may qualify in the future, as creditors that hold Covered Accounts. Therefore, the goal of this Program is to assist County departments with detecting, preventing, and mitigating identity theft using Red Flag Rules, which are a mandatory part of any identity theft prevention program pursuant to the FACT Act. The Red Flag Rules included in this program are designed to ensure that Miami-Dade County departments stay alert for signs or indicators that an identity thief is actively misusing another individual's sensitive data, typically to obtain products or services from Miami-Dade County. Furthermore, the Program provides for a periodic updating process to reflect changes in risks to Miami-Dade County's customers.

II. ADOPTION

This Program was developed by a working group including members of the County Executive Office, the County Attorney's Office, representatives from 28 participating County departments and Jackson Memorial Hospital. Considering the size and complexity of the County's operations and account management systems, the nature and scope of the County's activities, and the patterns and risks of identity theft, the working group determined that this Program was appropriate for Miami-Dade County. This countywide program forms the overall Red Flags policy for the County and allows individual departments to develop more detailed internal procedures to the extent necessary.

This Program was approved by the Miami-Dade County Board of County Commissioners on _____ _____, 2010.

III. 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.

"Central Repository" means the electronic database operated by Miami-Dade County and administered by the Program Administrator. The Central Repository is utilized to report all instances of suspected or confirmed identity theft, as well as to store and record all identity theft incidents and any other reports related to Red Flags under this Program.

"Covered Account" means (i) any account the County offers or maintains primarily for personal, family or household purposes, that involves multiple payments or transactions; and (ii) any other

account the County offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the County from identity theft.

"County" means Miami-Dade County, a political subdivision of the State of Florida.

"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 (i) any person or entity that regularly extends, renews, or continues Credit; (ii) any person or entity that regularly arranges for the extension, renewal, or continuation of Credit; (iii) any assignee of an original Creditor who participates in the decision to extend, renew, or continue credit; or (iv) any person or entity that defers payment for goods and services.

"Customer" means any person who maintains a Covered Account with a Creditor.

"Employees" means County employees, contractors, consultants, temporary workers, service providers, and includes all personnel affiliated with third parties.

"Executive Governance Committee" means executive team appointed by the County Manager responsible for appointing a Program Administrator and to ensure an annual review of the status of the Program. The Committee shall be composed of at least seven members as follows; two (2) Assistant County Managers, the Director of the Miami-Dade County Enterprise Technology Services Department, the Finance Department Director, the Public Housing Authority Director, the Water and Sewer Director, and the General Services Administration Director.

"FACT Act" means Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

"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 Customer.

"FTC" means the Federal Trade Commission.

"Functional Leader" means the County departmental representative charged with assisting with the day-to-day administration of the Program. Functional Leaders are appointed by County Department Directors or their designees, and are responsible for monitoring and tailoring the Program as it relates to the functions of their particular department.

"Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

"Personal Identifying Information" means any name or number that may be used, alone or in conjunction with any other information, to identity a specific person, including, but not limited to, name, address, telephone number, social security number, date of birth, government passport number, employer or taxpayer identification number or unique electronic identification number.

"Program" refers to the County Identity Theft Prevention Program.

"Program Administrator" means the individual appointed by the Executive Governance Committee with primary responsibility for the implementation and oversight of the Program.

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

"Red Flag Rule" means 16 C.F.R. Section 681.2, which implements section 114 of the FACT Act of 2003.

"Service Provider" means a person or business entity that provides a service directly to the County relating to or in connection with a Covered Account.

IV. ASSESSMENT OF EXISTING BUSINESS PRACTICES

A County department must determine whether it is a creditor managing covered accounts as defined by the FACT Act. This is established through a two-step process as detailed in Attachment 1 which requires responses to four questions as follows:

1. Does the department provide goods or services first to County customers and allow these customers to pay later? *(Example: payment for utilities)*
2. Does the department grant loans, arrange for loans, or an extension of credit, or make credit decisions? *(Example: Affordable Housing Assistance Loan Program)*
3. Does the department offer or maintain accounts for personal, family, and household purposes that permit multiple payments or transactions? *(Example: mortgage loans, utility accounts)*
4. Does the department offer or maintain accounts for which identity theft is a reasonably foreseeable risk that may impact County customers or the safety and soundness of Miami-Dade County? *(Example: small business accounts, financial assistance applications, medical information)*

Once the department has established that is a creditor with covered accounts, the department must adhere to the Red Flags rules.

In order to identify relevant red flags, the County considered specific business processes associated with offering or maintaining Accounts. County employees with the ability to request and review customers' Personal Identifying Information when engaging in any of the following activities must be prepared to identify Red Flags indicating potential for identity theft:

a. Opening new Accounts;
b. Accessing existing Accounts;
c. Modifying existing Accounts; and
d. Closing existing Accounts.

Red Flags may also arise when a County customer service representative physically interacts with customers in order to engage in any of the foregoing account activities, or when customers directly engage in any of the foregoing account activities by submitting required Personal Identifying Information either through an automated phone system or via the internet, and such Personal Identifying Information is later reviewed by a County employee.

V. IDENTIFICATION OF RED FLAGS

The following items have been identified as potential red flag sources or categories that may indicate an instance of identity theft:

a. Alerts, Notifications and Warnings from Credit Reporting Agencies

i. Consumer credit report includes a fraud alert;

ii. Notice or report from a credit agency of an active duty alert for a customer or applicant;

iii. Notice or report from a credit agency of credit freeze and/or a notice of address discrepancy for a customer or applicant; or

iv. There is indication of activity that is inconsistent with a customer's usual pattern of activity, such as an unusual increase in the volume of credit inquiries, unusual increase in the number of established credit relationships; or a material change in the use of credit.

b. Suspicious Documents

i. An application appears to have been altered or forged or gives the appearance of having been destroyed and reassembled;

ii. Documents provided for identification appear to have been altered or forged; or

iii. Photograph, physical description and/or other information on the identification is not consistent with the appearance of a person presenting the identification.

c. Suspicious Personal Identifying Information

i. Information provided by the customer is inconsistent with other information provided by the customer;

ii. Information on the identification presented is not consistent with readily accessible information on file with the County;

iii. Information provided is inconsistent when compared against external information sources (for example, address does not match any address in the consumer report, and/or Social Security Number has not been issued or is associated with a deceased person by the Social Security Administration);

iv. Information provided is associated with known fraudulent activity as indicated by internal or third-party sources (for example, address and/or phone number on an application is the same as the address provided on a previous fraudulent application);

v. Information provided is of a type commonly associated with fraudulent activity (for example, address on an application is fictitious and/or phone number is invalid);

vi. Social Security Number, address and/or telephone number provided is the same as those provided by another customer;

vii. The customer or person opening a Covered Account fails to provide all required personal identifying information on an application or in response to a notification that the application is incomplete; or

viii. When administering security questions, the customer or individual opening a Covered Account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

d. Suspicious Account Activity or Unusual Use of Account

i. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's Covered Account;

ii. The County is notified that the customer is not receiving mail sent by the County, such as Account statements;

iii. Following a change of address for a Covered Account, the County receives a request to:

1. Add new, additional, or replacement goods or services;

2. Add authorized users on the Covered Account; or

3. Change the Covered Account holder's name.

iv. A Covered Account is used in a manner that is not consistent with established patterns of activity;

v. A Covered Account is used after it has been inactive for a reasonably lengthy period of time;

vi. The County is notified that a Covered Account has unauthorized activity;

vii. Payments stop on an otherwise consistently up-to-date Covered Account;

viii. Unauthorized access to or use of customer's Covered Account information; or

ix. Breach of the County's computer system security.

e. Alerts From Third Parties

i. Notice to the County from a customer, identity theft victim, law enforcement official, or other individual or entity that the County has opened or is maintaining a fraudulent account for a person engaged in identity theft.

VI. DETECTION OF RED FLAGS

a. New Covered Accounts

In order to detect any of the red flags identified above associated with the opening of a new Covered Account, County employees will take steps to obtain and verify the identity of the person opening the Covered Account. Each department responsible for offering Covered Accounts is expected to document the steps they will take, considering methods such as:

i. Requiring certain Personal Identifying Information such as name, date of birth, address, government-issued identification, and, where feasible, to compare such Personal identifying Information using records on file with the County or records on file with a third-party source, such as a consumer reporting agency;

ii. Verifying the identity presented (for example, examine the picture on the government-issued identification); and

iii. Independently contact the customer in the event of phone or internet setup of new Covered Accounts and require the establishment of security questions during the initial set-up and opening of the Covered Account.

b. Existing Covered Accounts

In order to detect any of the red flags identified above for an existing Covered Account, employees will take steps to monitor transactions with a Covered Account. Each department responsible for monitoring Covered Accounts is expected to document the steps they will take, considering methods such as:

i. If an individual is requesting information in person, or via telephone, fax, or email, authenticate the customer by verifying the identification of the individual prior to providing the requested information;

ii. Verifying the validity of requests to change billing addresses, and/or confirming changes, such as sending change confirmation to email address on file;

iii. Verifying changes in banking information given for billing and payment purposes, such as contacting the individual via the customer information on file prior to making any changes, or verifying ownership of the new bank account by contacting the appropriate financial institution; and

iv. Verify Personal Identifying Information for customers requesting a refund, and requiring managerial approval before granting any and all refunds.

VII. PREVENTION AND MITIGATION OF IDENTITY THEFT

In the event a County employee has observed any Red Flags associated with a new or existing Covered Account, the relevant department must respond immediately and mitigate damages to the existing or new Covered Account.

a. New Account Prevention and Mitigation

With regards to a new Covered Account, one or more of the following actions will be taken by the department to rectify the situation:

i. Monitor the Covered Account for evidence of Identity Theft;

ii. Contact the customer to discuss possible actions;

iii. Refuse to open a new Covered Account;

iv. Close a newly opened Covered Account;

v. Report to the Program Administrator as provided under the Program; and

vi. Notify law enforcement through established Program channels.

b. Existing Account Prevention and Mitigation

For an existing Covered Account, the County may discontinue the services associated with that Covered Account, and one or more of the following actions will be taken by the department to rectify the situation:

i. Cancel transactions determined to be fraudulent;

ii. Monitor the Covered Account for evidence of identity theft;

iii. Contact the Customer to discuss possible actions;

iv. Change the passwords, security codes, or other security devices that permit access to an existing Covered Account;

v. Re-open an existing Covered Account with a new account number;

vi. Close an existing account;

vii. Report the incident to the Program Administrator as provided under the Program; and

viii. Notify law enforcement if necessary through established Program channels.

c. Address Discrepancy Mitigation

In the event of address discrepancy notification from a consumer reporting agency indicating the address given by the consumer differs from the address contained in the report, the County shall:

i. Request formal documentation to support the address given by the consumer;

ii. Verify the address by using information on file, public records, or external sources; and

iii. Furnish the consumer's confirmed address to the consumer reporting agency from which it received the notice of address discrepancy.

d. Bill for Services Mitigation

If a customer or individual claims they received a bill for services that they did not request, the department that issued the bill will investigate to determine if the bill for services was processed erroneously as a result of clerical error. If so, the department will correct the mistakenly issued bill and notify the customer or individual that the error has been resolved.

However, if the County Department conducting the billing investigation determines that the bill for services is accurate and warranted, and the customer or individual maintains he or she was not the recipient of the services identified in the bill, the following procedures apply:

i. The department that issued the bill will instruct the customer or individual to file a report with law enforcement officials alleging Identity Theft;

ii. The department will provide the customer or individual one of the following documents in order to facilitate the customer or individual's ability to file an identity theft incident report with law enforcement officials:

   1. An Identity Theft Affidavit developed by the FTC, see Exhibit A attached.
   2. An Identity Theft Affidavit developed by the Office of the Florida Attorney General, see attached Exhibit B.

iii. The department will review a copy of the report filed by the customer or individual with law enforcement and obtain the report and/or case number for the County's records, and submit it to the Central Repository;

iv. The relevant department must notify the Program Administrator, as well as collection agencies, if applicable, and suspend collection efforts for all associated accounts if and when law enforcement initiates an identity theft investigation; and

v. The department will inform the customer or individual that he or she must cooperate with comparing his or her Personal Identifying Information with the records maintained by the County. Failure to cooperate or to provide the required information and statements listed above may not allow law enforcement officials to establish that identity theft has occurred, and will prevent any corrective action on behalf of the County.

If, following an investigation by law enforcement, it appears that the customer or individual has been a victim of identity theft that resulted in the County providing services to someone else under the name and account of the customer or individual, the appropriate County department will take the following actions:

i. Provide the results of the investigation to the Program Administrator;

ii. Refund any amounts received in error to the customer or individual; and

iii. If applicable, notify any consumer credit reporting agencies related to the customer or individual that the account was a product of identity theft.

If, following the completion of a law enforcement investigation, it does not appear that the individual has been a victim of identity theft, the County department will give written notice to the customer or individual that he or she is responsible for payment of the bill for service, and collection efforts will resume.

After an identity theft incident regarding a bill for services has been confirmed, the relevant compromised account must be cleansed, and all inaccuracies corrected. Actions taken to uncover and resolve the presence of fraudulent activity may also require revision to the policies and procedures of this Program.

VIII. PROGRAM ADMINISTRATION

a. Program Oversight

i. Program Administrator

The Program Administrator shall be responsible for the overall administration and oversight of the Program and shall review annual reports and recommendations submitted by departments for updates, changes, and modifications to the Program. In doing so, the Program Administrator will consider the County's experiences with identity theft situations, changes in identity theft methods, changes in detection and prevention techniques, changes in law, changes in departmental operations, and changes in the County's arrangements with other entities, service providers, and third parties. The Program Administrator will also be responsible for:

1. Coordinating preliminary investigations of suspected or confirmed incidents of Identity Theft;
2. Assisting the Miami-Dade County Enterprise Technology Services Department in maintaining a Central Repository of incidents related to identity theft reported by departments.
3. Preparing annual reports and recommendations to the Executive Governance Committee and serving as the primary liaison between different County Departments under the Program and the Executive Governance Committee;
4. Alerting County departments of identity theft incidents within 48 hours of their detection; and
5. Ensuring that County employees are appropriately trained.

ii. Department Functional Leaders

Each Department Director shall appoint a Functional Leader within their particular Department responsible for being readily familiar with the Program. Functional Leaders shall be responsible for:

1. Working together with their Department Director on the day-to-day administration of the Program;
2. Working together with their Director to develop specific Program implementation procedures for their particular Departments; and
3. Making recommendations to review, update, and/or modify the Program.

b. Service Provider Oversight

In the event the County enters into a contract with a service provider to perform an activity in connection with one or more Covered Accounts, the County will verify that the service provider conducts its activities in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. To accomplish this, the County will:

i. Require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the provider's activities; and

ii. Require the provider to immediately notify the County in writing of any incidents of identity theft.

c. Program Violations

If a Red Flag incident investigation reveals any violation of Program procedures or protocol, the County shall implement immediate corrective actions including:

i. Modification of a process, practice, or recording system to better protect the confidentiality of Personal Identifying Information; and

ii. Disciplinary action up to and including termination of the employee in accordance with County disciplinary policies.

d. Employee Training

Any employee with the ability to open a new Covered Account, or access, manage, or close an existing Covered Account will receive mandatory training on identifying and detecting Red Flags. Employees will also be trained in the appropriate response actions in the event that an instance of identity theft is suspected. Management personnel will also receive training on the contents of this Program.

Program training will be overseen by the Program Administrator and implemented by the Miami-Dade County Human Resources and Enterprise Technology Services Departments.

County employees will be re-trained annually, and should receive notice whenever the Program is updated to include new methods of identifying and detecting Red Flags, or if new response actions are implemented.

e. Reporting Requirements

Department Directors or their designees shall report to the Program Administrator all instances of suspected or confirmed identity theft within 48 hours of their discovery by utilizing the Central Repository, and will submit recommendations to update the Program as needed.

Whenever Departments are notified by a customer, individual, service provider, law enforcement agency, or consumer credit reporting agency of possible identity theft involving County services, the incident must be documented in the Central Repository and the Program Administrator must be notified.

If applicable, the County will provide the consumer reporting agencies with a description of the identity theft event.

For all instances of suspected or confirmed identity theft, the County shall advise the victim to notify local law enforcement and obtain a case number. The County will make available all the relevant details associated with the identity theft event.

f. Program Review and Update

The Program Administrator will be responsible for annually auditing all Program procedures and protocol in order to enforce and maintain the Program.

The Program Administrator will submit an annual report to the Executive Governance Committee detailing the County's compliance with the FTC Red Flags Rule. The Committee will review any recommended changes or improvements to the Program with the County Attorney's Office and Audit and Management Services before determining whether to approve any changes to the Program.

The Program Administrator's annual report will address the following topics:

i. Effectiveness of the policies and procedures addressing the risk of identity theft in connection with the opening of new Covered Accounts, as well as the risk of identity theft in connection with the management of existing Covered Accounts;

ii. Incidents involving identity theft and the Program Administrator's response; and

iii. Recommendations for material revisions to the Program to reflect changes in:

1. Risks both to customers and to the County;
2. Qualification of Covered Accounts; and
3. Methods to detect and address Red Flags.

Attachment 1

RED FLAGS RULE CRITERIA QUESTIONNAIRE

Department Name: **Reporting Fiscal Year:**	**Responses**	
1) Does your Department provide goods or services first to County customers and allow County customers to pay later? *(Example: payment for utilities)*	If YES, you are a CREDITOR, and proceed to Question 3.	If NO, proceed to Question 2.
2) Does your Department grant loans, arrange for loans, or an extension of credit, or make credit decisions? *(Example: Affordable Housing Assistance Loan Program)*	If YES, you are a CREDITOR, and proceed to Question 3.	If NO, you are NOT a CREDITOR.
3) Does your Department offer or maintain accounts for personal, family, and household purposes that permit multiple payments or transactions? *(Example: mortgage loans, utility accounts)*	If YES, you maintain COVERED ACCOUNTS and are subject to Red Flag Rules.	If NO, proceed to Question 4.
4) Does your Department offer or maintain accounts for which identity theft is a reasonably foreseeable risk that may impact County customers or the safety and soundness of Miami-Dade County? *(Example: small business accounts, financial assistance applications, medical information)*	If YES, you maintain COVERED ACCOUNTS and are subject to Red Flag Rules.	If NO, you do not maintain COVERED ACCOUNTS.

Based on your responses to the questions above, does your Department qualify as a "creditor" that maintains "covered accounts?" *(Please circle one response)* **YES** **NO**

If your Department qualifies as a "creditor" that maintains "covered accounts," please list the type of services and accounts subject to the Red Flags Rule:

Department Representative: _____ _____

Employee Signature Employee Name and Title

Exhibit A

Identity Theft Affidavit

(Prepared by the FTC)

Instructions for Completing the ID Theft Affidavit

To make certain that you do not become responsible for the debts incurred by the identity thief, you must provide proof that you didn't create the debt to each of the companies where accounts were opened or used in your name.

A working group composed of credit grantors, consumer advocates and the Federal Trade Commission (FTC) developed this ID Theft Affidavit to help you report information to many companies using just one standard form. Use of this affidavit is optional. While many companies accept this affidavit, others require that you submit more or different forms. Before you send the affidavit, contact each company to find out if they accept it.

You can use this affidavit where a **new account** was opened in your name. The information will enable the companies to investigate the fraud and decide the outcome of your claim. (If someone made unauthorized charges to an **existing account**, call the company to find out what to do.)

This affidavit has two parts:

- **ID Theft Affidavit** is where you report general information about yourself and the theft.

- **Fraudulent Account Statement** is where you describe the fraudulent account(s) opened in your name. Use a separate Fraudulent Account Statement for each company you need to write to.

When you send the affidavit to the companies, attach copies (**NOT** originals) of any supporting documents (e.g., drivers license, police report) you have.

Before submitting your affidavit, review the disputed account(s) with family members or friends who may have information about the account(s) or access to them.

Complete this affidavit as soon as possible. Many creditors ask that you send it within two weeks of receiving it. Delaying could slow the investigation.

Be as accurate and complete as possible. You *may* choose not to provide some of the information requested. However, incorrect or incomplete information will slow the process of investigating your claim and absolving the debt. Please print clearly.

When you have finished completing the affidavit, mail a copy to each creditor, bank or company that provided the thief with the unauthorized credit, goods or services you describe. Attach to each affidavit a copy of the Fraudulent Account Statement with information only on accounts opened at the institution receiving the packet, as well as any other supporting documentation you are able to provide.

Send the appropriate documents to each company by certified mail, return receipt requested, so you can prove that it was received. The companies will review your claim and send you a written response telling you the outcome of their investigation. **Keep a copy of everything you submit for your records.**

If you cannot complete the affidavit, a legal guardian or someone with power of attorney may complete it for you. Except as noted, the information you provide will be used only by the company to process your affidavit, investigate the events you report and help stop further fraud. If this affidavit is requested in a lawsuit, the company might have to provide it to the requesting party.

Completing this affidavit does not guarantee that the identity thief will be prosecuted or that the debt will be cleared.

ID Theft Affidavit

Victim Information

(1) My full legal name is _____
(First) (Middle) (Last) (Jr., Sr., III)

(2) (If different from above) When the events described in this affidavit took place, I was known as

_____
(First) (Middle) (Last) (Jr., Sr., III)

(3) My date of birth is _____
(day/month/year)

(4) My social security number is _____

(5) My driver's license or identification card state and number are _____

(6) My current address is _____

City _____ State _____ Zip Code _____

(7) I have lived at this address since _____
(month/year)

(8) (If different from above) When the events described in this affidavit took place, my address was _____

City _____ State _____ Zip Code _____

(9) I lived at the address in #8 from _____ until _____
(month/year) (month/year)

(10) My daytime telephone number is (____)_____

My evening telephone number is (____)_____

How the Fraud Occurred

Check all that apply for items 11 - 17:

(11) ☐ I did not authorize anyone to use my name or personal information to seek the money, credit, loans, goods or services described in this report.

(12) ☐ I did not receive any benefit, money, goods or services as a result of the events described in this report.

(13) ☐ My identification documents (for example, credit cards; birth certificate; driver's license; social security card; etc.) were ☐ stolen ☐ lost on or about _____.
(day/month/year)

(14) ☐ To the best of my knowledge and belief, the following person(s) used my information (for example, my name, address, date of birth, existing account numbers, social security number, mother's maiden name, etc.) or identification documents to get money, credit, loans, goods or services without my knowledge or authorization:

Name (if known)	Name (if known)
Address (if known)	Address (if known)
Phone number(s) (if known)	Phone number(s) (if known)
additional information (if known)	additional information (if known)

(15) ☐ I do NOT know who used my information or identification documents to get money, credit, loans, goods or services without my knowledge or authorization.

(16) ☐ Additional comments: (For example, description of the fraud, which documents or information were used or how the identity thief gained access to your information.)

_____

_____

_____

_____

_____

(Attach additional pages as necessary.)

Victim's Law Enforcement Actions

(17) (check one) I ☐ am ☐ am not willing to assist in the prosecution of the person(s) who committed this fraud.

(18) (check one) I ☐ am ☐ am not authorizing the release of this information to law enforcement for the purpose of assisting them in the investigation and prosecution of the person(s) who committed this fraud.

(19) (check all that apply) I ☐ have ☐ have not reported the events described in this affidavit to the police or other law enforcement agency. The police ☐ did ☐ did not write a report.
In the event you have contacted the police or other law enforcement agency, please complete the following:

(Agency #1)	(Officer/Agency personnel taking report)
(Date of report)	(Report Number, if any)
(Phone number)	(e-mail address, if any)

(Agency #2)	(Officer/Agency personnel taking report)
(Date of report)	(Report Number, if any)
(Phone number)	(e-mail address, if any)

Documentation Checklist

Please indicate the supporting documentation you are able to provide to the companies you plan to notify. Attach copies (NOT originals) to the affidavit before sending it to the companies.

(20) ☐ A copy of a valid government-issued photo-identification card (for example, your driver's license, state-issued ID card or your passport). If you are under 16 and don't have a photo-ID, you may submit a copy of your birth certificate or a copy of your official school records showing your enrollment and place of residence.

(21) ☐ Proof of residency during the time the disputed bill occurred, the loan was made or the other event took place (for example, a rental/lease agreement in your name, a copy of a utility bill or a copy of an insurance bill).

(22) ☐ A copy of the report you filed with the police or sheriff's department. If you are unable to obtain a report or report number from the police, please indicate that in Item 19. Some companies only need the report number, not a copy of the report. You may want to check with each company.

Signature

I declare under penalty of perjury that the information I have provided in this affidavit is true and correct to the best of my knowledge.

_____ _____

(signature) (date signed)

Knowingly submitting false information on this form could subject you to criminal prosecution for perjury.

_____

(Notary)

[Check with each company. Creditors sometimes require notarization. If they do not, please have one witness (non-relative) sign below that you completed and signed this affidavit.]

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

Fraudulent Account Statement

Completing this Statement

- Make as many copies of this page as you need. **Complete a separate page for each company you're notifying and only send it to that company.** Include a copy of your signed affidavit.
- List only the account(s) you're disputing with the company receiving this form. **See the example below.**
- If a collection agency sent you a statement, letter or notice about the fraudulent account, attach a copy of that document (**NOT** the original).

I declare (check all that apply):

☐ As a result of the event(s) described in the ID Theft Affidavit, the following account(s) was/were opened at your company in my name without my knowledge, permission or authorization using my personal information or identifying documents:

Creditor Name/Address *(the company that opened the account or provided the goods or services)*	**Account Number**	**Type of unauthorized credit/goods/services provided by creditor** *(if known)*	**Date issued or opened** *(if known)*	**Amount/Value provided** *(the amount charged or the cost of the goods/services)*
Example Example National Bank 22 Main Street Columbus, Ohio 22722	01234567-89	auto loan	01/05/2000	$25,500.00

☐ During the time of the accounts described above, I had the following account open with your company:

Billing name _____

Billing address _____

Account number _____

1-877-IDTHEFT (1.877.438.4338)

www.consumer.gov/idtheft

Average time to complete: 10 minutes

Identity Theft Victim's Complaint and Affidavit

A voluntary form for filing a report with law enforcement, and disputes with credit reporting agencies and creditors about identity theft-related problems. Visit ftc.gov/idtheft to use a secure online version that you can print for your records.

Before completing this form:

1. Place a fraud alert on your credit reports, and review the reports for signs of fraud.
2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

About You *(the victim)*

Now

(1) My full legal name: _____
First Middle Last Suffix

(2) My date of birth: _____
mm/dd/yyyy

(3) My Social Security number: _____-_____-_____

(4) My driver's license: _____ _____
State Number

(5) My current street address:

_____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(6) I have lived at this address since _____
mm/yyyy

(7) My daytime phone: (____)_____
My evening phone: (____)_____
My email: _____

Leave (3) blank until you provide this form to someone with a legitimate business need, like when you are filing your report at the police station or sending the form to a credit reporting agency to correct your credit report.

At the Time of the Fraud

(8) My full legal name was: _____
First Middle Last Suffix

(9) My address was: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

(10) My daytime phone: (____)_____ My evening phone: (____)_____
My email: _____

Skip (8) - (10) if your information has not changed since the fraud.

30

The Paperwork Reduction Act requires the FTC to display a valid control number (in this case, OMB control #3084-0047) before we can collect – or sponsor the collection of – your information, or require you to provide it.

About You (the victim) (Continued)

Declarations

(11) I ☐ did OR ☐ did not authorize anyone to use my name or personal information to obtain money, credit, loans, goods, or services — or for any other purpose — as described in this report.

(12) I ☐ did OR ☐ did not receive any money, goods, services, or other benefit as a result of the events described in this report.

(13) I ☐ am OR ☐ am not willing to work with law enforcement if charges are brought against the person(s) who committed the fraud.

About the Fraud

(14) I believe the following person used my information or identification documents to open new accounts, use my existing accounts, or commit other fraud.

(14): Enter what you know ~~about anyone~~ you believe was involved (even if you don't have complete information).

Name: _____
First Middle Last Suffix

Address: _____
Number & Street Name Apartment, Suite, etc.

_____
City State Zip Code Country

Phone Numbers: (____)_____ (____)_____

Additional information about this person: _____

(15) Additional information about the crime (for example, how the identity thief gained access to your information or which documents or information were used):

(14) and (15): Attach additional sheets as needed.

_____

_____

_____

_____

_____

_____

_____

Documentation

(16) I can verify my identity with these documents:

(16): Reminder: Attach copies of your identity documents when sending this form to creditors and credit reporting agencies.

☐ A valid government-issued photo identification card (for example, my driver's license, state-issued ID card, or my passport).
If you are under 16 and don't have a photo-ID, a copy of your birth certificate or a copy of your official school record showing your enrollment and legal address is acceptable.

☐ Proof of residency during the time the disputed charges occurred, the loan was made, or the other event took place (for example, a copy of a rental/lease agreement in my name, a utility bill, or an insurance bill).

About the Information or Accounts

(17) The following personal information (like my name, address, Social Security number, or date of birth) in my credit report is inaccurate as a result of this identity theft:

(A) _____

(B) _____

(C) _____

(18) Credit inquiries from these companies appear on my credit report as a result of this identity theft:

Company Name: _____

Company Name: _____

Company Name: _____

(19) Below are details about the different frauds committed using my personal information.

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

Name of Institution | Contact Person | Phone | Extension

Account Number | Routing Number | Affected Check Number(s)

Account Type: ☐ Credit ☐ Bank ☐ Phone/Utilities ☐ Loan
☐ Government Benefits ☐ Internet or Email ☐ Other

Select ONE:
☐ This account was opened fraudulently.
☐ This was an existing account that someone tampered with.

Date Opened or Misused (mm/yyyy) | Date Discovered (mm/yyyy) | Total Amount Obtained ($)

(19): If there were more than three frauds, copy this page blank, and attach as many additional copies as necessary.

Enter any applicable information that you have, even if it is incomplete or an estimate.

If the thief committed two types of fraud at one company, list the company twice, giving the information about the two frauds separately.

Contact Person: Someone you dealt with, whom an investigator can call about this fraud.

Account Number: The number of the credit or debit card, bank account, loan, or other account that was misused.

Dates: Indicate when the thief began to misuse your information and when you discovered the problem.

Amount Obtained: For instance, the total amount purchased with the card or withdrawn from the account.

Your Law Enforcement Report

(20) One way to get a credit reporting agency to quickly block identity theft-related information from appearing on your credit report is to submit a detailed law enforcement report ("Identity Theft Report"). You can obtain an Identity Theft Report by taking this form to your local law enforcement office, along with your supporting documentation. Ask an officer to witness your signature and complete the rest of the information in this section. It's important to get your report number, whether or not you are able to file in person or get a copy of the official law enforcement report. Attach a copy of any confirmation letter or official law enforcement report you receive when sending this form to credit reporting agencies.

Select ONE:

- ☐ I have not filed a law enforcement report.
- ☐ I was unable to file any law enforcement report.
- ☐ I filed an automated report with the law enforcement agency listed below.
- ☐ I filed my report in person with the law enforcement officer and agency listed below.

(20):
Check "I have not..." if you have not yet filed a report with law enforcement or you have chosen not to. Check "I was unable..." if you tried to file a report but law enforcement refused to take it.

Automated report:
A law enforcement report filed through an automated system, for example, by telephone, mail, or the Internet, instead of a face-to-face interview with a law enforcement officer.

_____
Law Enforcement Department State

_____ _____
Report Number Filing Date (mm/dd/yyyy)

_____
Officer's Name (please print) Officer's Signature

_____ _____
Badge Number Phone Number

Did the victim receive a copy of the report from the law enforcement officer? ☐ Yes OR ☐ No

Victim's FTC complaint number (if available): _____

Signature

As applicable, sign and date *IN THE PRESENCE OF* a law enforcement officer, a notary, or a witness.

(21) I certify that, to the best of my knowledge and belief, all of the information on and attached to this complaint is true, correct, and complete and made in good faith. I understand that this complaint or the information it contains may be made available to federal, state, and/or local law enforcement agencies for such action within their jurisdiction as they deem appropriate. I understand that knowingly making any false or fraudulent statement or representation to the government may violate federal, state, or local criminal statutes, and may result in a fine, imprisonment, or both.

_____ _____

Signature Date Signed (mm/dd/yyyy)

Your Affidavit

(22) If you do not choose to file a report with law enforcement, you may use this form as an Identity Theft Affidavit to prove to each of the companies where the thief misused your information that you are not responsible for the fraud. While many companies accept this affidavit, others require that you submit different forms. Check with each company to see if it accepts this form. You should also check to see if it requires notarization. If so, sign in the presence of a notary. If it does not, please have one witness (non-relative) sign that you completed and signed this Affidavit.

_____

(Notary)

Witness:

_____ _____

(signature) (printed name)

_____ _____

(date) (telephone number)

Exhibit B

Identity Theft Affidavit

(Prepared by the Office of the Florida Attorney General)

Florida's Identity Theft Victim Kit

A guide for victims of identity theft, detailing what to do and who to contact.

This kit is designed to help you work through the process of resolving your identity theft case and clearing your name. While there are many general identity theft resource guides available, this kit was specifically developed to provide assistance to Floridians who are identity theft victims, as well as individuals in other states who had their personal information fraudulently used in the state of Florida.

Navigating through the system as an identity theft victim can be a lengthy and confusing process. As you contact law enforcement, creditors, and financial institutions, it is important that you keep track of the actions you take and retain a record of your progress.

When your identity is stolen your personal identifiers can be misused in a variety of different ways. As soon as you become aware that your information has been misused, there are several basic steps you should take that apply to nearly all kinds of identity theft cases:

Step One

Report the incident to the fraud department of the three major credit bureaus.

- Ask the credit bureaus to place a "fraud alert" on your credit report.
- Order copies of your credit reports so you can review them to see if any additional fraudulent accounts have been opened in your name or if any unauthorized charges have been made to other accounts.
- Request a victim's statement that asks creditors to contact you prior to opening new accounts or making changes to any existing accounts.

Contact information for the three major credit bureaus is as follows:

37

Equifax
P.O. Box 740241
Atlanta, GA 30374-0241
To order your report: 1-800-685-1111
To report fraud: 1-800-525-6285
TDD: 800-255-0056
www.equifax.com

TransUnion
Fraud Victim Assistance
P.O. Box 6790
Fullerton, CA 92634-6790
Email: fvad@transunion.com
To order your report: 1-800-888-4213
To report fraud: 1-800-680-7289
TDD: 877-553-7803
www.transunion.com

Experian
P.O. Box 9532
Allen, TX 75013
To order your report: 1-888-EXPERIAN (397-3742)
To report fraud: 1-888-EXPERIAN (397-3742)
TDD: 800-972-0322
www.experian.com

Step Two

Contact the fraud department of each of your creditors.

- Gather the contact information for each of your credit accounts (credit cards, utilities, cable bills, etc.) and call the fraud department for each creditor.

- Report the incident to each creditor, even if your account at that institution has not been tampered with. Close the accounts that you believe have been compromised. Ask the credit bureaus to place an "alert" on any accounts that remain open.

- Follow-up in writing immediately. The Federal Trade Commission provides an Identity Theft Affidavit (attached), a standardized form used to report new accounts fraudulently opened in your name. Check with the company to see if they accept this form. If not, request that they send you their fraud dispute form.

- Confirm all conversations in writing. Follow behind your phone call with a letter and any necessary documentation to support your claim.

38

- Call the Federal Trade Commission at 1-877-IDTHEFT (438-4338) and request a copy of their brochure "Identity Crime: When Bad Things Happen to Your Good Name." This brochure contains sample dispute letters to help get you started as well as more information on resolving credit problems. The brochure is also available through the Federal Trade Commission website at www.ftc.gov

Step Three

Contact your bank or financial institution.

- If your checks have been stolen, or if you believe they have been used, contact your bank or credit union and stop payment right away.

- Put stop payments on any outstanding checks that you are unsure about.

- Contact the major check verification companies and request they notify retailers who use their databases not to accept your checks:

  TeleCheck 1-800-710-9898 or 927-0188
  Cetergy, Inc 1-800-437-5120
  International Check Services 1-800-631-9656

- Call SCAN at 1-800-262-7771 to learn if bad checks have been passed in your name.

- If you suspect your accounts have been compromised, cancel your checking and savings accounts and obtain new account numbers.

Step Four

Report the incident to law enforcement.

- Contact your local police department or sheriffs office to file a report. Under Florida Statute 817.568, the report may be filed in the location in which the offense occurred, or, the city or county in which you reside.

- When you file the report, provide as much documentation as possible, including copies of debt collection letters, credit reports, and your notarized ID Theft Affidavit.

- Request a copy of the police report. Some creditors will request to see the report to remove the debts created by the identity thief.

What Else Can I Do?

File a complaint with the FTC's Identity Theft Clearinghouse

The Clearinghouse is the federal government's repository for ID theft complaints. Complaint information is entered into a central database, the Consumer Sentinel, which is accessed by many local and state law enforcement agencies in Florida, as well as Florida's Attorney General, for identity theft investigation. Call the toll-free hotline at 1-877-IDTHEFT.

Flag your Florida Driver's License.

At your request, the Fraud Section of the Department of Highway Safety and Motor Vehicles (DHSMV) will place a flag on your driver's license if you are a victim of identity theft (regardless of whether your Florida Driver's License has been compromised). To reach the Fraud Section, call (850) 617-2405. You will be asked to submit your request in writing to:

Department of Highway Safety and Motor Vehicles
DDL/BDI - Fraud Section, Room A327
Neil Kirkman Building
Tallahassee, FL 32399-0570

If you believe that the identity thief has actually used your personal information to secure a Florida Driver's License or Identification Card, DSHMV will conduct a fraud investigation. To initiate this investigation, request a DHSMV Identity Theft Report Form and mail it to the address above. The form is also available through the DHSMV website at www.hsmv.state.fl.us

Get assistance through Florida's Fraud Hotline.

Florida's Attorney General provides a toll-free fraud hotline for Floridians who are the victims of Fraud. Contact the hotline at 1-866-9-NO-SCAM (1-866-966-7226). Trained advocates can help provide additional resource information in your area.

Check your Florida criminal history information.

In some instances of identity theft, a victim may be faced with a criminal record for a crime he or she did not commit. The Florida Department of Law Enforcement (FDLE) can provide a Compromised Identity Review (based on a fingerprint comparison of state criminal history files) to determine what, if any, criminal history belongs to you, and if any arrest records have been falsely associated with you as a result of someone using your identity. If a fingerprint check determines you are an identity theft victim, FDLE will work with local law enforcement agencies to attempt to clear fraudulent data from the criminal history files and provide you with a Compromised Identity Certificate. For more information, contact FDLE's Quality Control Section at (850) 410-8880 or visit www.fdle.state.fl.us

Contact the Florida Department of Law Enforcement.

After you have filed a report with local law enforcement and with the FTC's Identity Theft Clearinghouse, you may contact FDLE. FDLE Special Agents who work identity theft cases may be able to provide additional guidance and assistance. Check your phone book to find the nearest FDLE Regional Operations Center or visit www.fdle.state.fl.us

Remove your personal identifiers from Florida court records.

Any person has the right to request the Clerk or County Recorder to redact/remove his or her Social Security number, bank account number, credit, debit or charge card number from an image or copy of an Official Record that has been placed on such Clerk's/County Recorder's publicly available Internet website, or in a court file. If you believe your personal information appears in a publicly available record, contact your County Clerk's Office to initiate a request. A listing of all County Clerks can be found at www.flclerks.com

Report Mail Theft to the U.S. Postal Inspection Service.

The U.S. Postal Inspection Service will investigate if your mail has been stolen by an identity thief and used to obtain new credit or commit fraud. Incidents should be reported to your nearest U.S. Postal Inspection Service district office. Check your telephone book for your local office or visit www.usps.com

Report Passport Fraud to the U.S. Department of State.

If your passport is lost or stolen, or you believe it is being used fraudulently, contact your local Department of State field office. Check your telephone book for your local office or visit www.state.gov

Protect your Social Security number.

The Social Security Administration can verify the accuracy of the earnings reported on your social security number. To check for inaccuracies or fraud, order a copy of your Personal Earnings and Benefit Estimate Statement (PEBES) from the Social Security Administration by calling 1-800-772-1213 or visiting www.ssa.gov

41

Identity Theft Prevention Program Governance Structure

MIAMI-DADE COUNTY

PROPOSED OVERSIGHT STRUCTURE

EXECUTIVE GOVERNANCE COMMITTEE
(2) ACMs, ETSD Dir. FIN Dir., PHA Dir., WASD Dir., GSA Dir.

Executive Chair/Sponsor
Appointed by the Governance Board

- CAO
- AMS
- COMMUNITY ADVISOR

[redacted]

- ETSD
- HRD
- LAW ENFORCEMENT

FUNCTIONAL TEAMS
Functional Leaders appointed by the Governance Board

LOANS TEAM	UTILITIES TEAM	SERVICE PROVIDERS TEAM	MISCELLANEOUS TEAM
Functional Leaders	Functional Leaders	Functional Leaders	Functional Leaders

DEPARTMENTAL TEAMS

- PHA
- HFA
- HCD
- SBD
- OCI
- WASD
- DSWM
- MDAD
- DERM
- GSA
- FIN
- MDFR
- ASD
- DPM (CONTRACTORS, EXTERNAL SERVICE PROVIDERS)
- TBD

eh