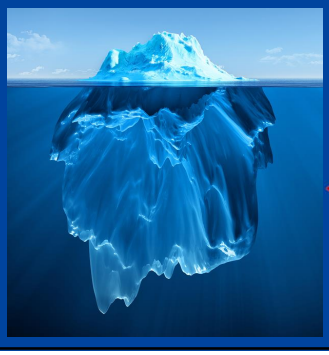
Tax Professionals: Protect Your Clients and Protect Yourself from Identity Theft

Presented by Dean Saul, EA, NAEA, NTPI, NTXEA
134 N Cowan Avenue
Lewisville, TX 75057-3765
Voice: 972.221.5943
Fax: 972.221.7675

IDENTITY THEFT

IDENTITY THEFT

We see



The Reality

Why is this a problem?

Å Many business issues vie for your attention
Å Top 3 business concerns:
- ï New clients (27%)
- ï Staying current (24%)
- ï Data security (15%)

1 in 10 accountants report having lost client data; nearly 1 in 4 report having clients victims of ID theft.

- ï SourceMedia Research August 2016 Cybersecurity Study

ÅWhy is this a problem?

Identity thieves are Increasingly targeting ***tax professionals***.

These criminals – many of them:

- Å Sophisticated
- Å Organized syndicates

Gathering personal data to file fraudulent federal and state income tax returns.

Who can fight this crime?

NO ONE ENTITY CAN FIGHT THIS CRIME

IT TAKES ALL OF US, WORKING TOGETHER

IRS WORK GROUPS

- Authentication
- Communication and Taxpayer Awareness
- Financial Services
- Information Sharing

IRS WORK GROUPS

- Information Sharing and Analysis Center (ISAC)
- Tax Professionals
- Strategic Threat Assessment and Response (STAR)

"Dirty Dozen" List of Tax Scams to Avoid

- ❖Phone Scams
- ❖Phishing
- ❖Identity Theft
- ❖Return Practitioner Fraud
- ❖Offshore Tax Avoidance
- ❖Inflated Refund Claims

"Dirty Dozen" List of Tax Scams to Avoid

- ❖Fake Charities
- ❖Hiding Income with Fake Documents
- ❖Abusive Tax Shelters
- ❖Falsifying Income to Claim Credits
- ❖Excessive Claims for Fuel Tax Credits
- ❖Frivolous Tax Arguments (@ least 50!)

New for 2017

- ÅEmphasis remains on authentication of legitimate tax filers, information sharing and cybersecurity.
- ÅMost activities will be invisible to taxpayers

New for 2017

- Expanding from 2 to 50 million a pilot program to add a 16 digit Verification Code to Forms W-2.
- Expanded definition of Ultimate Bank Account (UBA): includes all refund transfer products, including gift and pre-paid cards, paper checks and direct deposit.

New for 2017

- Some states are using:
- Driver's License w/issue and expiration date
- Financial industry - external leads program

Just announced:

- Over the next 5weeks, IRS will be sending ***all*** active e-Services users who have access to the transcript delivery system a letter (via U.S. Postal Service) asking the individual to validate his or her identity within 30 days. These letters started going out in batches last week.

ÅSee:

https://www.irs.gov/individuals/important-update-about-your-eservices-account

Tax Practitioners

1. ***How are Tax Practitioners Impacted?***
2. ***What is your role as a practitioner?***
3. ***What Can you Do?***

How are Tax Practitioners Impacted?

1. ***Most important: If your client database is compromised, you can be out of business!***
2. ***Perhaps worse:***
   a. ***Your clients will sue you***
   b. ***You may have to provide free credit reporting for years***
   c. ***Loss of Client confidence and their referrals***

What is your role as a Practitioner?

You have a legal responsibility to have safeguards in place to protect client information. Taxpayer data is defined as ***any*** information obtained or used in the preparation of a tax return.

What is your role as a Practitioner?

Å***Critical Steps:***

ÅSee IRS Publication 4557
ÅNever leave taxpayer data, including data left on hardware and media, unsecured
ÅSecurely dispose of taxpayer information

What is your role as a Practitioner?

Å***Critical Steps:***

ÅRequire password changes every 60–90 days & go for complexity
ÅStore taxpayer data in secure systems and ***encrypt*** information when transmitting across networks
ÅEncrypt e-mail containing taxpayer data (X2)

What is your role as a Practitioner?

- Secure and restrict access to paper documents, computer disks, flash drives and other media to authorized users only
- Use caution: allowing or granting remote access to internal networks

What is your role as a Practitioner?

- Terminate access of terminated employees
- Create security requirements for your entire staff regarding computer information systems, paper records and use of taxpayer data

What is your role as a Practitioner?

- Provide periodic staff update training
- Protect your facilities from unauthorized access and potential dangers

What is your role as a Practitioner?

- Complete a risk assessment to identify risk and potential impacts of unauthorized access
- Create a plan on the required steps to notify taxpayers should you be the victim of any data breach or theft

What is your role as a Practitioner?

- Write and follow an Information Security plan
- Consider performing background checks and screen individuals before granting access to taxpayer information

- Register for e-News for Tax Professionals or follow the IRS Twitter and Facebook social media for tax professionals.

What Can you Do?

- Check your PTIN – ***often***
- Encrypt your computer(s)
- Encrypt your e-mails

What Can you Do?

- Use firewalls
  - ***@ least 1 hardware and***
  - ***1 software***
- ***Consider 'Cloud' storage***

What Can you Do?

- Use a secure portal for exchanging sensitive client information
- Redact social security numbers on paper(s)
- Lock file storage areas

What Can you Do?

- Be alert for phishing scams
- Periodically Run a security "deep scan" to search for viruses and malware

What Can you Do?

- Strengthen passwords for both computer access and software access
- review Publication 4557 @ <https://www.irs.gov/pub/irs-pdf/p4557.pdf>,

Questions?

FTC FACT Act Red Flags Rule Template

Important: If you choose to use this template as a guide, you must adapt it to reflect your individual firm. Without the analysis and modification required to fit your firm's situation, your Identity Theft Prevention Program (ITPP) will not comply with regulatory requirements.

This template is an optional guide for firms to assist them in fulfilling their requirements under the Federal Trade Commission's (FTC) Red Flags Rule, which implements obligations imposed by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The Red Flags Rule requires specified firms to create a written Identity Theft Prevention Program (ITPP) designed to identify, detect and respond to "red flags"—patterns, practices or specific activities—that could indicate identity theft. "Identity theft" is a fraud committed or attempted using the identifying information of another person without authority.

Template Use

The obligation to develop a written Red Flags Rule ITPP is not a "one-size-fits-all" requirement, so **you must customize this template to fit your particular firm's situation.** If any of the language does not adequately address your firm's business situation, you will need to prepare your own language. You are responsible for ensuring that the program fits your firm's business and that you implement the program. The language in this template is designed to be a starting point and to walk you through developing your firm's ITPP. Following this template does not guarantee compliance, or create any safe harbor, with FTC or FINRA rules, the federal securities laws or state laws.

- *TEXT EXAMPLES* are provided in this template to give you sample language that you can modify to create your firm's ITPP.

- Material in *italics* provides instructions, the relevant rules and other resources that you can use to develop your firm's plan; you will likely want to delete this material—and the introductory material that is boxed in the first pages of this document (*i.e.*, the material up to "[Firm Name]")—from your final ITPP.

FTC Red Flags Rule Only

This template addresses only the FTC's Red Flags Rule, which was adopted November 9, 2007, with an enforcement start date extended to December 31, 2010. It does not address the Identity Theft Red Flags Rules of the federal financial institution regulatory agencies (Office of the Comptroller of the Currency, the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision and the National Credit Union Administration) that were also adopted November 9, 2007. It also does not address related FTC regulations, adopted on the same date, that require policies and procedures for 1) credit and debit card issuing firms to assess the validity of changes of address

notifications and 2) credit report using firms to respond to a credit reporting agency's notice of address discrepancy; enforcement of those regulations began November 1, 2008. If those regulations apply to your firm, FINRA expects it to have policies and procedures in place to comply with them.

Red Flags Rule Coverage and Periodic Review

Under the FTC Rule, your firm must prepare an ITPP if it is either a "financial institution" or a "creditor" and offers "covered accounts." FINRA anticipates that most member firms will be required to prepare an ITPP under the Red Flags Rule. Even if it does not have to prepare an ITPP now, your firm must have internal controls to periodically review its operations, and prepare an ITPP if it later becomes a financial institution or a creditor that offers covered accounts.

Financial Institution. Your firm is a "financial institution" if it provides, either directly or indirectly through your clearing firm, consumer "transaction accounts," which are accounts that allow account holders to make withdrawals for payment or transfer of funds to third parties by telephone transfers, checks, debit cards or similar means. Since "consumer" is defined as an individual, a firm without individuals as clients would not be a financial institution under this definition.

Creditor. Your firm is a "creditor" if it regularly extends, renews or continues credit (such as margin) or arranges for its extension, renewal or continuation (such as through a clearing firm). A firm that is not a financial institution because it has only institutional customers can still be a creditor if it extends credit, or arranges to extend credit, for any of its customers.

Covered Accounts. If your firm is either a financial institution or a creditor, you must then analyze whether it offers "covered accounts," which are any accounts that either 1) your firm offers primarily for personal, family or household purposes and involve multiple payments (such as credit card, margin, checking or savings accounts), or 2) involve a reasonably foreseeable risk from identity theft to customers or the safety and soundness of your firm.

Send questions about complying with the Red Flags Rule to *RedFlags@ftc.gov*.

Rules: 16 Code of Federal Regulations (C.F.R.) §§ 681.1(b) and (d).

Program Elements

The four program elements for an ITPP specified in the FTC Red Flags Rule require your firm to:

(1) identify relevant red flags for the covered accounts that the firm offers or maintains, and incorporate those red flags into its ITPP;
(2) detect red flags that have been incorporated into the ITPP of the financial institution or creditor;

(3) respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
(4) update the ITPP and its red flags periodically to reflect changes in identity theft risks to customers and the firm.

Rules: 16 C.F.R. §681.1(d)(2).

Program Administration
To administer your ITPP, your firm must:

(1) get approval of the initial written ITPP from the firm's board of directors, an appropriate committee of it, or, if there is no board, a designated member of senior management;
(2) involve the board, committee or the designated member of senior management in the oversight, development, implementation and administration of the ITPP;
(3) train staff to implement the ITPP; and
(4) oversee service provider arrangements.

Rules: 16 C.F.R. §681.1(e).

Resources

FINRA

- FINRA Regulatory Notice 08-69 (Fair and Accurate Credit Transactions Act of 2003)
- Podcast: FTC's Red Flags Rule Template
- Podcast: FACT Act Red Flags Rule
- Regulation S-P: Privacy of Consumer Financial Information, including Final Rule, 2005 Amendment, 2008 Proposed Amendments, FINRA Comment Letter on 2008 Proposed Amendments and FAQ

FTC

- FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (Delay of Enforcement Until December 31, 2010)
- FTC Extends Enforcement Deadline for Identity Theft Red Flags Rule (Delay of Enforcement Until June 1, 2010)
- FTC's Fighting Fraud with the Red Flags Rule: A How-To Guide for Business
- Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, Final Rule, Federal Trade Commission and the Federal Financial Institution Regulatory Agencies (FTC Red Flags Rule)
- FTC's Complying with the Red Flags Rule: Do-It-Yourself Program for Businesses at Low Risk For Identity Theft
- FTC Identity Theft Site

Other

- e-CFR Title 16 Commercial Practices Part 681–Identity Theft Rules
- Guidance on Authentication in Internet Banking Environment- Federal Financial Institutions Examination Council's (FFIEC)
- Treasury Final Rule Regarding Broker/Dealer Customer Identification Programs (05/09/03) (under Anti-Money Laundering (AML) Rules and Regulations on FINRA's AML Web page)

[Firm Name]
Identity Theft Prevention Program (ITPP) under the FTC FACT Act Red Flags Rule

---

I. Firm Policy

State your firm's objectives for your ITPP.

TEXT EXAMPLE: Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 16 C.F.R. § 681.1(d).

II. ITPP Approval and Administration

State who is responsible for initial approval of this ITTP, which should be your board of directors or an appropriate board committee; or, if you have no board, a designated member of senior management. State who is responsible for the oversight, development, implementation and administration of the ITPP, which may be a designated member of senior management, your board or a board committee.

TEXT EXAMPLE: The firm's Board of Directors, *or* the [*Name*] Committee of the Board, *or* [*Name, title*], a member of senior management, approved this initial ITPP. [*Name, title*], a member of senior management, is the designated identity theft officer and is responsible for the oversight, development, implementation and administration (including

staff training and oversight of third party service providers of ITTP services) of this ITPP.

Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a).

III. Relationship to Other Firm Programs

Describe how this ITPP relates to your firm's other programs to protect customer data, such as the data safekeeping and disposal procedures under Regulation S-P, your Customer Identification Program ("CIP") and red flags detection under your AML Compliance Program.

TEXT EXAMPLE: We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, [and] our CIP and red flags detection under our AML Compliance Program [and *list any others*] in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts.

Rule: 16 C.F.R. § 681.1, Appendix A, Section I.

IV. Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, your firm must assess certain risk factors and sources, as well as the categories and examples listed in Supplement A to Appendix A of the FTC's Red Flags Rule (See Resources, above). This consideration forms the basis for modifying the attached Red Flag Identification and Detection Grid to cover your firm's situation and experience.

TEXT EXAMPLE: To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks likely, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II.

V. Detecting Red Flags

Your firm's ITPP must address how, in connection with opening and maintenance its covered accounts, it will detect the Red Flags it identified in Part IV above and set out in the first column of attached Grid. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using your CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address. How your firm will detect each of its identified Red Flags is to be set out in the second column of the attached Grid.

TEXT EXAMPLE: We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML compliance procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III.

VI. Preventing and Mitigating Identity Theft

Your firm's ITPP must provide responses to its detected Red Flags that match the risk involved.

TEXT EXAMPLE: We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely. Based on this and our review of the FTC's identity theft rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

Procedures to Prevent and Mitigate Identity Theft

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Applicants. For Red Flags raised by someone applying for an account:

1. Review the application. We will review the applicant's information collected for our CIP under our AML Compliance Program (e.g., name, date of birth, address,

and an identification number such as a Social Security Number or Taxpayer Identification Number).

2. Get government identification. If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport. If the applicant is submitting an electronic application via our Web site, we will use [*describe your Internet authentication methods; under Resources, above, see the Guidance on Authentication in an Internet Banking Environment-Federal Financial Institutions Examination Council's (FFIEC)*].
3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    a. Contacting the customer
    b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker [or] the Social Security Number Death Master File [or *list other sources*]
    c. Checking references with other affiliated financial institutions, or
    d. Obtaining a financial statement.
4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account.
5. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.
6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice under state law. *[Note*: *See National Conference of State Legislators' listing of state notification requirements (This site may not be updated or comprehensive. Each firm is responsible to research all applicable state requirements. State and local laws and regulations are not uniform. All broker-dealers must have policies and procedures reasonably designed to prevent and detect violations of the laws and regulations of the jurisdictions in which they operate.)]*

Access seekers. For Red Flags raised by someone seeking to access an existing customer's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a

data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.

4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
    a. Firm information (both introducing and clearing firms):
        i. Firm name and CRD number
        ii. Firm contact name and telephone number
    b. Dates and times of activity
    c. Securities involved (name and symbol)
    d. Details of trades or unexecuted orders
    e. Details of any wire transfer activity
    f. Customer accounts affected by the activity, including name and account number, and
    g. Whether the customer will be reimbursed and by whom.
6. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.
7. Notification. If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers or other required under state law. [*see note at 6, under "Applicants" above]*
8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that our response to a data breach does not limit or eliminate our insurance coverage.
9. Assist the customer. We will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Offering to change the password, security codes or other ways to access the threatened account;
    b. Offering to close the account;
    c. Offering to reopen the account with a new account number;
    d. Not collecting on the account or selling it to a debt collector; and
    e. Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Rule: 16 C.F.R. § 681.1(d)(iii) and Appendix A, Section IV.

VII. Clearing Firm and Other Service Providers

If your firm uses a clearing firm or other service providers in connection with its covered accounts, it must ensure that the providers comply with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft.

TEXT EXAMPLE: Our firm uses a clearing firm [*and other service providers*] in connection with our covered accounts. We have a process to confirm that our clearing firm and any other service provider that performs activities in connection with our covered accounts, especially other service providers that are not otherwise regulated, comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by contractually requiring them to have policies and procedures to detect Red Flags contained in our Grid and report detected Red Flags to us [*or* take appropriate steps of their own to prevent or mitigate the identify theft *or* both]. Our clearing firm is [*name, address, phone number, e-mail address, Web site*] and our contact person at that clearing firm is [*name, phone number, e-mail*]. Our other service providers that perform activities in connection with our covered accounts are: [*list service provider's name, address and phone number, and e-mail address.*]

Rule: 16 C.F.R. § 681.1(e)(4) and Appendix A, Section VI.(c).

VIII. Internal Compliance Reporting

Describe how your firm's staff will report your ITPP's compliance with the regulations.

TEXT EXAMPLE: Our firm's staff who are responsible for developing, implementing and administering our ITPP will report at least annually to our [Board *or* committee *or* designated member of senior management] on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP.

Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.(b).

IX. Updates and Annual Review

Describe your firm's update policy and annual review of your ITPP.

TEXT EXAMPLE: Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm.

In addition, our firm will review this ITPP annually, on [*date*], to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm.

Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b).

X. Approval

Approve the firm's ITPP by signing below.

TEXT EXAMPLE: I approve this ITPP as reasonably designed to enable our firm to detect, prevent and mitigate identity theft.

Rule: 16 C.F.R. § 681.1 (e)(1)&(2) and Appendix A, Section VI.(a).

Signed: _____

Title: _____

Date: _____

ATTACHMENT: Red Flag Identification and Detection Grid (Grid)

[FIRM NAME]

Red Flag Identification and Detection Grid

This grid provides FTC categories and examples of potential red flags. Please note these examples are not exhaustive nor a mandatory checklist, but a way to help your firm think through relevant red flags in the context of its business. Some examples may not be relevant to your firm, while others may be relevant when combined or considered with other indicators of identity theft. Modify the cells in the table below as described in the FTC FACT Act Red Flags Template Section IV, Identifying Relevant Red Flags, and Section V, Detecting Red Flags. If any categories and examples under them do not apply to your firm, delete the rows containing them. Likewise, add rows for any not on the list that you need to add based on your risk factor and sources assessment. For example, if your firm does not use consumer credit reports, delete the "Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency" and the rows of Red Flag examples 1 – 4 under it.

TEXT EXAMPLE:

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. A fraud or active duty alert is included on a consumer credit report.	We will verify that the fraud or active duty alert covers an applicant or customer and review the allegations in the alert. [In addition, *describe any other steps your firm takes*].
2. A notice of credit freeze is given in response to a request for a consumer credit report.	We will verify that the credit freeze covers an applicant or customer and review the freeze. [In addition, *describe any other steps your firm takes*].
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	We will verify that the notice of address or other discrepancy covers an applicant or customer and review the address discrepancy. [In addition, *describe any other steps your firm takes*].
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	We will verify that the consumer credit report covers an applicant or customer, and review the degree of inconsistency with prior history. [In addition, *describe any other steps your firm takes*].
Insert other red flags in this category based on your firm's own experience or its knowledge of likely new methods of identity theft.	*Insert how your firm would detect these red flags you have identified.*
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Our staff who deal with customers and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged. [In addition, *describe any other steps your firm takes*].

6. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with customers and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it. [In addition, *describe any other steps your firm takes*].
7. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with customers and their supervisors will ensure that the identification and the statements of the person presenting it are consistent. [In addition, *describe any other steps your firm takes*].
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with customers and their supervisors will ensure that the identification presented and other information we have on file from the account, such as [*describe the information*] are consistent. [In addition, *describe any other steps your firm takes*].
9. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with customers and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled. [In addition, *describe any other steps your firm takes*].
Insert other red flags in this category based on your firm's own experience or its knowledge of likely new methods of identity theft.	*Insert how your firm would detect these red flags you have identified.*
Category: Suspicious Personal Identifying Information	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	Our staff will check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match. [In addition, *describe any other steps your firm takes*].
11. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	Our staff will check personal identifying information presented to us to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables [*or describe other internal consistency tests made*].
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent. [In addition, *describe any other steps*

	your firm takes].
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff will validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services. [In addition, *describe any other steps your firm takes*].
14. The SSN presented was used by someone else opening an account or other customers.	Our staff will compare the SSNs presented to see if they were given by others opening accounts or other customers. [In addition, *describe any other steps your firm takes*].
15. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff will compare address and telephone number information to see if they were used by other applicants and customers. [In addition, *describe any other steps your firm takes*].
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded. [In addition, *describe any other steps your firm takes*].
17. Inconsistencies exist between what is presented and what our firm has on file.	Our staff will verify key items from the data presented with information we have on file. [In addition, *describe any other steps your firm takes*].
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	Our staff will authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report. [In addition, *describe any other steps your firm takes*].
Insert other red flags in this category based on your firm's own experience or its knowledge of likely new methods of identity theft.	*Insert how you would detect these red flags you have identified.*
Category: Suspicious Account Activity	
19. Soon after our firm gets a change of address request for an account, we are asked to add additional access means (such as debit cards or checks) or authorized users for the account.	We will verify change of address requests by sending a notice of the change to both the new and old addresses so the customer will learn of any unauthorized changes and can notify us. [In addition, *describe any other steps your firm takes*].
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and	We will review new account activity to ensure that first and subsequent payments are made, and that credit is primarily used for other than cash advances and securities easily converted into cash. [In

securities easily converted into cash.	addition, *describe any other steps your firm takes*].
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	We will review our accounts on at least a monthly basis and check for suspicious new patterns of activity such as nonpayment, a large increase in credit use, or a big change in spending or electronic fund transfers. [In addition, *describe any other steps your firm takes*].
22. An account that is inactive for a long time is suddenly used again.	We will review our accounts on at least a monthly basis to see if long inactive accounts become very active. [In addition, *describe any other steps your firm takes*].
23. Mail our firm sends to a customer is returned repeatedly as undeliverable even though the account remains active.	We will note any returned mail for an account and immediately check the account's activity. [In addition, *describe any other steps your firm takes*].
24. We learn that a customer is not getting his or her paper account statements.	We will record on the account any report that the customer is not receiving paper statements and immediately investigate them. [In addition, *describe any other steps your firm takes*].
25. We are notified that there are unauthorized charges or transactions to the account.	We will verify if the notification is legitimate and involves a firm account, and then investigate the report. [In addition, *describe any other steps your firm takes*].
Insert other red flags in this category based on your firm's own experience or its knowledge of likely new methods of identity theft.	*Insert how you would detect these red flags you have identified.*
Category: Notice From Other Sources	
26. We are told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	We will verify that the notification is legitimate and involves a firm account, and then investigate the report. [In addition, *describe any other steps your firm takes*].
We learn that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	We will contact the customer to learn the details of the unauthorized access to determine if other steps are warranted. [In addition, *describe any other steps your firm takes*].
Insert other red flags in this category based on your firm's own experience or its knowledge of likely new methods of identity theft.	*Insert how your firm would detect these red flags you have identified.*

Written ID Theft Program Template

Use this Template to draft your own written Identity Theft Prevention Program.

1. Copy the Template sections below into your own document, ideally on company letterhead or another official company header so that it is easily identified as an official company document.
2. Fill in the blanks with the information you gather as you design your program.
3. Edit or delete any pre-filled information that does not match what you will actually do.
4. Obtain your Board of Directors' or company owners' formal approval of the written Program and document the date upon which it was approved.

[Type in your Company's Name]'s Identity Theft Prevention Program

[Type in your company name] has established this Identity Theft Prevention Program to help protect our customers, consumers and the lenders we represent generally against identity theft. This program is designed to comply with the requirements of the Fair and Accurate Credit Transactions Act (FACTA) Red Flags Rule and provide assurance to both our customers and the lenders with which we do business that [Type in your company name] is actively involved in the effort to prevent identity theft and related frauds in mortgage lending.

Risk Assessment

[Type in your company name] has performed an identity theft risk assessment to assess the Identity Theft Red Flags that we might encounter in our business. We have identified the following relevant Red Flags:

1. Notice from a customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently.
2. A fraud or active duty alert in a borrower's credit report.
3. An address discrepancy alert in a borrower's credit report.
4. Notice of a credit freeze in response to a credit report inquiry.
5. A photo ID that appears to be forged or altered.
6. An application form that appears to have been forged or altered.
7. _____
8. _____
9. _____
10. _____

[Add items as needed to this list to fill in as many Red Flags as you identify in your business matched back to the 26 suggested red flags guidelines especially these for brokers "Alerts and notifications or warnings from a Credit Repository #1,2,3,4,10,11,12, 13,14, 26 " "Suspicious Identifying Information #5,6,7,9) and "potentially "other suspicious Personal Information derived for an account opening" such as #15, 16) The numbers referred to above specifically correspond to the FACTA guidelines List of Suggested Alerts in Appendix J of the FACTA Red Flags Ruling.]

Written ID Theft Program Template

Red Flags Detection

[Type in your company's name] will detect the Red Flags we have identified in the following ways:

1. All employees are required to immediately notify the individual responsible for our Identity Theft Prevention Program if they are notified by a consumer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently. The same procedure applies if our credit report vendor, Informative Research, notifies us that a consumer has contacted them regarding possible fraud related to our request for a credit report.
2. [Type in your company's name] is utilizing Informative Research's Red Flags Risk Platform to draw our attention to alerts in the borrower's credit report such as fraud alerts and address discrepancies. It is our policy to respond with mitigation procedures specifically to all triggered alerts when the risk rating on RFRP shows a High or Elevated risk Level. Indicated risk levels below "Moderate" should be scanned in comparison with the entire loan file.
3. Any discrepancies between information provided by a borrower and information obtained from a third party will trigger further review to assess if a Red Flag is present.
4. Employees will be trained in detecting signs of forged or altered documents such as driver's licenses, loan applications, or tax documents.
5. _____
6. _____
7. _____
8. _____
9. _____
10. _____

[Add items as needed to this list. Your Program should describe how you will detect each of the Red Flags you have identified in the first section.]

Responding to Red Flags to Prevent and Mitigate Identity Theft

[Fill in your company's name] has established the following procedures to respond to Red Flags:

1. When notified by a customer, a victim of identity theft, a law enforcement agency, or someone else that an application may have been made fraudulently, [Type in your company's name] will:
    1) Immediately halt processing on the loan while the claim is investigated or, if the loan has been funded, notify the lender of the possible fraud.
    2) Investigate fully by whatever means are available, e.g., police reports, identifying documentation provided by the consumer, etc.
    3) Request removal of the inquiry from the consumer's credit file by the credit bureaus if the application proves to be fraudulent.
2. If [Type in your company's name] receives a fraud or active duty alert in a borrower's credit report, our staff will take the actions recommended by the Red Flags Risk Platform to resolve the possible issues raised by this Red Flag,

3. If [Type in your company's name] receives an address discrepancy alert in a borrower's credit report our staff will take the actions recommended by the Red Flags Risk Platform to resolve the possible issues raised by this Red Flag.
4. If [Type in your company's name] receives notice of a credit freeze in response to a credit report inquiry, our staff will [fill in your step-by-step procedure]
5. If [Type in your company's name]suspects a photo ID may be to be forged or altered [fill in your step-by-step procedure].
6. If [Type in your company's name] suspects an application form may have been forged or altered [fill in your step-by-step procedure].
7. _____
8. _____
9. _____
10. _____

Employee Training

[Type in your company's name] will provide Red Flags training to employees pertinent to their job functions, as follows:

Job Function: [Example: Loan Processor]
[Example: Loan Processors are likely to encounter Red Flags on a regular basis, and will therefore receive Red Flags at hire and in annual refresher courses. Loan Processors will receive additional training any time the Identity Theft Prevention Program is updated but in general, shall use the Red Flags Risk Addendum and follow the specific mitigation therein for files shown to as having a "High" or "Elevated Risk" level.]

Job Function: Loan Officers
[Fill in how training will be provided.]

Job Function: Other?
[Fill in how training will be provided.]

Service Providers

[Type in your company's name] uses the following service providers in connection with our covered accounts:

1. Informative Research (credit reporting). Informative Research verifies that its procedures support our Red Flags compliance. Specifically, if IR detects a Red Flag pertaining to one of our borrowers, using IR's Red Flags Risk Addendum will are immediately notified so as to respond appropriately.
2. Bureau Credit Fraud Alerts from Experian's "Fraud Shield", TransUnion's "High Risk Fraud Alerts", and or Equifax's "Safe Scan"
3. [Fill in any other service providers which may include IR's access to the Social Security Administration via its Consent Based Social Verification service]

Written ID Theft Program Template

Program Updates

[Type in your company's name] will review this Identity Theft Prevention Program as appropriate to ensure that the Program addresses all identified Red Flags in the program. The Program Administrator will ensure that the Program is reviewed and updated if changes occur in our business or practices, in available methods to detect and respond to Red Flags, or changes in identity theft risks warrant a revision of the program. At a minimum, the Program Administrator will Review the program 'at least annually/quarterly/monthly' to verify that it remains current.

Designated Program Administrator

[Type in your company's name] designates the following senior staff member to administer this Program:

Name: _____

Title: _____

Board/Senior Management Approval

This Program is approved by:

Signature: _____

Name &Title: _____

Signature: _____

Name &Title: _____

Signature: _____

Name &Title: _____

As of [fill in the date of the approval].