

Identity Theft Red Flags Rule – Work Program

Identity Theft Red Flags Rule – Work Program

The Identity Theft Red Flags Rule is a new regulatory requirement for financial institutions. The purpose for this document is to outline the actions and steps needed to execute the engagement.

Client Profile

The following is the client information:

Profile Items	
Entity Name:	
Address 1:	
Address 2:	
City:	
State:	
Zip Code:	
Country:	
Contact Person:	
Email:	
Phone:	

Entity Information

The following is the client information:

Entity Type	
Bank	
Savings Association	
Credit Union	
Mortgage Lender	
Mortgage Broker	
Consumer Lender	
Student Lender	
Auto Dealer	
Utility Company	
Phone Company	

Asset Size	
Less than or equal to 100 Million	
Greater than \$100 million to \$500 million	
Greater than \$500 million to 1 billion	
Greater than 1 billion to \$50 billion	
Greater than \$50 billion	

Account Information

The following is the client information:

Accounts Offered: Consumer Accounts		
Checking accounts		
Savings accounts		
Time deposits		
Mortgage loans		
HELOC		
Construction loans		
Deposit Secured loans		
Unsecured loans		
Motor vehicle loan		
Motor vehicle lease		
Credit cards		
Line of credit		
Overdraft		
Tax anticipation refund loan		
Student Loan		
Utility (i.e., gas, water, electric, etc.)		
MMDA		

Accounts Offered: Business Accounts		
Checking accounts		
Savings accounts		
Time deposits		
Mortgage loans		
HELOC		
Construction loans		
Deposit Secured loans		
Unsecured loans		

Methods to Access		
Web site		
In person (single location/branch)		
In person (multiple locations/branches)		
Telephone (human interaction)		
Telephone (touchtone/voice response)		
Other		

Methods to Open		
Web site		
In person (single location/branch)		
In person (multiple locations/branches)		
Mail		
Telephone		
Fax		
Other		

Risk Assessment Information

The following is the risk assessment information:

Past Incidents - Amounts		
Number of incidents		
Damages in Dollars		

Past Incidents - Types		
Fraudulent withdrawals from accounts		
Fraudulent use of calling cards numbers		
Fraudulent use of credit card/debit cards		
Fraudulent creation of credit/debit cards		
Fraudulent change of address request		
Counterfeit checks		
Social Engineering – telephone		
Social Engineering – mail		
Social Engineering – email		
Social Engineering – website		
Social Engineering – in person		

Service Providers		
Remote Hosting		
Application Service Providers (ASP)		

Alerts and/or Red Flags

The following outlines alerts and/or red flag information:

Alerts, Notifications or Warnings from a consumer report Agency		
Fraud alert		
Active duty alert		
Credit/security freeze		
Notice of address discrepancy		
Recent activity inconsistent with historical activity on consumer report:		
<ul style="list-style-type: none"> • Increase in inquiries • Unusual number of recently established credit relationships • Material change in the use of credit • Account closed for cause or identified for abuse of privileges+ 		

Suspicious Documents	
Documents provided for identification appear to have been altered or forged.	
The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.	
Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.	
Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.	
An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	

Suspicious Personal Identifying Information	
Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example: <ul style="list-style-type: none"> a. The address does not match any address in the consumer report; or b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File. 	
Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.	
Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: <ul style="list-style-type: none"> a. The address on an application is the same as the address provided on a fraudulent application; or b. The phone number on an application is the same as the number provided on a fraudulent application. 	
Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example: <ul style="list-style-type: none"> a. The address on an application is fictitious, a mail drop, or prison; or b. The phone number is invalid, or is associated with a pager or answering service. 	
The SSN provided is the same as that submitted by other persons opening an account or other customers.	
The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.	
The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.	
Personal identifying information provided is not consistent with personal identifying information that is on file with the financial	

institution or creditor.		
For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.		

Unusual Use of, or Suspicious Activity related to, the Covered Account		
Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.		
A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example: a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.		
A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example a. Nonpayment when there is no history of late or missed payments; b. A material increase in the use of available credit; c. A material change in purchasing or spending patterns; d. A material change in electronic fund transfer patterns in connection with a deposit account; or e. A material change in telephone call patterns in connection with a cellular phone account.		
A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).		
Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.		
The financial institution or creditor is notified that the customer is not receiving paper account statements.		
The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.		

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor		
The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.		

Detection Methods

The following outlines detection methods:

Account Opening	
Follow BSA/AML, CIP Procedures	
BSA – Bank secrecy Act. AML - Anti-money Laundering CIP - Customer Identification Program	
Investigated alerts from Consumer Reporting Agency (CRA)	
Inspect application documents	
Inspect identification documents	
Compare identification information to internal information for other similar account holders	
Verify that identification document presented is of the type issued by a government	
For online applications, confirm that IP address is consistent with applicant’s indicated geographic location	
Validate Social Security Number	
Use shared secrets (e.g., the applicant is asked for information only the institution and the application knows)	
Determine county of application? Residence	
Require multiple confirmations of true identity	
Use of external databases (CRA, public records)	

Response Method

The following outlines response methods:

Response Procedures	
Determine whether a suspicious activity report (SAR) should be filed	
When identify theft is detected in an account, investigate the account holder’s other accounts for identity theft	
For online account access, if an IP address is not recognized, require the account holder to answer a challenge question	
In the event of failed website or automated telephonic authentication, require applicant or account holder to contact a service representative	
Investigate Red Flag and temporarily suspend account	
Investigate Red Flag, but do not suspend account	
Monitor the account for evidence of identity theft	
Contact the applicant or account holder	
Change passwords, security codes, or other security devices that permit access to a covered account	
Reopen the account with a new account number	
Refuse to open an account	
Close existing account	