Red Flags Rule

Gain the upper hand on the Identity Theft Red Flags Rule

BizID℠ — This product draws on multiple databases to provide a comprehensive commercial fraud and authentication tool that quickly analyzes data on business and business principal information. Through a single inquiry, BizID:

- Validates and verifies business and guarantor application data

- Delivers customizable decisioning, business guantor and blended scoring

- Provides high-level alerts and detailed information from multiple sources

- Identifies previously submitted application elements

Knowledge IQ℠ — This product leverages Precise ID comprehensive data assets, analytics and decisioning to deliver interactive challenge and response questions to consumers for an added level of confidence and authentication:

- Knowledge-based (out-of-wallet) authentication

- Credit and noncredit versions

- Flexibly weighted and progressive questioning

- Multiple delivery options

- Performance monitoring

Credit Profile Report — Generated by Experian's File One℠ system, the report provides an exhaustive search of an applicant's credit history and monitors, evaluates and makes decisions based on changes in the customer profile:

- More than 215 million credit-active consumers via File One

- Consumer statements

- Credit freeze

- FACTA address discrepancy

- Social Security number issuance

- Tradeline history and activity

Social Search — This tool instantly matches and retrieves the latest consumer identifying information reported on the input Social Security number from the File One database:

- Multiple Social Security numbers per search (20)

- Multiple consumers per Social Security number (10)

- Multiple addresses per consumer

- Fair Credit Reporting Act (FCRA) and non-FCRA versions

- Additional demographics

- First and last reported dates

About Decision Analytics

Experian's Decision Analytics business combines data intelligence, analytics, software and consulting to help clients optimize profitability and improve performance. Its enterprise-wide decisioning capabilities enable clients to manage and mitigate credit risk; prevent, detect and reduce fraud; meet regulatory obligations; and gain operational efficiencies. Trusted by leading businesses worldwide, Experian's Decision Analytics business provides the intelligence to make accurate and informed decisions to help clients better manage their customer relationships.

To find out more about Experian's Red Flag–relevant capabilities, contact your local Experian sales representative or call 1 888 414 1120.

Now is the time to act. Confidently comply with FACTA requirements.

The effective date for landmark identity theft legislation has arrived, and financial institutions must comply with sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). These Red Flag guidelines apply to "covered accounts" defined as (1) an account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Each financial institution or creditor must develop and implement a written Identity Theft Prevention Program that is:

- Designed to detect, prevent and mitigate identity theft in connection with its covered accounts

- Appropriate to the size and complexity of its business and the nature and scope of its activities

A Red Flag is "any pattern, practice or specific activity indicating potential identity theft."[1] The 26

Red Flag guidelines focus on five general categories:

- Alerts, notifications or warnings from a consumer reporting agency

- Suspicious identification documents

- Suspicious personal identifying information, such as a suspicious Social Security number or address change

- Unusual use of an account or other dubious account-related activity

- Notices from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft in connection with your accounts

A Red Flag–compliant program:

- Identifies relevant red flags and incorporates them into the program

- Detects red flags that have been incorporated into the program

- Responds to detected red flags to prevent and mitigate identity theft

- Ensures the program remains current with identity theft trends

[1]This quote and the information contained in this document are derived from the Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003. This information is provided for promotional purposes only and is not intended, nor should it be misconstrued as, legal advice.

These policies apply to both account applications and existing accounts and may be combined with other information security and fraud prevention programs.

Streamline your Identity Theft Program
Experian's Decision Analytics and Credit Services businesses provide a number of Red Flag–relevant products and services to help you work toward a comprehensive Identity Theft Prevention Program and Red Flag compliance. The final Red Flag ruling in 2007 grants companies the flexibility to implement a risk-based program suited to their unique needs. While the rules can seem vague and open to interpretation, Experian® has the capabilities to help you customize your program to meet your compliance requirements.

If you are covered under the Red Flags Rule will need to make informed decisions to expedite the process and optimize your resources. We can support you by creating and delivering an appropriate and measurably effective Identity Theft Prevention Program. Our Red Flag–relevant products and services combine to provide:

- Consumer credit and noncredit data assets
- Detailed consumer identity information
- Flexible delivery options

- Targeted analytics
- Custom and best-practice decisioning
- Knowledge-based authentication

Integrate Experian's tools into your Identity Theft Prevention Program
Fraud Shield℠ — Through a series of checks, searches and counters, Fraud Shield returns indicators that provide specific high-risk descriptions and discrepancies related to identity elements:

- Twenty-seven high-risk warnings across address, Social Security number and credit establishment
- Discrepancies in age related to Social Security number, trades and identity elements
- Victim statements

Precise ID℠ — This comprehensive fraud prevention and detection platform combines detailed consumer authentication results with powerful analytics and customizable decisioning:

- Credit and noncredit data sources and product versions
- Detailed consumer identity checking results and records
- Flexible, client-customized compliance decisioning
- Shared application data and checks
- Targeted models and decisioning
- National Fraud Database℠

Overview — Integrate Experian's tools into your Identity Theft Prevention Program

Rule/Subrule	Fraud Shield℠	Precise ID℠ for Account Opening	Precise ID℠ for Identity Screening	Precise ID℠ for Compliance	Knowledge IQ℠	File One℠ Credit Profile	Social Search	BizID℠
Category — Alerts, Notifications or Warnings from a Consumer Reporting Agency								
A fraud or active-duty alert is included with a consumer report.	●	●				●	●	●
A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.		●	●	●		●	●	●
A consumer reporting agency provides a notice of address discrepancy.	●	●	●	●		●	●	●
A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:								
a. A recent and significant increase in the volume of inquiries;	●	●				●	●	●
b. An unusual number of recently established credit relationships;	●					●		
c. A material change in the use of credit, especially with respect to recently established credit relationships; or						●		
d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.						●		
Category — 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:								
a. The address does not match any address in the consumer report; or	●	●	●	●		●	●	●
b. The Social Security number 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 Social Security number 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:								
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:								
a. The address on an application is fictitious, a mail drop or a prison; or	●	●	●	●		●	●	●
b. The phone number is invalid or is associated with a pager or an answering service.		●	●	●				●

Rule/Subrule	Fraud Shield℠	Precise ID℠ for Account Opening	Precise ID℠ for Identity Screening	Precise ID℠ for Compliance	Knowledge IQ℠	File One℠ Credit Profile	Social Search	BizID℠
Category — Suspicious Personal Identifying Information								
The Social Security number 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 address 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 a consumer report.					●			
Category — 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. 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.								
Category — 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.	●	●				●	●	●