Complying with the “Red Flag Rules” and “FACT Act Address Discrepancy Rules”

May 2008
Table of Contents

Introduction 3
ID Analytics for Compliance and the Red Flag Rules 4
Comparison with Alternative Approaches 4
ID Analytics for Compliance - In-Depth Approach to Red Flags 5
Red Flag Compliance - Best Practices 6
Address Discrepancies 7
Resolving Address Discrepancies 8
In Summary 9
About ID Analytics, Inc. 9
Introduction

The Red Flag rules became effective on January 1, 2008; organizations must comply with the rules by November 1, 2008. The rules seek to protect lenders and consumers from the detrimental impact of identity fraud. Affected creditors are now required to design and implement procedures for detecting and preventing identity fraud at the point of account origination as well as during management of existing accounts.

The Red Flag rules allow for significant flexibility. They were designed to be appropriate to the size, complexity of operations, and nature of a creditor’s activities. For compliance purposes, a Red Flag is defined as a “pattern, practice, or specific activity that indicates the possible existence of identity theft.”

The rules require affected organizations to administer a “written program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.” Covered accounts include credit cards, mortgages, auto loans, margin accounts, cell phone accounts, utilities, checking, or savings accounts primarily used for personal, family, or household purposes.

Competitive business practices dictate that these new regulatory requirements must be met without increasing operational costs, delaying legitimate transactions, or escalating customer abandonment rates. A Red Flag program must contain reasonable policies and procedures to address the following four requirements:

1. **Identify**: Specify Red Flags that are relevant to a particular institution.
2. **Detect**: Red Flags must be detected in the ordinary course of operations.
3. **Respond**: Detected Red Flags must be evaluated and resolved.
4. **Evolve**: Document a detailed process for periodically updating the program to reflect changes in risk.

In addition to the Red Flag rules, all lenders must also form a reasonable belief that a credit report belongs to a specific consumer in cases of address discrepancy. In particular, credit card issuers must take special precautions when executing change of address requests. This paper will articulate how ID Analytics for Compliance™ assists in satisfying these regulatory requirements.
ID Analytics for Compliance and the Red Flag Rules

ID Analytics for Compliance evaluates and interprets more than one hundred proprietary identity risk variables that are indicative of identity fraud, covering more than two dozen Red Flags. Based on information from the ID Network®, the nation’s only real-time, cross-industry compilation of identity information, ID Analytics for Compliance delivers a unique, high-resolution indication of identity risk while effectively satisfying compliance obligations using a powerful identity-centric strategy called Personal Topology™.

Personal Topology is an abstract representation of the complete ID Network view of an individual’s particular identity characteristics including connectedness to other individuals along with their unique identity characteristics. This view of individual identities and their interrelationship with other identities provides unique visibility into the presence of Red Flags and the actual risks they might indicate. ID Analytics for Compliance not only detects the presence of Red Flags using the ID Network, but automatically resolves Red Flags for low-risk identities. By applying Advanced Analytics℠, ID Analytics for Compliance reduces the need for manual reviews by up to 50%.

ID Analytics for Compliance was specifically designed to eliminate costly compliance burdens by delivering on-demand identity intelligence that has been proven effective throughout the communications, financial services, mortgage, retail, and auto lending industries for more than five years. In fact, this same technology is already included as a core component of Red Flag compliance programs at Fortune 500 institutions.

Comparison with Alternative Approaches

Most commercially-available Red Flag offerings focus primarily on the first two aspects of compliance – specification and detection. So, even though a company may have specified applicable Red Flags and implemented a system to detect those Red Flag conditions, it is now faced with the challenging problem of resolving the Red Flags that are triggered. Resolving a flag means that an organization “should provide for appropriate responses … that are commensurate with the degree of risk posed.” In other words, organizations should make a risk-based assessment of each triggered flag.

In a non-automated world, a fraud analyst would be notified of a particular Red Flag (e.g. address associated with multiple phone numbers) related to an individual case (e.g. an auto loan application) and then seek evidence as to whether or not the Red Flag is indicative of possible identity theft.
The fraud analyst would look at a variety of additional, independent sources to gather information about the actual address and phone information of the applicant; the fraud analyst might also examine the applicant’s information for common data entry errors such as transposition, dropped digits, etc. In the end, the fraud analyst would use judgment to reach a subjective (rather than an objective, risk-based) assessment that a particular Red Flag either “looks like fraud” or “doesn’t look like fraud.”

In contrast to this non-automated methodology, ID Analytics for Compliance applies identity intelligence to the Red Flag resolution challenge – using Advanced Analytics to examine the real-time Personal Topology associated with the identity information of the particular case at hand and determining if that identity (considered as a whole) is at risk of identity theft. This replaces the subjective assessment of the fraud investigator with an objective, risk-based assessment of the likelihood of identity risk – based on the ID Network’s millions of reported fraud events and hundreds of millions of non-fraud events.

Each flag is weighed against dozens of other variables to generate a comprehensive risk evaluation of the identity in question. If this evaluation indicates a low risk of identity theft, it means that the detected Red Flags were not indicative of identity theft and, thus, are resolved. When an identity is considered high-risk, specific Red Flags may be reported to the creditor in order to focus review efforts. Alternative technologies that only provide detection of specific flags, as opposed to risk-based analytics such as those provided by ID Analytics for Compliance, require that all triggered flags must be manually cleared and resolved, even for low-risk identities.

**ID Analytics for Compliance – In-Depth Approach to Red Flags**

ID Analytics for Compliance provides a solid foundation for Red Flag programs across a variety of industries. Any Red Flag program must contain reasonable policies and procedures to address the following four requirements:

1. **Identify:** Specify Red Flags that are relevant to a particular institution.

In addition to specifying relevant Red Flags, the program must also specify the sources of Red Flags (e.g., a shared fraud network, such as the ID Network). The ID Network contains more than 1 billion risk events with more than 2 million reported instances of identity fraud – ID Analytics has used this unique collection of identity risk data to categorize and understand relevant Red Flag conditions. ID Analytics for Compliance provides a real-time, comprehensive assessment of identity risk as well as specific Red Flags which provide supporting detail for high-risk interactions.

A sample of Red Flags within the ID Analytics for Compliance solution:

- Verification indicators which reflect whether or not an identity element is valid (e.g., SSN is a validly issued SSN; Date of Birth (DOB) is complete, etc.)
- Fraud indicators which are set to true if the input data is associated with reported frauds in the ID Network (e.g., SSN associated with fraud)
- Indicators which specify whether or not the input data elements are associated with each other (e.g., name linked to DOB in ID Network)
- Combination indicators that signal the risk associated with a combination of input data elements (e.g., Combination of SSN with other elements is risky)
- Velocity indicators which quantify the number of instances an identity element has been submitted to the ID Network during a given duration
2. Detect: Red Flags must be detected in the ordinary course of operations.
ID Analytics for Compliance evaluates more than 100 proprietary identity risk variables covering more than two dozen specified Red Flags. All variables are evaluated against the ID Network which contains detailed information on 2 million reported frauds. Identity risk can be evaluated in real-time or in batch across any customer communication channel.

3. Respond: Detected Red Flags must be evaluated and resolved.
ID Analytics for Compliance evaluates relevant Red Flags and weighs these flags, individually and in combination with multiple identity risk variables, to establish a statistically sound, empirically-based assessment of identity risk. The results are delivered as either a Low-Risk or High-Risk indicator based on a pre-determined identity risk threshold.

Not only does ID Analytics for Compliance detect the presence of Red Flags via the ID Network, but the Red Flags are actually resolved for low-risk identities via risk-based analytics. The Advanced Analytics used by ID Analytics for Compliance are already in use by Fortune 500 communications companies and financial institutions due to the proven ability to lower manual review rates by up to 50%.
Fewer manual reviews translate into lower operational costs, an improved customer experience, and protection of consumer privacy. When further authentication is necessary for high-risk identities, Certain ID™ is available to generate and deliver strong authentication questions that are top of mind for legitimate individuals. These questions are based on data from the ID Network, not public records.
The unique identity information within the ID Network ensures that Certain ID creates questions that are very difficult for someone perpetrating identity fraud to answer correctly. This is consistent with the regulatory suggestion (in Supplement A to Appendix J of the Red Flag rules) that asking challenge questions can trigger a Red Flag if “the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.” By avoiding dependence on publicly available information, Certain ID delivers a strong, yet cost-effective approach to resolving identity risk.

4. Evolve: Document a detailed process for periodically updating the program to reflect changes in risk.
The Red Flag rules state that “financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.”
The ID Network receives an average daily flow of 45 million attributes. This daily influx of identity-related data provides insight into changing fraud patterns. ID Analytics looks for evolving relationships among identity patterns and our portfolio of Advanced Analytics is updated to detect these new patterns. The ID Network is the nation’s only real-time, cross-industry compilation of identity information.

Red Flag Compliance – Best Practices

In order to provide guidance to creditors tasked with developing their own Red Flag programs, the Red Flag regulations include an Appendix containing examples of specific Red Flags. These examples should be considered standard benchmarks that regulators will likely consider when evaluating an organization’s Red Flag program. ID Analytics for Compliance automatically evaluates the Red Flag examples focused on Suspicious Personal Identity Information (PII) while transparently resolving these flags for low-risk transactions – in real-time. ID Analytics for Compliance provides unique capabilities that can identify, detect, and resolve the illustrative Red Flags related to “Suspicious Personal Identifying Information” based on data within the ID Network. The specific details include:
Address Discrepancies

In addition to resolving Red Flags, ID Analytics for Compliance provides resolution for address discrepancies as required by the Fair and Accurate Credit Transactions Act (FACTA). Given that more than 40 million Americans change their address annually, and millions more have address discrepancies across credit bureaus, ID Analytics has delivered a unique, practical approach to regulatory compliance that relies on accurate, up-to-date information and a unique perspective of identity risk.

New FACTA regulations going into effect concurrently with the Red Flag rules have two new requirements focused on resolution of address discrepancies. First, if a credit bureau detects an address discrepancy between a credit report and the address submitted on an inquiry, any user of the report must "form a reasonable belief that a consumer report relates to the consumer about whom it has requested the consumer report." In other words, the creditor must demonstrate that the credit report was retrieved for the correct identity. Second, credit card issuers are required to evaluate the validity of an address change request made in close proximity to a request for a new credit card.

The mere existence of an address discrepancy does not indicate fraud or error. The vast majority of address discrepancies are the result of latency in the credit reporting process. Credit reports were not designed to serve as the most current information on an individual. Address discrepancies are often the result of legitimate individuals relocating to a new address.

An address discrepancy could also reflect a typographical or other error in the consumer report or on the application itself. But, in the most sinister case, a discrepancy may reflect a fraud scheme where the perpetrator seeks to take control of a consumer account by moving that account to a new address. ID Analytics for Compliance can automatically distinguish between benign address variations with low identity risk and those address variations where the risk to the identity is of concern.
Resolving Address Discrepancies

ID Analytics retains substantial, proprietary information related to address risk. Through the feeds of information from its contributing members, the ID Network receives legitimate address changes as well as reported frauds on a daily basis. ID Analytics for Compliance can determine whether a specific address is a Post Office box, mail drop, prison, campground or other address type with a high likelihood of being associated with fraud. In addition, the ID Network contains detailed information on two million reported frauds including specific addresses used and the identity elements associated with these addresses over time.

However, assessing the risk of an address in isolation is an ineffective approach to resolving address discrepancies. ID Analytics for Compliance evaluates address risk by weighing and comparing dozens of variables in order to generate a comprehensive risk evaluation. These variables include other identity variables such as name, phone number, SSN, data of birth, and reported fraud information. This evaluation assesses the risk of an address discrepancy as it relates to a given identity. By evaluating identity and address risks in combination, ID Analytics can reveal suspicious linkage patterns. Examples of suspicious patterns include addresses associated with multiple or fictitious identities, a high velocity of credit applications at a given address, an address associated with a reported fraud, or a type of address associated with high identity risk.

ID Analytics for Compliance performs a rigorous and comprehensive analysis in order to determine to what degree, if any, an address discrepancy contributes to identity risk. If this comprehensive evaluation indicates a low risk of identity theft, then the address discrepancy is considered resolved.

ID Analytics for Compliance can also resolve address discrepancies in cases where an applicant has recently moved to a new address. These scenarios are particularly relevant to phone and utility providers as these companies are often the first point of consumer contact following a change of address. In these cases, a review of internal corporate records will not help because the address is new with respect to the particular consumer. Asking the consumer to demonstrably verify their address information will be burdensome because the consumer will not likely have supporting documents (e.g., a lease) easily accessible. Additionally, this supporting documentation can be easily forged. Traditional data matching sources also will not work as the new address will not yet have appeared in public records as being associated with this consumer.

The most viable option for resolving address discrepancies in cases of first use is to focus on the address submitted by the consumer and determine whether the new address - in combination with historical address information, identity behavior patterns, and anomaly detection algorithms - poses a high level of identity risk. By automatically resolving address discrepancies that generate a low level of identity risk, creditors can satisfy regulatory requirements without dramatically increasing operational costs.
In Summary

ID Analytics offers an effective compliance solution that will satisfy address discrepancy and Red Flag rule requirements pertaining to Suspicious Personal Identity Information while avoiding unnecessary review costs and account origination delays. Specifically, ID Analytics for Compliance will:

- **Minimize The Impact of Red Flag and Address Discrepancy Compliance** – ID Analytics identity risk solutions are 3X more effective than leading credit bureau technology. This equates to fewer reviews and reduced customer friction.

- **Satisfy Legislative Compliance Examples** – Illustrative examples contained in the Red Flag guidelines should be considered benchmarks that regulators will likely consider when evaluating Red Flag programs.

- **Resolve Red Flags and Address Discrepancies** – Automatically resolves Red Flags for low-risk identities resulting in lower operational costs.

- **Protect Consumer Privacy** – Data within the ID Network is never sold or distributed. Each automated resolution of a Red Flag or address discrepancy (avoiding a manual review) is one less time that a consumer’s sensitive information is handled or reviewed.

About ID Analytics, Inc.

ID Analytics, the leader in on-demand identity intelligence, provides unprecedented real-time visibility into the risk of individuals, protecting both organizations and consumers. ID Analytics pioneered identity scoring technology. ID Analytics combines three unique capabilities to assess risk and improve the customer experience across all consumer touch points: the ID Network®—the nation’s only real-time, cross-industry compilation of identity information; Personal Topology™—individual’s particular identity characteristics and their connectedness to each other; and ID Analytics’ proprietary Advanced Analytics℠. Leading communications and financial services companies, as well as major retailers, government agencies and healthcare insurers, all trust ID Analytics to provide solutions that drive new revenue opportunities, reduce financial losses, and facilitate compliance with federal regulations. ID Analytics is based in San Diego, CA.