

ID ANALYTICS FOR RED FLAGS COMPLIANCE

July 02, 2008

By TMCnet Special Guest

Identity Intelligence: The Key to Red Flags Rules Compliance

Javelin Strategy & Research recently reported that U.S. fraud losses reached a frightening \$45 billion in 2007. High profile data breaches at major U.S. firms such as TJX have raised the level of consumer consciousness about the potential dangers of identity fraud.

On November 1, 2008, the Federal Trade Commission will require financial services and other firms issuing credit to comply with Section 114 of the Fair and Accurate Transactions Act of 2003 (FACTA), otherwise known as the Red Flag rules. These regulations will require consumer-facing enterprises to build Red Flag rules capabilities into their online and call center applications to ensure compliance.

A comprehensive "identity intelligence" strategy can minimize the impact of the Red Flag rules by providing organizations identity risk assessments for individuals doing business with them, from the point of account origination to the end of the account lifecycle. These identity risk assessments can give organizations an advantage in their efforts to identify Red Flags and easily resolve them, while keeping compliance costs under control, maintaining a seamless customer experience and even protecting the privacy of individual consumers.

Identity Intelligence & The Regulations

Identity intelligence is the value derived from an analysis of an individual's particular identity characteristics, including one's connectedness to other individuals and their unique identity characteristics. This analysis uses advanced analytics and incorporates information from credit applications, financial transactions, various payments, general demographics, and changes to personal data such as name or address. The results provide organizations the ability to assess the identity risk of any consumer in real-time.

The FACTA legislation defines a Red Flag as a "pattern, practice, or specific activity that indicates the possible existence of identity theft." Organizations must identify the Red Flags most relevant to their organizations, be able to detect them during the ordinary course of business and respond by evaluating and resolving the detected Red Flags. Finally, creditors must be able to update their compliance program to reflect any changes in risk to the organization.

Identity intelligence can help organizations identify relevant risks and resolve them. These are two very critical advantages to organizations implementing Red Flag Rules compliance solutions.

Identifying & Detecting Red Flags

Company-specific risk factors can include logical variables such as those identifying inconsistencies between addresses and zip codes and relationship variables such as whether a phone number is linked to fraud or simply an unusual application activity.

A shared fraud network such as ID Analytics' ID Network can help an organization define these variables, comparing their own experiences with fraud with those of other organizations contributing to the network. This collective knowledge can provide critical insights into potential identity theft and fraud risk indicators.

An institutional Red Flag programs can use these indicators to detect relevant Red Flags during the ordinary course of operations, such as the verification of a consumer's identity before the opening of a new account.

For existing customers, Red Flag solutions should be able to monitor transactions where there is identity risk, such as unusual change of address requests attempting to send bills to different addresses.

Responding to Red Flags

The regulations require organizations to “provide for appropriate responses to the Red Flags ... that are commensurate with the degree of risk posed.” But many Red Flag offerings in the market today take a rules-based approach to compliance, focusing primarily on specification and detection and leaving resolution unaddressed.

Organizations that can effectively detect and resolve Red Flags for low-risk consumers can reduce manual review processes that cost a company resources and can drive away customers.

If this review process is not automated, a fraud analyst must be notified and put to the task of evaluating whether or not each Red Flag is indicative of identity fraud. After looking at a variety of additional independent sources to gather information related to a questionable address or phone number, for instance, an analyst might also examine the address and phone information for common data entry errors such as transposition or dropped digits. The analyst will then make a subjective assessment that a particular Red Flag either “looks like fraud” or “doesn't look like fraud.”

The extra staff required for such roles can become expensive and the time taken to resolve each case can degrade what should be a seamless customer experience with the organization. Furthermore, consumers could be uncomfortable with the fact that such an analyst could have access to such a significant amount of information about them.

On the other hand, if this process is automated, an organization can quickly and cost-effectively resolve the majority of detected Red Flags and maintain a quality customer experience. Such an implementation could evaluate each Red Flag based on a pre-determined identity risk threshold, enabling organizations to easily classify results as either low or high risk. The human element that brings cost pressure is also addressed as well as the common concern over consumer privacy - there is one less person touching personal information.

By leveraging identity intelligence, an automated implementation can achieve an objective assessment of the likelihood of identity risk based on a knowledge base of reported fraud events and non-fraud events.

Each flag can be evaluated against dozens of other variables to generate a comprehensive risk evaluation of the identity in question. The faster an organization can determine that an account represents a low risk for identity theft, the faster Red Flags can be resolved.

An automated implementation should also be able to address the higher risk Red Flags through a process such as presenting customers with a set of questions. Ideally, authentication of an account holder's identity should be based on questions that are very difficult for someone perpetrating identity fraud to answer correctly. Federal regulators have suggested that such question not rely on easily compromised sources such as the information found in a customer's wallet or in a credit report. Such identity authentication should depend on more than publicly-available information and this requires access to a comprehensive body of information that only a shared fraud network like the ID Network can provide.

Updating the Red Flags Program

Finally, the Red Flag Rules require that a compliance program contain a detailed process for periodically updating the program to reflect changes in risk. This adaptive requirement states that “financial

institutions and creditors should update their 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.”

This, again, requires access to data that provides insight into changing fraud patterns and evolving relationships between identity patterns. As these patterns change, Red Flag implementations must be updated to address the new risks.

Age of Analytics

It has been said that the Information Age has been eclipsed by the Age of Analytics, where power resides with those who are best able to make sense of the growing body of information about ourselves. By helping organizations analyze identity and fraud behavior patterns, identity intelligence and a shared fraud network can be powerful assets in minimizing the impact of the Red Flags Rules regulations.

They help organizations gain critical visibility into individual identities and the fraud that threatens them, allowing them to easily define and implement flag indicators and automate resolution processes. This visibility can also protect consumer privacy by reducing the number of manual reviews of low-risk identities and provide insights on emerging threats to which Red Flags programs must adjust over time.

Furthermore, as an increasing number of fraud threats emerge over time, organizations are best served if they are able to adapt to new conditions. Identity intelligence and shared fraud networks such as ID Analytics' ID Network are enablers for this adaptability, preparing organizations for this set of regulations and the next.

Mr. Oscherwitz is the chief privacy officer and vice president of government affairs for ID Analytics Inc., a provider of on-demand identity intelligence services. Previously he was counsel to Sen. Dianne Feinstein, D-Calif., and represented her on the Senate Judiciary subcommittee on terrorism, technology, and homeland security.