

Meeting Identity Theft Red Flags Regulations with IBM Fraud, Risk & Compliance Solutions



Astute financial services leaders know that they need to leverage Red Flags Compliance investments to not only meet regulatory requirements but to also achieve additional business advantages.

Financial Services organizations are rushing to meet the new Identity Theft Red Flags guidelines jointly issued by the OCC, Board, FDIC, OTS, NCUA and FTC implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) and final rules implementing section 315 of the FACT Act.

The rules implementing section 114 require each financial institution or creditor to:

- Develop and implement a written Identity Theft Prevention Program (Program) *to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts.*
- Requires credit and debit card issuers to *assess the validity of notifications of changes of address under certain circumstances.*

Highlights

- **Integrate IBM Entity Analytics Solutions into existing systems to help meet 11 of the 26 Red Flags**
- **Assure you know the people behind the transactions to improve AML compliance**
- **Detect and prevent in real-time many other forms of fraud (credit card fraud, mortgage loan fraud, insider fraud, etc.)**

Additionally, the Agencies are issuing joint rules under section 315 that provide guidance regarding reasonable policies and procedures that a user of consumer reports must employ when a consumer reporting agency sends the user a *notice of address discrepancy*.

Given the mandatory compliance date of November 1, 2008, most financial institutions are looking to incorporate these new requirements in the context of their existing Anti-Money Laundering (AML) systems.

Assuring Compliance with IBM Entity Analytics Solutions

The ID theft Red Flags guidelines are divided into four major categories:

- Information from Consumer Reporting Agencies
- Suspicious Documents
- Suspicious Personal Identifying Information
- Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons

Across these four major categories, the flags deal with detecting and/or responding to events that may help detect and prevent identity theft.

The challenge is how to differentiate between an event that is "normal" and one that is "suspicious" or "potentially suspicious".

Four seemingly unique identities...



Figure 1: How would your system decide if this is a potentially suspicious pattern?

However, this is not an easy task for a variety of reasons. Even the best banking systems are exposed to naturally occurring data degradation such as data entry errors, or naturally occurring events (people move, change their names, etc.). Much more difficult to detect are deliberate deceptions. Consider the example in Figure 1. How would your system decide if this is a potentially suspicious pattern?

The IBM Identity Resolution solution has algorithms and intelligence that will flag to your systems and/or fraud analysts the fact that there are, indeed, suspicious patterns above. These capabilities are based on decades of best practices and insights gained from analyzing the techniques that are typically used repeatedly by people attempting to steal an identity or create fraudulent

identities to carry out a variety of illegal activities.

Now look at the same scenario in Figure 2. The red boxes and arrows show where data has been reused without any modifications (ex: using the same telephone number with different names and addresses). The grey boxes and arrows show where data has been modified slightly and then reused (i.e. adding or dropping a digit in an address or reversing date and month of birth).

Even one identity thief can do a significant amount of damage, but consider how much greater harm can be done by a group of fraudsters working together. *For example: could your system identify someone who is related in non-obvious ways to a known fraud suspect?*



Figure 2: IBM Identity Resolution detects and flags many techniques typically used to create fraudulent identities.

Quickly determine if a client or prospect has relationships with anyone that is considered "high risk"

<p>Attn: Joseph Carbella</p> <p>Presenting suspicious identities, including shared account with ...</p>	<p>Dr. Jaafar Singh</p> <p>Who listed the same address as...</p>	<p>Mahmut Mazhar</p> <p>Suspect in the armed robbery of a bank and who shares a phone number with...</p>	<p>Larry Cho</p> <p>Listed on consolidated watch list for funding terrorist activities</p>
----------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

Figure 3: IBM Relationship Resolution detects and flags subtle and hidden linkages between individuals that may represent criminal networks.

In Figure 3, we can see that the person on whom we have just received a fraud alert, Larry Cho, is related by only three degrees of separation to an existing account holder. This alerts you to the fact that you

should beware of continuing to have Joseph Carbella as a client.

The IBM Relationship Resolution solution has algorithms and intelligence that will flag to your systems and/or

fraud analysts the fact that there are non-obvious relationships between current or potential account holders and people who are known fraudsters. These capabilities are based on decades of best practices and insights gained from analyzing the techniques that groups of criminals typically use to work together to carry out a variety of illegal activities.

IBM Entity Analytic Solutions and 11 of the 26 Red Flags

Let's examine a summary of 11 selected red flags and consider briefly how the IBM Entity Analytics Solution can help lower identity thefts and achieve compliance automatically and in near real-time:

Information from Consumer Reporting Agencies

Red Flag 1. A fraud or active duty alert is included with a consumer report. *Ensure that you do not have accounts for people related in any way to persons who are named in fraud alerts.*

Red Flag 2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report. *Examine accounts for people related in any way to persons who are named in credit freeze reports.*

Red Flag 3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 571.82(b) of this part. *Examine current accounts and applications for suspicious patterns relating to address discrepancy information.*

Suspicious Documents

Red Flag 5. Documents provided for identification appear to have been altered or forged. *Examine current accounts and applications for suspicious patterns relating to name(s), addresses, phone numbers, etc., used on the suspicious documents to determine if you have other clients you may not want to continue to have as clients.*

Red Flag 9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled. *Examine current accounts and applications for suspicious patterns relating to name(s), addresses, phone numbers, etc., used on the suspicious application to determine if you have other clients you may not want to continue to have as clients.*

Suspicious Personal Identifying Information

Red Flag 10. 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 address on an application is fictitious, a mail drop, or a prison; or
- c. The phone number is invalid, or is associated with a pager or answering service.

Examine current accounts and applications for non-obvious relationships where the same inconsistent information (address, phone number, etc.) is being used.

Red Flag 12. 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.

Examine applications real-time for obvious and non-obvious re-use of known fraudulent addresses, phone numbers, etc., to flag people who should be denied accounts.

Red Flag 14. The SSN provided is the same as that submitted by other persons opening an account or other customers. *Automatically receive alert when a Social Security Number on an application matches that of an existing customer or account.*

Red Flag 15. 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. *Automatically receive alerts when prospects or clients are attempting to use information that is same or similar to that of others (see figure 2 above).*

Red Flag 17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor. *Automatically receive alerts real-time when inconsistent information is provided. For example,*

the same name with two different addresses or two different home telephone numbers.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons

Red flag 26. 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. *Quickly determine if any information used in the fraudulent account (address, phone number, date of birth, SSN, etc.) has been used (either exactly or modified lightly) in found in any other accounts or applications.*

Leveraging Red Flags Compliance for Additional Business Advantage

Astute financial services leaders know that they need to leverage compliance investments to not only meet regulatory requirements but to also achieve additional business advantages. As previously noted, most financial institutions plan to implement Identity Theft Red Flags guidelines within their AML systems.

IBM Entity Analytics Solutions can complement existing transactional AML systems and help reduce the possibility of money being laundered through a financial institution. Transaction monitoring systems do just that – they monitor transactions within an account. They cannot differentiate between monitoring the accounts of multiple people versus monitoring accounts of a person using multiple identities.

IBM Entity Analytics Solutions can complement existing transactional AML systems by automatically flagging in real-time persons trying to create fraudulent identities as well as networks of people related in obvious and non-obvious ways. *The fact that this is done in near real-time means that you can detect and prevent money laundering and payments fraud before it happens.*

For more information

Identity Theft Red Flags guidelines must be implemented by November 1, 2008. IBM Entity Analytics Solutions (Identity Resolution and Relationship Resolution) can be integrated into your existing AML systems to

help assure compliance with various identity-related red flags and, at the same time, extend and enhance your AML capabilities and reduce payments fraud. IBM has other related assets that can help with other flags, such as unstructured searches, ETL requirements and best practices relating to compliance.

For more information about these solutions, please visit

www.ibm.com/software/data/ips/solutions/tfi/banking.html



© Copyright IBM Corporation 2008


IBM (United States of America)
Entity Analytic Solutions
6600 Bermuda Rd, Suite A
Las Vegas, Nevada
United States of America, 89119

Printed in the United States of America
3/08
All Rights Reserved.

DB2, IBM, the IBM logo, and the On Demand logo are trademarks of International Business Machines Corporation in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

 Printed in the United States of America on recycled paper containing 10% recovered post-consumer fiber.