ACAMS Connection
A bi-weekly e-zine for ACAMS members
Association of Certified Anti-Money Laundering Specialists®
ACAMS®

Section: ACAMS Connection
Title: How can I be better prepared to identify financial fraudsters?
Date: 9/30/2009

In spite of banks' best efforts to meet the requirements for know your customer (KYC) and enhanced due diligence (EDD), financial criminals, fraudsters, drug lords and other unsavory individuals still lurk in the customer databases of many institutions.

David Schiffer, President, Safe Banking Systems, has over thirty years' expertise developing software and methodologies that take watch list filtering to the next level. Recently, the company's proprietary software and techniques for collective entity resolution identified several convicted terrorists and criminals that still held valid FAA Certification. Within twenty four hours of these names being revealed to the TSA and the FAA by a New York Times reporter, six of the licenses were revoked. An article appeared in the New York Times (http://www.parsintl.com/19158.pdf), which described the individuals and the action taken by the FAA.

Yet, the question remains: if the FAA and the TSA could miss terrorists and criminals of this magnitude, what are you missing? And, what additional steps can you take to identify and root out fraudsters and other potential threats from your customer database? David Schiffer offers some advice:

• Outsource List Management Services. Monitoring and managing a set of watch lists is labor-intensive, costly and prone to error. Select an automated service that goes beyond list consolidation and offers data enhancement and optimization. Ongoing review and validation of information continually improves data integrity, which results in more accurate resolution.

• Understand what is contained in a watch list reference file. The integrity of this file is paramount. Factors such as single name aliases, alternate spellings, name parsing, unknown information and extraneous text can impact the quality of the data and ultimately the filtering results.

• Focus on quality as well as quantity. Intelligent filtering should not only reduce the quantity of alerts but should also improve the quality of the alerts generated. A truly comprehensive risk-based process objectively identifies the most prominent and notorious politically exposed persons (PEPs) and other high-risk entities in a database. It analyzes the complex relationships with their underlying attributes, information sources and related entities and ranks their political and criminal exposure to flag those alerts with the highest relevance and those most likely to be true.

• Invest in ongoing compliance training to stay ahead of the risk. Staff are the first line of defense to safeguard your institution's financial and reputational integrity. Well-trained compliance staff will understand the data and how to identify links and relationships within the data. An advanced curriculum that explores variations in the spelling of names, the diverse cultural naming conventions, name order complexities and other common inconsistencies can greatly improve investigative skills. The ability to distinguish true matches quickly and

efficiently will no doubt save an institution money in the long run.

• Prepare and Prevent. An ounce of prevention is worth a pound of cure. When conducting due diligence for a merger or acquisition or preparing for regulatory examination, the consequences can be detrimental if risk cannot be evaluated quickly and accurately. An independent forensic analysis can alleviate all doubt by prioritizing the highest risk first. This is an effective, pre-emptive measure to identify and root out potential threats from your customer database or from the database of the proposed acquisition.

Forward-thinking institutions that focus their efforts on the five points above will have taken the critical steps to mitigate risk and safeguard their reputations against financial fraudsters lurking in their databases.