ACAMS® TODAY
The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

The PEPs challenge

Managing alerts is a continuing dilemma for even the most sophisticated financial institutions. Having too many Politically Exposed Persons (PEPs) and high-risk entities, with too many common names, will generate too many alerts. How to reduce the volume and improve the quality of alerts is every institution's conundrum. What steps can be taken to flag the highest risk alerts for further investigation? To limit false positives? To generate and prioritize the more relevant alerts? To make the review process manageable — and defensible to regulators?

Developing a defensible strategy, while implementing sound operational processes in a dynamic regulatory environment, requires a risk-based approach. Effective PEP scanning will ensure that the financial institution can:

- identify potential customer risk
- meet all regulatory requirements
- maximize the efficiency of its resources
- realize optimal return on its technology investment
- leverage synergies with other enterprise-wide risk management or fraud prevention programs

It is difficult, if not impossible, to address these issues without an adequate investment in technology. Yet, more often than not, traditional models for determining return on investment (ROI) and cost will be applied when evaluating anti-money laundering (AML) and compliance technology purchases. Attempts to calculate ROI to determine whether to invest in a system do not normally consider the ways that risk mitigation and potential loss avoidance can create ROI value. Financial institutions should be mindful of the broader benefits of ROI when assessing technology options.

Institutions that have introduced PEPs filtering understand the pain that too many false positives and irrelevant alerts cause to resource allocation and productivity. That has become an all too familiar complaint. And, they understand that name matching for PEPs is only one component of a sound AML strategy.

With that in mind, here are five key operational strategies that institutions should consider in meeting the PEPs filtering challenge head on:

1) Determine how the definition of PEPs applies to your institution's risk profile

The Financial Action Task Force (FATF) is an inter-governmental body that develops and promotes national and international policies to combat money laundering and terrorist financing. More than 130 countries have endorsed the FATF 40 Recommendations as the leading international AML standard. Recognizing the absence of a clear definition for a PEP, FATF issued guidelines defining the term. Various government pronouncements, such as the USA PATRIOT ACT and the European Union Directive, offer similar definitions for a PEP, which include:

- A current or former senior official, elected or appointed, in the executive, legislative, administrative, military, or judicial branch of a foreign government.
- A senior official of a major foreign political party.
- A senior executive of a foreign government-owned commercial enterprise such as a corporation or business.
- An immediate family member of such an individual, meaning spouse, parents, siblings, children, and spouse's parents or siblings.
- Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate of a senior foreign political figure.

Interpretations of this definition vary from country to country and from institution to institution. Some focus only on foreign political figures, while others may limit the definition to the national or regional level. Despite multiple interpretations, one thing is clear — PEPs pose a heightened risk.

To mitigate this risk, institutions must first weigh their tolerance for risk vis-à-vis business considerations, such as generating revenue, and practical considerations, such as safeguarding the bank's reputation. Although high net worth or prominent individuals may be considered desirable as private clients, when they are identified as PEPs, and put in the context of their positions of influence and network of relationships, they are likely to bring increased risk of reputational harm to the

Reprinted with permission from the September/October 2008 Vol. 7 No. 5 issue of *ACAMS Today* magazine, a publication of the Association of Certified Anti-Money Laundering Specialists

financial institution. Plus, legal entities associated with them cannot be exempt from scrutiny, since money laundering activities frequently involve private companies, trusts, charities and foundations.

While risk management and its related risk assessment process remain specific to a financial institution's own internal policies and risk appetite, it is important to note that a risk-based approach is not only considered "best practices" in the industry but is also endorsed at the international level. An effective risk assessment process includes:

- Establishing risk-based procedures to determine if a customer is a PEP.
- Providing adequate training and developing a management approval process for establishing an account relationship with a PEP.
- Instituting a comprehensive review to determine the source of funds and/or assets applied to transactions and account activities of a PEP.
- Ongoing monitoring and enhanced due diligence of the PEP account relationship.

Risk can be mitigated only by identifying PEPs in your customer information file, determining if your institution's risk profile supports continuing the customer relationship, and establishing enhanced monitoring that meets international standards and regulatory requirements.

2) Optimize available databases of PEPS and other heightened risk entities

Providers of watch-list databases are in the business of building and updating data to serve a vast community of users worldwide. They scan hundreds of thousands of information sources across the globe to populate their databases with thousands of profiles of every conceivable high-risk entity. Fraudsters, terrorists, PEPs, money launderers and others are available, along with multiple fields of identification and risk categories.

The challenge for compliance officers is to maximize value from this torrent of data and use it to reduce risk. More often than not, organizations pay for the entire database but use only a fraction of the information available. Filtering against a larger subset of the database to prove a return on investment does not make sound business sense unless there is a process in place to identify, rank and manage the alerts generated.

There is no single right answer when it comes to deciding which lists to use, what percentage of names to match against, what fields and attributes to search and how to sort through the data to return meaningful results. These decisions will — and should — vary from institution to institution. Understanding where the greatest exposure lies based upon your organization's risk profile should be the driving force in deciding what and how much to filter. Are there specific geographic regions that pose a heightened threat? Are high-ranking government officials worldwide a concern? Or is keeping a watchful eye on local politicians important?

There is no single right answer when it comes to deciding which lists to use

Once an institution can pinpoint areas of concern, metrics provide a useful tool for identifying key variables (e.g., geography, names, position, ranking, etc.) and apportioning the risk embodied in those variables to individuals so that a risk profile develops. Filtering against a well-targeted subset will return a manageable number of high-quality alerts. The 80/20 rule, well-known as a business rule-of-thumb, is no less applicable here: Financial institutions can typically expect to cover 80 percent of their exposure by filtering against 20 percent of a particular list. The 80/20 rule reflects the distribution of risk in a database and highlights why it is critical to identify risk sources and scan against those specific subsets, rather than perform a global scan of a broader nature.

Databases are living entities that grow and change constantly. A pro-active approach to mitigating risk requires ongoing vigilance and tweaking of the filtering and matching processes. As institutions become more skilled at identifying risk categories and implement improved processes to identify and review alerts, they will be able to expand filtering to other subsets within the database, thereby deriving greater value from this often underused asset.

3) Establish criteria to automate processes and decision alerts

The role of compliance in protecting the reputation of a financial institution has become essential to its core business operations. AML policies must be fully integrated with routine business operations to prevent and detect activities that could lead to negative publicity, reputational damage and regulatory penalties. Once institutions understand the nature of their risks, regulatory requirements and institutional brand protection policies, they should carefully evaluate possible automated solutions. Automation becomes essential when prioritizing high-risk activities across multiple business lines, since manual processes are time-consuming, costly and ineffective, especially when dealing with large volumes of customer information and transactions.

A combination of human resources and technology is necessary to adapt to business and regulatory changes while driving process efficiencies. Most financial institutions are interested in solutions that:

- Mitigate risks identified in their risk assessments,
- Can be implemented in months rather than years,
- Have lower infrastructure and support costs,
- Are scalable to meet changing needs.

A sound AML program will be customized to fit an institution's blend of assets, customers, geographic locations, products, services and risk tolerance. There is, however, a common set of criteria for developing effective processes. A sound AML program should be:

- **Well-defined:** The process passes a reality check and is appropriately documented.
- **Defensible:** It withstands examination, and decisions can be justified to internal auditors and external regulators.
- **Dependable:** It ensures the desired results based on risk mitigation policies.
- **Repeatable:** It is iterative and supports ongoing "tweaking".
- **Flexible:** It can be adapted to ongoing changes to regulatory requirements, operational workflow and risk assessment.

Establishing "best practices" for scanning customer data means identifying relevant data to be detected by an automated filter as well as any data that might be useful to staff who investigate the alerts generated. Also, by selecting the optimal

Only by understanding the examination process and what types of controls regulators are seeking can an institution be prepared

configuration to meet their process flow requirements, institutions will maximize the impact of their technology investment.

Regardless of the software a bank selects and the time and expense of implementation, the key to success is whether an institution has developed effective procedures and processes to resolve the exceptions produced by the systems. And, more important, if it has trained, skilled professionals to execute those procedures.

4) Understand how specialized AML/compliance software for exposure ranking can streamline workflow and facilitate filtering

Since 2001, large and small institutions alike have jumped on the AML software bandwagon. No longer able to fly under the radar or to simply assume exposure to be low-risk, organizations now have an obligation to assess their relative risks. In a December 2007 report, Celent, the worldwide research and advisory firm, predicted that global risk and compliance spending would surpass US $14 billion in 2008. A portion of this spending is no doubt geared toward solutions that address exposure ranking.

Getting the most from your AML software provider goes further than simply reducing false positives. Institutions are faced with the challenge of optimizing the filtering process by identifying relevant alerts, prioritizing review, minimizing processing time, quantifying risk and developing a manageable overall approach.

Although systems have become more "intelligent," the dynamic nature of database information means that no system will identify 100 percent of PEPs 100 percent of the time. Understanding where your institution lies on the risk-exposure continuum will enable you to tailor filtering and PEP coverage to your institution's specific appetite for risk. Be prepared with a realistic appreciation of the trade-off between assuring broad PEP coverage and keeping the number of alerts manageable. Coverage that is too broad will generate an unwieldy number of alerts, making review in a timely fashion difficult, if not impossible. Coverage that is too narrow risks overlooking PEPs and other heightened risk entities.

Look for a system that filters across various characteristics for each customer or PEP (e.g., geography, business associates, family members, position, etc.), identifies points of correlation and conflict, and rates the strength of the matches. Risk ranking, which raises the profile of relevant alerts, creates a more efficient review process. It enables compliance staff to make prudent use of time by focusing investigation on a manageable number of high-priority alerts.

The right AML and compliance system can enhance filtering and improve workflow by:

- Prioritizing relevant alerts,
- Eliminating irrelevant hits,
- Reducing false positives,
- Objectively ranking relative political exposure of PEPs,
- Tailoring the level of filtering to match an institution's risk profile

The result is a more manageable process that supports timely review of alerts, makes decisions about alerts more efficiently, makes judicious use of resources, reduces costs, and ultimately lessens an institution's exposure.

5) Identify pre-emptive measures that can be taken to prepare for regulatory reviews

In addition to meeting internal regulatory controls, financial institutions are subject to comprehensive examination by regulatory authorities on an ongoing basis. These examinations are intended to:

- Assess the effectiveness of the institution's AML and compliance programs,
- Assess compliance with regulatory requirements governed by their jurisdiction,
- Provide a review of risk management practices.

Only by understanding the examination process and what types of controls regulators are seeking can an institution be prepared. To begin with, examination procedures have changed. In the past, they were audit-driven and focused primarily on testing transactions. Now, exams scrutinize the actual policies and processes that have been implemented. Regulators look for risk-based, streamlined policies and procedures, effective data management and thoroughly trained employees.

Practical application of the institution's written policies, procedures and processes is a first step in determining the overall adequacy of a compliance program. Institutions will be expected to prove their processes are well-documented and well-tested and that risk-based decisions were justified. A defensible process includes a system of internal controls to ensure ongoing compliance, independent testing of those controls and maintaining adequate documentation.

Ongoing risk-based monitoring of PEPs and other high risk entities is at the core of a steadfast compliance program and will ensure that a financial institution is prepared for a review at any time. A risk-based strategy can be justified both internally and to regulators. Consideration should be given to adopting a broader view when scanning for PEPs and other high risk entities. This means not only scanning for compliance, but also for fraud prevention and reputational risk.

A pro-active, risk-based strategy will not only include self-audits but will also employ periodic forensic analyses of customer information files. This pre-emptive measure prioritizes identification of the highest risk and most relevant alerts, which are frequently buried beneath large volumes of false positives pending further investigation. As regulators continue to require more robust AML programs, forensic analysis can be an effective tool in preparing for regulatory examination, conducting due diligence for a merger/acquisition or implementing a new line of business.

In summary

The last 10 years have brought enormous change to the ways financial institutions address AML and compliance demands. No longer a back-office, transaction-driven exercise, compliance monitoring is now closely aligned with strategic and operational goals. Increasingly sophisticated technology, systems, data gathering and data mining techniques will continue to influence the face of PEPs filtering and compliance. Understanding the risks and market forces that impact your business, along with developing a flexible framework that can readily be adapted to these internal and external drivers, will provide institutions with the best offense for winning the PEPs challenge.

David Schiffer, president, Safe Banking Systems, Mineola, NY, USA, David.Schiffer@safe-banking.com

Safe Banking Systems, LLC
114 Old Country Road, Suite 320
Mineola, NY 11501 USA

TEL +1 631-547-5400
FAX +1 631-547-5415

www.safe-banking.com