OFAC Name Matching and False-Positive Reduction Techniques

To meet Office of Foreign Assets Control rules for combating money laundering, financial institutions need to take stock of new software tools that automate the process of identifying possible illegal activities and reduce the probability of unwarranted red flags.

Executive Summary

Complying with Office of Foreign Assets Control (OFAC) regulations[1] and transaction filtering are key requirements for all financial and nonfinancial institutions. Financial institutions are the primary medium for money laundering and they are typically more vulnerable compared with other businesses.[2]

As such, financial organizations are working to ensure that their payment networks and money transfer solutions are not used inappropriately by the customers listed on the Specially Designated Nationals (SDN)[3] list. However, legitimate transactions sometimes are flagged as problematic for "false" hits (also known as "false positives") during the transaction review process. Screening transactions and clients for possible sanction violations is an essential component of an effective compliance program.

It is a real challenge to identify and block suspicious transactions while processing higher volumes of legitimate straight-through transactions with greater accuracy and maintaining operational efficiency and client service level agreements (SLAs).

Financial institutions typically spend more time, money and resources investigating false positives as transaction volume and money transfer activity increases. This can be reduced by improving their OFAC compliance processes and implementing new software with sophisticated time-saving matching algorithms that recognizes different variants or misspellings of names and thus reduces the number of false positives to a minimum. Other approaches include intelligent automation workflows, robust management and audit controls, implementing industry best practices and gaining the technical ability to analyze past sanctions screening results.

This white paper offers advice on unique strategies to reduce the false-positive rate, including name-matching techniques and critical mitigation steps.

Anti-Money-Laundering Regulatory Requirements and Their Expansions

The fight over money laundering started in 1970 through the Bank Secrecy Act (BSA).[4] Since then, many additional regulations have been enacted to provide law enforcement and government agencies with the most effective tools to combat money laundering (see Figure 1). Post 9/11,

A Chronology of AML Activities

Year	Law or Group	Definition or Responsibilities	Content or Important Releases
1970	Bank Secrecy Act	The primary U.S. anti-money-laundering regulatory statute, enacted in 1970 and most notably amended by the USA PATRIOT Act in 2001.	Requires banks to track cash transactions, file CTRs for transactions of $10,000 or greater and report suspicious activity – and to keep records of various financial transactions.
1974	Basel Committee on Banking Supervision	Established by the central bank governors of the G10. Promotes sound supervisory standards worldwide.	Customer Due Diligence for Banks paper (2001). Sharing of financial records between jurisdictions in connection with the fight against terrorist financing (2002). General Guide to Account Opening and Customer Identification (2003). Consolidated KYC Risk Management paper (2004).
1986	Money Laundering Control Act	The first law in the world to make money laundering a crime.	This act criminalized the act of money laundering, prohibited structuring to avoid CTR filings and introduced criminal and civil forfeiture for BSA violations.
1989	Financial Action Task Force	An intergovernmental body with 34 member countries and two international organizations established by the G7 to develop policies to combat money laundering and terrorism funding.	Comprises 40 recommendations on money laundering and terrorist financing (see Figure 2).
1991	European Union	The EU directives on anti-money-laundering require EU member states to issue legislation to prevent their domestic financial systems from being used for money laundering.	1st EU Directive on Prevention of the Use of the Financial System for the Purpose of Money Laundering (1991). 2nd Directive (2001). 3rd Directive (2005).
2001	USA PATRIOT Act[5]	Enacted on October 26, 2001, it brought more than 50 amendments to the Bank Secrecy Act.	This piece of legislation significantly upped the ante and the regulatory burden on U.S. institutions, and has served as a driver of AML regulation in other countries.
2002	Wolfsberg Group	Association of 11 global banks. Aims to develop standards on money laundering controls for banks.	Wolfsberg Anti-Money-Laundering Principles for Private Banking (2012). The Suppression of the Financing of Terrorism Guidelines (2002). Anti-Money-Laundering Principles for Correspondent Banking (2014).
2004	Egmont Group	Informal networking group of financial intelligence units.	Statement of Purpose (2004). Principles for Information Exchange Between Financial Intelligence Units for Money Laundering Cases (2013). Best Practices for the Exchange of Information Between Financial Intelligence Units (2004).

Figure 1

FATF 40 Recommendations

A. Legal Systems

Recommendations 1, 2	- Scope of the criminal offense of money laundering.
Recommendation 3	- Provisional measures and confiscation.

B. Measures to Be Taken to Prevent Money Laundering and Terrorist Financing

Recommendation 4	- Financial institution secrecy laws.
Recommendations 5-12	- Customer due diligence and record-keeping.
Recommendations 13-16	- Reporting of suspicious transactions and compliance.
Recommendations 17-20	- Other measures to deter money laundering and terrorist financing.
Recommendations 21-22	- Preventive measures to the countries that do not or insufficiently comply with the FATF recommendations.
Recommendations 23-25	- Regulation and supervision.

C. Necessary Measures in Systems for Combating Money Laundering and Terrorist Financing

Recommendations 26-32	- Competent authorities, their powers and resources.
Recommendations 33-34	- Transparency of legal persons and arrangements.

D. International Cooperation

Recommendation 35	- International instruments.
Recommendations 36-39	- Mutual legal assistance and extradition.
Recommendation 40	- Other forms of cooperation.

Figure 2

Congress passed the USA PATRIOT Act, which dramatically expanded the security requirements to implement comprehensive customer due diligence (CDD)[6] policies, procedures and processes for all customers, and enhanced due diligence[7] (EDD) for high risk customers who pose a higher risk for money laundering and terrorist financing. For example, politically exposed persons (PEPs)[8] are considered high risks and require enhanced due diligence, predominantly while using private banking services. This act also provided a platform for other AML-related regulations and requirements to be enforced.

Key Elements of AML Solutions

Financial institutions are required to put enhanced AML capabilities in place. Banks require AML environments that can be reasonably expected to detect, deter and report suspicious activity. Key elements of AML solutions include:

- Know your customer (KYC).
- Customer due diligence (CDD).
- Suspicious activity monitoring.
- Case management services.
- Watch-list filtering.
- Record-keeping.
- Customer behavior.

Watch-List Filtering

Watch-list filtering solutions help financial institutions keep ahead of regulatory changes and eliminate the risk of fines and reputational exposure. They filter transactions and customers against sanctions. The Treasury Department, State Department and Commerce Department each maintains lists of companies and people that all U.S. citizens and companies are forbidden to do business with. The watch lists are frequently updated and contain thousands of names, hundreds of which are located in the United States. Business relationships with entities on these watch lists can result in extremely large fines and other penalties, including loss of export privileges or imprisonment.

Watch-list filtering was designed to detect matches against each part of the name. The screening criteria used by banks to identify name variations and misspellings must be based on the level of OFAC risk associated with the particular product or type of transaction. For example, in a high-risk area with a high volume of transactions, the bank's software should be able to flag close name derivations for review. The specially designated nationals (SDN) list provides name derivations, but may not include all such derivations. Advanced software may be able to catch variations of a name not included on the SDN list.

SDN List

SDN contains a list of individuals, groups and entities subject to economic sanctions by the U.S. Treasury and the Office of Foreign Assets Control. OFAC administers and enforces economic sanction programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using asset blocking and trade restrictions to execute foreign policy and national security goals. The SDN list is frequently updated and covers:

- Individuals and entities located anywhere in the world that are owned or controlled by, or acting on behalf of, the government of a sanctioned country.
- Specially-designated global terrorists/narcotics traffickers.
- Foreign terrorist organizations.
- Individuals identified as involved in the proliferation of weapons of mass destruction.
- Companies, banks, vessels and individuals that, at first glance, may not seem to be related to the sanction targets they represent.

Challenges in Updating Watch Lists

There are several types of watch lists published by governments or economic, political and law enforcement bodies. Lists published by commercial sources, such as politically exposed person (PEP) lists, and internal blacklists created by companies themselves may also be required for review.

The most common types of watch lists include:

- OFAC sanction lists (e.g., SDN; Palestine Legislative Council list).
- Other official watch lists (e.g., Interpol most wanted).
- Country-specific sanction list (e.g., China sanction list/Japan sanction list).
- Region-specific sanction list (e.g., Asian sanction list/European Union sanction list).
- Business-specific sanction list (e.g., trade-specific caution list of exporters).
- Internal lists: Banks generate this list for high-risk customers.

Above all, lists may not necessarily be applicable to all transactions. For example, the trade-specific sanction list may not apply for FX transactions, and the Japan sanction list may not be applicable for UK transactions. It may be applicable sometimes – the compliance officer will decide which list is applicable for which transactions. These days, financial institutions locate their screening units in one or two centralized locations. As such, the screening team screens transactions of different countries in multiple currencies in one location. Filtering software, however, needs the ability to apply a specific sanction list based on country or currency. Financial institutions are typically challenged to maintain a different sanction list of different lines of businesses/countries in one common piece of software.

Name-Matching Technology

Algorithms are the key to matching; the effectiveness of matching technology is defined by how powerful the algorithms are. Useful algorithms have powerful routines that are specially designed to compare names, addresses, strings and partial strings, business names, spelling errors, postal codes, tax ID numbers, data that sounds similar (such as "John" and "Jon") and more. Filtering capabilities range from simple name-checking functions to complex algorithms that can search and format/unformat text data from multiple payment and messaging systems with a high degree of accuracy.

The simplest filters offer "exact hit" matches to the SDN list, and robust filters use a variety of techniques to ensure that true negatives are not missed while the number of false positives is reduced. High-end OFAC engines offer sophisticated filters that identify all possible matches, confirm the reason and location of the hit within the transaction/message and provide tools to compare the hit with the entry in the OFAC database. These products offer the flexibility to bypass or stop certain transactions and include or exclude sanction lists with the help of rules. Some filters allow the bank to choose the fields within a given payment source (e.g., SWIFT Fields 50, 52 and 59) to be filtered, which substantially reduces processing time. There are two common types of matching technology on the market today: deterministic and probabilistic.

Deterministic aka Exact or Rules-Based Matching Technology

Deterministic matching uses a combination of algorithms and business rules to determine when two or more records match through unique identifiers such as SSN/passport/TIN numbers. It exactly matches on specified common fields; it generates links based on the number of individual identifiers that match among the available data sets. This is the easiest, quickest linking strategy; however, deterministic matching systems have a relatively lower degree of accuracy compared with probabilistic matching, and it suits applications where the number of records is relatively small (less than two million).

Probabilistic Matching Technology

Probabilistic matching refers to comparing several field values between two records, and assigning each field a weight that indicates how closely the two field values match. The sum of the individual fields' weights indicates the likelihood of a match between two records. Probabilistic matching technology performs statistical analysis on the data and determines the frequency of items. It then applies that analysis to weigh the match, similar to the way that the user can weight the relevance of each row.

Name-Matching Mechanism

Matching is the process of comparing two data sets in order to either identify the exact or potential match. Matching is often used to link records that have some sort of relationship. Since data does not always reveal the relationship between two elements, matching technology helps define rules for possible related items. This can be done in many different ways, but the process is often based on algorithms or programmed loops, where processors perform sequential analyses of each individual piece of a data set, matching it against each individual piece of another data set, or comparing complex variables like strings for particular similarities. The matching process looks at every word in each name/address line and the complete string of words in the transactions.

Matching algorithms manage foreign translations, misspellings and typing errors, alternate spellings, abbreviations, truncated words, synonyms, acronyms, first name initials, search codes (e.g., SWIFT BIC Code, IBAN) and compound or concatenated words. They accept as input any message/text file format, and will determine in milliseconds if there are names, companies, vessels, sanctioned countries or banking codes that match the selected sanction list, and this sanction list can be a combination of any official, internal and large third-party lists.

Direct Match or Exact Match (Deterministic)

A matching relationship between the two records is direct when these two records are a match by the underlying rule. When a customer name exactly matches with the name in the sanction list, financial institutions must react appropriately to comply with the USA PATRIOT Act and OFAC requirements. Noncompliance has resulted in significant fines/penalties as well as damage to the institution's reputation.

Payment String	Sanction Target	Matching Decision
David Carlos	David Carlos	Match
Osama Bin Laden	Osama Bin Laden	Match
Fidel Castro	Fidel Castro	Match

Indirect Match

A matching relationship between two records is indirect when they do not match each other; however, each of these matches may match a third record. For example, we may consider the strings ABCDEF, XBCPQR, ABCPQR. For instance, matching rules may conclude no direct match relationship between the first two strings, but each of these matches to the third string.

Payment String	Sanction Target	Matching Decision
David Carlos	Not on the list	Not a match
John Peter	Not on the list	Not a match
David Peter	David Peter	Match to Sanction List

Partial Match (Probabilistic)

Matching software may report possible matches when customer information is the same or similar to the watch list entity information. Two records show this type of relationship (very common in real life) when some (not all) elements of the first record match to some (not all) elements of the second record. A typical example will be the records corresponding to father and son living at the same address where many elements such as the last name, address and residence phone number might be matching, but the first name (and probably the middle name), mobile numbers, e-mail addresses and other such fields will not match. Extended families usually share a common last name. All of these same or similar names make it very challenging for the software to differentiate between them.

Additional information such as address, identification number, gender, height and age are needed to help determine the true match through further investigation.

Payment String	Sanction Target	Matching Decision
John Paul Castro	John Peter Castro	Partial Match – Paul ≠ Peter
David Jol Chung	Daniel Jol Chung	Partial Match – David ≠ Daniel
John Longman	Emily Longman	Partial Match – John ≠ Emily

Fuzzy Matching (Probabilistic)

Fuzzy matching is the implementation of algorithmic processes (fuzzy logic) to determine the similarity between elements of data such as business name, personal name or address information. The fuzzy logic feature allows the algorithm to detect and evaluate near matches rather than require exact matching. Depending on the algorithm, it may consider alternate nicknames, such as "Mike" or "Mickey." Names (person, place or entity) would be easy to match if they were consistent; however, launderers use different techniques to bypass filter detection.

Sanction Target	Payment String	Matching Decision
Peter	Petr	Match through fuzzy logic
Qadir	Kadar	Match through fuzzy logic
Rahim	Raheem	Match through fuzzy logic

Phonetic Matching (Probabilistic)

Phonetic matching is the process of matching data using algorithms/functions that have been created and focus on how a word is pronounced rather than how it is spelled. A phonetic algorithm matches two different words with similar pronunciation to the same code, which allows phonetic similarity-based word set comparison and indexing. There are words that have different spellings but similar pronunciation and should be matched, such as Sofia and Sophia/Reynold and Renauld, etc. Hence, a matching engine is required to build connections based on different phonetic transformation[9] rules. Soundex, metaphone and double metaphone are the commonly used techniques while implementing phonetic-based matching.

Sanction Target	Payment String	Direct Match
Sofia	Sophia	Fuzzy Logic
Reynolds	Renaults	Fuzzy Logic
Smith	Smyth	Fuzzy Logic

The table below highlights various name variations.

Misspelling in names	Mike Jackson, Michael Jakson, Michael Jaxon, Mike Jaxson, Michael Jakson
Phonetic spelling differences	Michel, Michal, Miguel
Nicknames	Mike, Mick, Mikey
Initials	M J Jackson, Michael Joseph Jackson
Titles	Dr., Mr.
Missing name components	Michael Joseph Jackson, Michael Jackson
Out-of-order name components	Joseph Jackson, Michael, Michael Joseph Jackson
Omission of letters	Jackson for Jacson
Interchanging of vowels	Hussein for Hussien
Doubling of consonants	Mohamed for Mohammed
Cultural variations	William for Bill, Alexander for Alexi

False Positives Are a Burden

A false positive is the case where a transaction is associated with a genuine customer who is blocked because of a name or another match. False positives found by OFAC screening are a significant burden to financial institutions. Significant cost and effort are required to clear possible violations that are found to be unwarranted. This time-consuming process delays the payment release, which results in monetary expense by forcing firms to engage more human investigators.

False positives cannot be completely prevented; however, they can be minimized by using advanced software. The false-positive rate reflects the efficiency of the system. A 5% false-positive rate on one million transactions would result in the detection of fifty thousand false positives. Significant cost, time and effort are required to investigate and clear false positives. This also impacts straight-through processing rates, placing the organization at a competitive disadvantage. Sadly, a 5% false-positive rate is on the low side, which is really a nominal figure since most organizations see false-positive alerts between 50% and 70% of the time. For example, payment to a client who lives in Kerman, California could be blocked due to a match with city of Kerman, Iran.

False Negatives Are a Risk

A false negative is the case where a transaction is associated with a sanctioned entity but is not detected by the system. Failure to identify a sanctioned entity can be dire for a bank; it leads to an enforcement action against the bank and a reputational risk. For example, payment for SDN list entity Intermarket Holdings Limited (located at Harare, Zimbabwe) is not detected by the system.

OFAC List Penalties

For U.S. firms, OFAC compliance is an important aspect of doing business with foreign firms and individuals. U.S. firms must make sure they are not doing businesses with sanctioned individuals or firms.

All companies incorporated in the U.S., as well as their foreign subsidiaries, must comply with OFAC requirements. Failing to comply with OFAC regulations — and therefore doing business with specially designated nationals or other listed entities — opens companies and individuals to legal action and leads to substantial fines and possible imprisonment for employees.

- Unintentional violations:
  - Potentially forfeit the value of the contract or payment plus pay a fine.
  - Recent increase to $250,000 per IEEPA violation, retroactively applied.
  - Mitigating factors include:
    - Compliance plan (25% to 50% reduction).
    - First offense (25% to 50% reduction).
    - Self-reported violations (50% or greater reduction).
- Intentional violations: Fine for double the amount of transaction, plus criminal fines and imprisonment.
- Criminal penalties up to $10 million and 30 years in prison.
- Civil penalties:
  - Trading with the Enemy Act: $65,000.
  - International Emergency Economic Powers Act: $11,000.
  - Iraqi Sanctions Act: $325,000.
  - Foreign Narcotics Kingpin Designation Act: $1,075,000.
  - Anti-Terrorism and Effective Death Penalty Act: $55,000.
- Violations may result in blocked funds and seized goods, negative publicity and loss of reputation (see Figure 3).

Civil Penalties and Enforcement Information

Year	Number of Cases	Penalties/ Settlements (in $U.S.)	Highest Penalty (in $U.S.)	Description
2013	27	137,075,560	33,122,307	Royal Bank of Scotland plc agreed to remit $33,122,307 to settle potential civil liability for apparent violations of OFAC regulations.
			91,026,450	Weatherford International Ltd. agreed to remit $91,026,450 to settle potential civil liability for apparent violations of OFAC regulations.
2012	16	1,139,158,727	375,000,000	HSBC Holdings plc agreed to remit $375,000,000 to settle potential civil liability for apparent violations of OFAC regulations.
			619,000,000	ING Bank N.V. agreed to remit $619,000,000 to settle potential civil liability for apparent violations of OFAC regulations.
2011	21	91,650,055	88,300,000	JPMorgan Chase Bank N.A agreed to remit $88,300,000 to settle potential civil liability for apparent violations of OFAC regulations.
			1,661,672	Sunrise Technologies and Trading Corporation agreed to remit $1,661,672 to settle potential civil liability for apparent violations of OFAC regulations.

Figure 3

False-Positives Mitigation

False positives must be mitigated as much as possible, without creating new false negatives. The following series of steps will greatly reduce the number of false positives:

- **Screen sentences separately.** Filters should separate names, addresses and cities from other data. They should not combine these with other data in the sentence. Some filters will match words from anywhere and will screen data regardless of the order or the distance between them. Thus, Jose Gonzales who lives on Martinez Street might match with the blocked name Jose Martinez Gonzales. The filter should screen only the respective sentence such as name, address, etc., to minimize false matches.
- **Screen accounts separately.** Filters should screen personal and corporate accounts separately. For example, Mayan King Limited, which is a company in the SDN list, could match with the customer name Maya.
- **Screen vessels separately and match names with vessel names.** Shipping vessels or cargo ships have been a specific focus of OFAC over the past several years because of their ability to move large quantities of oil and petroleum products as well as uranium and other chemical materials necessary to the production of weapons of mass destruction by government and commercial entities specifically designated by OFAC. Vessels came into the sanction radar for carrying/smuggling weapons of mass destruction and narcotics. Detecting vessel names is a real challenge because they ply different tactics to misguide the system. Hence, it is recommended to screen the vessel category separately and create the rules specific to vessels matching with customer names.

  The following are tactics used to hide the identification of vessels and making them hard to trace for the eyes of investigators:

  - Using a vessel name such as Celestina/Carmela (owned by Islamic Republic of Iran Shipping Lines (IRISL)), which could be the name of a genuine customer.
  - Flip-flopping the names from one vessel to another and frequently changing the vessel names.
  - Using duplicate names.

The risk assessment process is a structured approach for assigning customers to different risk categories depending on specific attributes or behaviors. The customer or account is then monitored and managed according to the risk classification.

- **Determine screening fields.** In a message, the header block and text block or body contain most of the customer data. Identify and map the message to specific fields that have unique information subject to screening. The SDN list includes names and countries; therefore, fields such as name, country, passport numbers and TIN are more likely to be unique, so concentrate on screening fields.
- **Exclude local place names.** The address is not unique information for identifying a person, and such screening maximizes the risk of false positives. For example, an address of Havana, Illinois or Cuba, New York opens up opportunities for false positives, and the zip code could match the passport or TIN number. Exclude places such as street address, states, provinces, territories, zip codes and postal codes (numbers could match passport numbers).
- **Create rules for common names.** Names such as Jim/Jimmy, David, John and Mike are very common, and rules need to be created to avoid false positives.
- **Design customer risk profiles.** Customers should be classified based on their product lines, services, nature of transactions and geographic locations. The risk assessment process is a structured approach for assigning customers to different risk categories depending on specific attributes or behaviors. The customer or account is then monitored and managed according to the risk classification. Naturally, the institution would examine the behavior of high-risk customers more closely than low-risk ones. Parameters and scenarios could be applied differently to customers based on the potential risk they represent. The screening software should match customer data with multiple criteria.

  Take, for example, the following:

  - In a high-risk geographical location with a high volume of transactions, the software should be able to flag close name derivations for review.
  - In a high-risk geographical location with a high volume of transactions, the filtering software should send the transactions to the separate queue that is to be handled by the experts.

Quantity of Risk Matrix: OFAC Procedures

Low	Moderate	High
Stable, well-known customer base in a localized environment.	Customer base changing due to branching, merger or acquisition in the domestic market.	A large, fluctuating client base in an international environment.
Few higher-risk customers; these may include nonresident aliens, foreign individuals (including accounts with U.S. powers of attorney) and foreign commercial customers.	A moderate number of higher-risk customers.	A large number of higher-risk customers.
No overseas branches and no correspondent accounts with foreign banks. No electronic banking (e-banking) services offered, or products available are purely informational or non-transactional.	Overseas branches or correspondent accounts with foreign banks. The bank offers limited e-banking products and services.	Overseas branches or multiple correspondent accounts with foreign banks. The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payments or accounts opened via the Internet).
Limited number of funds transfers for customers and noncustomers, limited third-party transactions and no international funds transfers.	A moderate number of funds transfers, mostly for customers. Possibly, a few international funds transfers from personal or business accounts.	A high number of customer and noncustomer funds transfers, including international funds transfers.
No other types of international transactions, such as trade finance, cross-border ACH and management of sovereign debt.	Limited other types of international transactions.	A high number of other types of international transactions.
No history of OFAC actions. No evidence of apparent violation or circumstances that might lead to a violation.	A small number of recent actions (e.g., actions within the last five years) by OFAC, including notice letters, or civil money penalties, with evidence that the bank addressed the issues and is not at risk of similar violations in the future.	Multiple recent actions by OFAC, where the bank has not addressed the issues, thus leading to an increased risk of the bank undertaking similar violations in the future.

Figure 4

False Positive Mitigation Through Data Mining and the Tuning Process

Data Mining in Banking

Financial institutions manage huge amounts of banking data, and more data sets are being recorded daily. The growth of financial data collected far exceeds human capabilities to manage and analyze them efficiently in a traditional style. Global competitions, dynamic markets and the rapid increase in technological innovation have become important challenges for these organizations. They need to apply new business intelligence solutions because the traditional statistical methods do not have the capacity to analyze large data sets.

Data mining is used to solve business problems in patterns, causalities and correlations in financial information that are not obviously apparent to managers because of the volume of data. Data mining can first be used to analyze huge data sets and build customer profiles of different groups of the existing data. It can generate rules and models that can be used for understanding business performance and making new marketing initiatives, for market segmentation and risk analysis and for revising company customer policies.

Data Quality Is Key

Data quality is a key to this process; data sets have a different set of quality problems at the instance level. Some of them can be listed as missing values, dummy values or null. The independence and heterogeneity of each data source can also become data quality issues when an integrating task is required, as all conflicts must be solved. Fundamentally, data preprocessing steps are applied to deal with data quality issues. Techniques such as profiling, auditing, transformation and text analysis can be used to validate data, remove white spaces and possibly erroneous characters or split a single name field containing multiple attributes into a number of fields. These capabilities enable organizational data to be optimized to match rules.

Scanning solutions must be consistently accurate and return low false positives. Critically, all of these demands must be met while maintaining the lowest possible operational costs.

Historical Data Collection

The historical data collection phase starts with the initial collection of historical alerts followed by the gathering of supporting alert data: transactions, profiles and events. Because this process may require pulling lots of data from disparate systems, more time is spent on data gathering than on analytics. The goal is to build a set of data that can be used as input into the tuning and evaluation phases. Generally, a minimum of two to three months of historical data is needed; again, it differs depending on the scenario. The more data we get, the better it is for analysis.

Data Tuning Process

Fine-tune your operations to minimize errors and maximize efficiency. This process is to mitigate unnecessary hits. This tuning will help establish the proper balance point of true matches that must be stopped and reviewed with a lower quantity of false positives. It is a three-step process. There is no specific tuning process; it depends on the various factors such as line of business, volume and geographic location. Traditional statistical techniques such as logistic regression and comparing the results with more advanced data-mining techniques such as decision trees and neural networks are the generally applied tuning processes. The keys to applying tuning techniques are having quality historical data and using rigorous back-testing to review the before-and-after results of the tuning techniques. Once the tuning method has been selected, historical data will be tested in an existing OFAC test environment against the respective sanction lists to find out the false positive statistics. This statistic provides the results of before tuning and after tuning.

Exceptions aka Good Guys List Upload

Names that have been identified as false positives are "good guys," which need to be added to the OFAC filters in order to bypass false hits, reducing the volume and hit rate of the transactions. A good guy is created and tested before uploading into production. This process helps identify good guys or rules that can be used to mitigate volume in production.

Compliance Solutions

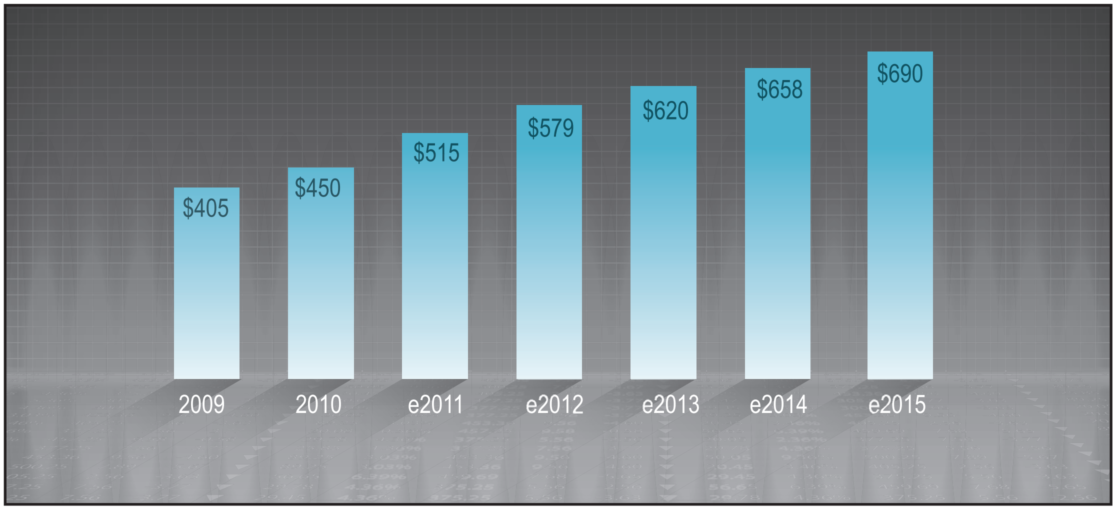
As a result of increased regulation, regulatory enforcement actions and new technology, financial institutions are under pressure to maintain regulatory compliance and high rates of efficiency. Scanning solutions must be consistently accurate and return low false positives. Critically, all of these demands must be met while maintaining the lowest possible operational costs.

The technology behind the watch-list software typically utilizes simple name-checking functions and complex algorithms that can accurately search formatted/unformatted text data from multiple payments and messaging systems to filter the correct result using different algorithms. Watch-list software can function with several algorithms and has the ability to turn on or off the algorithm depending on business requirements.

The global AML software market is expected to see an average annual growth of 9% over the next few years and reach over $690 million in 2015, according to a recent report published by the Aite Group.[10]

Anti-money-laundering software comprises several distinct functional areas: transaction monitoring, watch-list screening, customer due diligence (CDD), case management and reporting. This can be used as a suite or each component can also be used separately. To select an effective watch-list solution, companies should begin their process by understanding their current infrastructure. Every financial institution has its own unique mixture of policies, lines of business, business objectives and geographical locations. Each institution also has its own technology strategy and infrastructure. All these factors can help firms better understand their software requirements.

Global AML Software Market Size (U.S.$ millions), 2009 to e2015



Source: Alte Group
Figure 5

Looking Ahead

A false positive is not completely stoppable; however, the likelihood can be reduced to a certain extent. Launderers are using every means available at their disposal to launder the proceeds from their illegal activities. It is a real challenge for financial institutions to identify true hits and false positives. This white paper highlighted the different techniques of name matching and false-positive reduction to help minimize the false-positive count.

Financial institutions will continue to be pressured to screen transactions and customer lists for the likes of terrorists; they should upgrade their OFAC software on a regular basis because the first-generation OFAC software may not have much

Selected AML Software Vendors: A Virtual Long List

AML Suites		Watch-List Specialists	Specialist Technologies
3i Infotech	Ocean Systems	Accuity	AML RightSource
ACI Worldwide	Oracle/Mantas	Attus Technology	Basis Technology
Aquilan	SAS	Fircosoft	Intersoft KK
BAE/Detica Norkom	SunGard	Innovative Systems	KYC360
Cellent Finance Solutions	TCS	Lexis Nexis/Bridger	KYCNet
EastNets	Temenos/ViveLogica	NetBreeze	
Experian	Thomson Reuters/ Northland Solutions	Oracle / Datanomic	Pegasystems
FIS	Tonbeller	Thomson Reuters/ Complinet	Safe Banking Systems
Fiserv	Top Systems		Truth Technologies
Infrasoft	Verafin		
Jack Henry	Wolters Kluwer		
Nice/Actimize			

Source: Celent
Figure 6

advanced detecting behavior. The latest software provides added features for searching, data analyzing, recognizing patterns and profiling, including:

- Rapid verification of client name, address and date of birth using refined matching and disqualification techniques that result in fewer false positives.
- Ablity to identify key information such as account name and payment submitted/scanned date and to maintain log files.
- Identifying ACH and international ACH transactions and the ability to compare all applicable fields against OFAC and other watch lists.
- Creation of "good guys" and "bad guys" (customer) lists to reduce false positives and enable easy reporting of positive matches.
- Generate alerts and reports with transaction details.

There are numerous interdiction software packages that are commercially available. They vary considerably in cost and capabilities (see Figure 6). If your institution feels it needs to invest in software in its attempt to comply with OFAC regulations, OFAC recommends that you speak with an AML SME, or counterparts at other banks, about the systems they have in place and work with an independent third party to assess your organization's needs.

Footnotes

[1] The Office of Foreign Assets Control regulations are issued by the U.S. Department of the Treasury, which administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals against targeted foreign countries, terrorists, international narcotics traffickers and those engaged in activities related to the proliferation of weapons of mass destruction.

[2] Banks have been major targets in laundering operations because they provide a variety of services and instruments, including cashier checks, travelers checks and wire transfers — which can be used to conceal the source of illicit proceeds.

[3] OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, blacklisted countries. It also lists individuals, groups and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Their assets are blocked and U.S. persons are generally prohibited from dealing with them.

[4] This law requires financial institutions to track cash transactions, file reports detailing any suspicious activity and keep records of various financial transactions.

[5] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001.

[6] Such measures are taken to know and understand a customer and related beneficial owner(s), including the identification and verification of their identity.

[7] This applies for higher-risk customers who pose greater money-laundering or terrorist-financing risks and present increased exposure to banks; due diligence policies, procedures and processes should be enhanced as a result.

[8] These are individuals who occupy, or have occupied, prominent public positions, including prominent positions in international organizations, both within and outside Australia (or their close family or associates).

[9] This represents a line in the phonetic file, consisting of a sequence of symbols/letters which is rewritten in another sequence with certain criteria.

[10] The global AML software market is expected to see an average annual growth of 9% over the next few years and reach over $690 million in 2015, according to a recent report published by the Aite Group.

References

- http://www.treasury.gov/resource-center/sanctions/Documents/matrix.pdf.
- http://www.ffiec.gov/bsa_aml_infobase/pages_manual/OLM_113.htm.
- http://bankcrmconsulting.com/forms/BSA_Risk_Analysis_Chart.pdf.
- http://www.worldcompliance.com/Libraries/WhitePapers/OFAC_Compliance_White_paper.sflb.ashx.
- http://www.bankersonline.com/vendor_guru/innovativesystems/comp_is_091806.html.
- http://www.techopedia.com/definition/28041/data-matching.
- http://www.basistech.com/name-indexer.
- http://www.niada.com/PDFs/Publications/OFACGuide.pdf.
- http://homepages.cs.ncl.ac.uk/brian.randell/Genealogy/NameMatching.pdf.
- http://cs.anu.edu.au/techreports/2006/TR-CS-06-02.pdf.
- http://www.waset.org/journals/waset/v1/v1-47.pdf.
- http://www.celent.com/reports/trends-anti-money-laundering-2011.
- http://www.treasury.gov/resource-center/sanctions/CivPen/Pages/civpen-index2.aspx.

About the Author

Rajesh Ramachandran is a Senior Consultant within Cognizant Business Consulting's Banking and Financial Services Practice. He has 15 years of consulting experience in SWIFT, payments, risk and compliance. Rajesh has served several international clients in multiple geographies (Asia/U.S./EMEA). He holds a master's degree in business management with specialization in finance. Rajesh can be reached at Rajesh.Ramachandran3@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 75 development and delivery centers worldwide and approximately 178,600 employees as of March 31, 2014, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

Cognizant

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

© Copyright 2014, Cognizant. All rights reserved. No part of this document may be reproduced, stored in a retrieval system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the express written permission from Cognizant. The information contained herein is subject to change without notice. All other trademarks mentioned herein are the property of their respective owners.