CGI

Experience the commitment®

WHITE PAPER

Sanctions Compliance

Financial institutions need to meet rising sanctions compliance demands without disrupting customer service or incurring inordinate costs. While robust filtering technology is essential to managing compliance, the most cost-effective approach combines intelligent technology, people and processes while fostering self-learning and improvement in all three components. This white paper describes this three-pronged approach designed to help organizations reduce compliance risk and cost, while ensuring customer satisfaction.

March 2016

cgi.com

Introduction

Financial institutions face mounting challenges as they strive to comply with ever-expanding legal requirements for combatting money laundering and terrorist financing. The number of global watch lists and sanctioned activities continue to grow, as does pressure for organizations to extend their screening processes across the entire enterprise. Meanwhile, watch list data can change daily, further complicating the task of keeping up to date and running an efficient screening operation. Consequently, financial institutions are caught between their obligation to prevent illegal transactions and the rising costs of compliance. Each new watch-list requirement increases the compliance burden while potentially slowing transactions and customer service. Neither is good for the bottom line.

Financial institutions can successfully address these challenges with a sanctions compliance approach that integrates its people, processes, and technologies in a program aimed at continuous learning and improvement. In the technology arena, for example, watch list filtering software must have a self-learning capability that enables it to systematically reduce the number of “false positive” alerts. At the same time, the people who evaluate and make the approval decisions should be presented with complete and clear information on each alert; and they should have a workflow that enables them to reach out to others in their organization for guidance and support. These controlled and audited processes will foster collaboration among different departments for swift, effective decision making. Regular testing of technologies, processes, employees, and capabilities will ensure continued improvement as well.

Larger fines and penalties for non-compliance and reputational damage pose significant risks for financial institutions. But so does the rising costs of compliance. An integrated program also should include rigorous, cost-effective controls that satisfy the needs of both regulators and customers.

CGI

The rapid pace of globalization exposes organizations to increasingly greater sanctions risk.

The modern challenge of sanctions compliance

The increasing difficulty of sanctions compliance is highlighted by the growing fines that have been levied against financial institutions in recent years for failing to comply with anti-money laundering (AML) laws and other regulations. Banks have been fined hundreds of millions and even billions of dollars for alleged dealings with black-listed nations and drug kingpins, as well as for helping them launder money and evade sanctions. These banks have seen their net value suffer along with their reputations, while individual corporate executives have been subject to prosecution. As the global fight against money laundering and terrorist funding expands, the obligation to monitor transactions is also falling to large corporations, insurance companies, money services, and other types of businesses. Given the huge reputational risk and penalties faced by these businesses, why do so many still struggle to put in place effective compliance programs?

Several interrelated factors have converged to make sanctions compliance more complex and costly. First, the rapid pace of globalization exposes organizations to increasingly greater sanctions risk. Meanwhile, the number of individuals and entities on global watch lists continues to grow. In addition, sectoral sanctions, such as those targeting Russia's financial and energy sectors and prohibiting certain types of transactions, complicate the task of distinguishing between approved and not-approved transactions. Screening for Politically Exposed Persons (PEPs) also presents financial institutions with subjective decisions about who constitutes a PEP and whether domestic as well as foreign PEPs should be flagged.

AML regulations require companies to screen not just their customers, but also related third parties, such as suppliers and the entities with whom their customers are sending or receiving funds. Enhanced due diligence is also required, depending on the perceived risk of the third party. And all of this is occurring in exploding volumes of global transactions where terrorists and criminals are constantly changing their tactics and identities to avoid detection.

In short, the data haystack is getting larger, while the needles are increasing in number but are getting harder to find.

Sanctions compliance—the task of finding the needles—imposes a variety of costs on financial institutions. Organizations must invest in sophisticated technology that can automatically screen large volumes of transaction data and accurately identify watch-list violators. This is no easy task, given that individuals and entities are often identified (and misidentified) in a multitude of languages, spellings, and formats, each unique to the database or payment instruction where the information resides. Another cost is for the personnel who operate the technology and evaluate flagged transactions to determine whether to approve them.

At the same time, the evaluation process can slow and even disrupt legitimate transactions, causing customer dissatisfaction and loss of business. Organizations can speed decision making by increasing the resources devoted to resolving watch-list alerts, but this is a cost few companies can afford. Some companies have sought to keep transactions and revenue flowing by easing their screening controls at times of operational stress, but this approach has led to severe fines and penalties for non-compliance.

Cost-effective compliance through continuous learning and improvement

How can financial institutions meet the rising demands of sanctions compliance without disrupting customer service or incurring inordinate costs? Stated simply, they need to:

1. Find and halt every transaction involving watch-list people and entities

2. Minimize the costs and transactional friction associated with this activity

Implementing the right filtering software to automatically screen the transaction data and identify potential sanctioned entities is absolutely crucial to a cost-effective compliance program; but so is putting in place the right people and processes.

Each of these three components—technology, people, and processes—complements and reinforces the others. Equally important, each area must be implemented and maintained with an eye toward continuous learning and improvement. That is because the demands of sanctions compliance are always growing:

- Governments are creating new watch lists and sanctions, as well as raising the bar in the sophistication of matches required
- Terrorists and organized criminals are devising new tactics for avoiding detection, requiring tools and strategies that can keep pace
- Innovative technologies are creating new ways of making payments and transacting business

CGI's experience providing market-leading compliance technology and services has shown that the most successful organizations facilitate, nurture, and support an ability to adapt, learn, and improve their compliance capabilities in all three areas.

Following are the best practices we have observed within each of the technology, people, and process dimensions for achieving a comprehensive, balanced approach to sanctions compliance.

Implementing the right filtering software to automatically screen the transaction data and identify potential sanctioned entities is absolutely crucial for a cost-effective program.

Technology: Rigorous software filtering

Robust filtering software can reduce significantly the time and costs required for sanctions compliance by analyzing all transactions and automatically alerting companies to potential matches against watch lists. Transactions that generate alerts are then reviewed by payments operations and compliance experts who make the final determination of whether a transaction should be approved or denied. Figure 1 shows the four possible outcomes when transactions are screened by filtering software:

1. True Negatives (compliant transactions that are automatically approved)
2. True Positives (non-compliant transaction that are held up for review)
3. False Negatives (non-compliant transactions that are automatically but mistakenly approved)
4. False Positives (compliant transactions that are mistakenly held up for review)

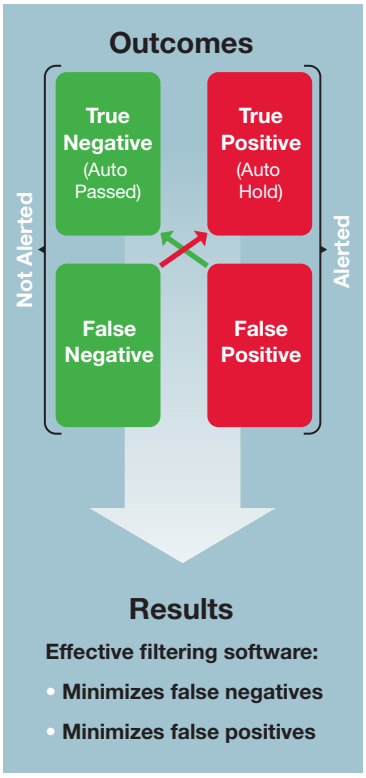
Companies will want to implement and calibrate filtering software to flag every watch-list transaction. That is, they do not want their software to mistakenly approve sanctioned entities (False Negatives), which could lead to fines and penalties.

However, companies will also want to reduce the number of legitimate transactions that are flagged as possible sanctioned entities (False Positives). Although an effective review process will eventually identify false positives, reviewing large numbers of such transactions carries numerous costs and risks. For example, a large volume of false positives can lead to:

- Poor customer experience for the legitimate transactions that are flagged and stuck in review
- Operator fatigue that causes real-hits to be mistakenly approved
- Increasing costs in terms of time and resources devoted to reviewing alerts

Financial institutions should look for several important properties and capabilities in their filtering software. At a simple level, the software should be able to screen new customers, as well as retroactively screen existing customers, when new people and entities are added to the watch lists or when customer data changes. It should also be able to screen financial messages in real-time and meet the throughput, resilience, and recovery requirements of the mission-critical payments environment. For powerful, effective screening, the software should also employ:

- "Fuzzy matching" techniques, which are sophisticated algorithms for identifying sanctioned people and entities, despite accidental or deliberate misspellings that obscure their true identity
- Native language capabilities to scan and interpret all foreign alphabets and scripts and transliterations
- Know Your Customer capabilities to provide identity verification and risk assessment during customer onboarding
- Algorithms that provide rapid, real-time scanning of transaction data
- Configurable scan settings and rules that enable fine-tuning to improve accuracy and achieve the organization's unique risk goals, as well as automating decisions based on the context of the hit and the transaction



Finally, one of the most important requirements for any filtering software is the capability for self-learning. Software that has a self-learning capability generates a feedback loop that improves the filter by automatically discovering the good guys, thereby reducing the number of false positives and streamlining the review process. The self-learning capability has been shown to reduce the number of false positive by up to 50% without reducing filtering accuracy or narrowing the net.

People: Trained and skilled professionals

Strict compliance depends on skilled professionals who use the compliance technology and evaluate each alert generated. The process for reviewing alerts requires different levels of expertise ranging from following procedures at first-level triage to in-depth knowledge of multiple sanction regimes at the highest levels. Each alert must be reviewed quickly and assigned an accurate risk score to speed transactions and minimize costs while also assuring full compliance. Finding and retaining the right people for this critical function requires:

- **Effective hiring procedures** that identify people with skills such as analytical thinking and a questioning mindset, as well as an ability to work collaboratively with colleagues across the organization when deciding whether to approve a transaction. Prospective employees must be able to grasp complex processes and spot hard-to-see relationships about people and groups. New sanctions programs, such as sectoral sanctions targeting Russia, may also require expertise in new languages.
- **Ongoing training of employees** to ensure they effectively apply the requirements of new sanctions and watch-list programs. The training should be standardized and provided annually, if not more often, to refresh skills and knowledge. Organizations should also take advantage of industry forums and other events which offer opportunities to exchange ideas, keep abreast of changing terrorist and criminal tactics, and learn best practices from other industry experts. For example, the Association of Certified Fraud Examiners (ACFE) and the Association of Certified Anti-Money Laundering Specialists (ACAMS) provide internationally recognized training and certification courses.
- **Change management support** to ensure that the organization understands and leverages new technologies and processes to strengthen and streamline compliance activities. Interdependencies among an organization's culture, capacity, processes, and behaviors can influence the results of planned changes. Effective change management will facilitate integration of the changes across all dimensions of the enterprise.
- **Career development and succession planning** to create a strong and enthusiastic cadre of compliance professionals. Companies should identify the critical roles on their compliance team and define the required qualifications and skills. With this information, they can put in place a program for professional development and establish desirable career paths within the organization. Succession planning will keep key positions filled.

Taken together, these activities will minimize compliance risk by ensuring that the organization maintains the high-quality human capital necessary to meet the challenges of today's rapidly changing compliance landscape.

Processes: Efficiency, collaboration, and learning

In addition to creating effective processes for hiring, training, and retaining compliance professionals, financial institutions should also develop and implement processes that facilitate swift, thorough, and efficient resolution of alerts generated by the filtering software. Each organization will develop processes reflecting its unique institutional culture and risk profile, but every program should include processes that:

- Standardize the procedures for triaging alerts
- Facilitate collaboration among cross-functional teams in areas such as payments operations, compliance, and customer facing departments
- Support participation in industry forums, both domestically and globally
- Support partnership with other industries
- Standardize the procedures for responding quickly and mitigating the impact following a compliance violation

Financial institutions should also develop processes to take full advantage of the capabilities offered by their filtering software. For example, "stripping" technology will alert a financial institution when there is a high probability that a transaction containing stripped data has been resubmitted for payment.

Testing of software, people, and processes is essential to maintaining a high-quality compliance program. For example, organizations should conduct tests whenever their technology is upgraded or changes are made to processes and procedures. The addition of new sanctions, countries, or entities to the watch lists should also prompt testing to ensure that software filters are recalibrated, people are educated and trained, and processes are adapted to new compliance requirements. Financial institutions can outsource testing to a third-party that can provide independent, automated testing of filtering software.

As mentioned earlier, each organization will implement processes reflecting its unique culture and goals, but the important point is that the processes should be developed, analyzed, and tested with conscious aforethought, as opposed to arising in an ad hoc manner.

Conclusion

Financial institutions recognize the need for stronger compliance controls, but they do not have unlimited budgets nor human capital resources. Robust filtering technology that automatically scans large volumes of transaction data is essential to managing compliance in today's complex financial markets, but the most cost-effective approach to compliance coordinates intelligent technology, people and processes. Key to success is building in mechanisms that foster self-learning and improvement in all three components. This not only allows organizations to calibrate their compliance program to achieve the highest levels of effectiveness and efficiency, but it also enables them to keep pace with a constantly changing compliance landscape. With a comprehensive approach that creates a foundation of continuous learning and improvement for people, processes, and technology organizations can reduce both compliance risk and compliance costs, while ensuring that legitimate transactions flow smoothly and customer satisfaction remains high.

Why CGI

CGI has partnered with commercial banks, central banks, financial services firms, payments bureaus, and other organizations to help them build enterprise-wide compliance programs that coordinate people, processes, and technology to achieve maximum efficiency and effectiveness. Our clients using this approach have strengthened compliance capabilities while simultaneously streamlining processes for automated scanning, reviewing, and approving transactions. Equally important, by facilitating continuous learning and improvement, this approach enables clients to regularly fine-tune their capabilities and adjust their compliance regime to meet changing requirements and mitigate evolving risks.

CGI's HotScan filtering technology is installed in 30 countries and filters 64% of the total value of currencies traded globally. Moreover, HotScan was ranked No. 1 for advanced technology in Celent's report, "Evaluating the Vendors of Watchlist and Sanctions Solutions."[1] We are trusted by some of the world's largest central banks and have been awarded the SWIFT Alliance Add-on Label since 2005. The HotScan Intelligent Self Learning module, which can be implemented alongside any scanning solution, can reduce false positives by up to 50%, lowering the number of payments requiring manual intervention without narrowing the net.

The Rising Cost of "Payment Stripping'

As regulators grow increasingly strict in enforcing laws regarding anti-money laundering and terrorist financing, the practice of "payment stripping" can put unprotected financial institutions at risk.

In a payment stripping scheme, material information is removed from a wire transfer to hide the identity of a sanctioned individual, entity, or country involved in paying or receiving funds. The removal of identifying information might be done by a rogue business office or employee, perhaps working in a remote location with little oversight. For example, after submitting a wire transfer that is rejected because a sanctioned party is involved, the business office will remove information to conceal the involvement of sanctioned party, thus allowing the illegal transaction to proceed.

Banks facilitating or failing to prevent payment stripping have forfeited hundreds of millions of dollars in settlements with U.S. authorities. To exercise proper due diligence, financial institutions should implement both employee training and filtering software to flag and prevent payment stripping.

[1] Neil Katkov, PhD, "Evaluating the Vendors of Watchlist and Sanctions Solutions," Celent, April 18, 2013

cgi.com

About CGI

Founded in 1976, CGI is one of the largest IT and business process services providers in the world. We combine innovative services and solutions with a disciplined delivery approach that has resulted in an industry-leading track record of delivering 95% of projects on time and within budget. Our global reach, combined with our proximity model of serving clients from 400 locations worldwide, provides the scale and immediacy required to rapidly respond to client needs. Our business consulting, systems integration and managed services help clients leverage current investments while adopting technology and business strategies that achieve top and bottom line results. As a demonstration of our commitment, our client satisfaction score consistently measures 9 out of 10.

For more information, visit **cgi.com** or email **banking.solutions@cgi.com.**