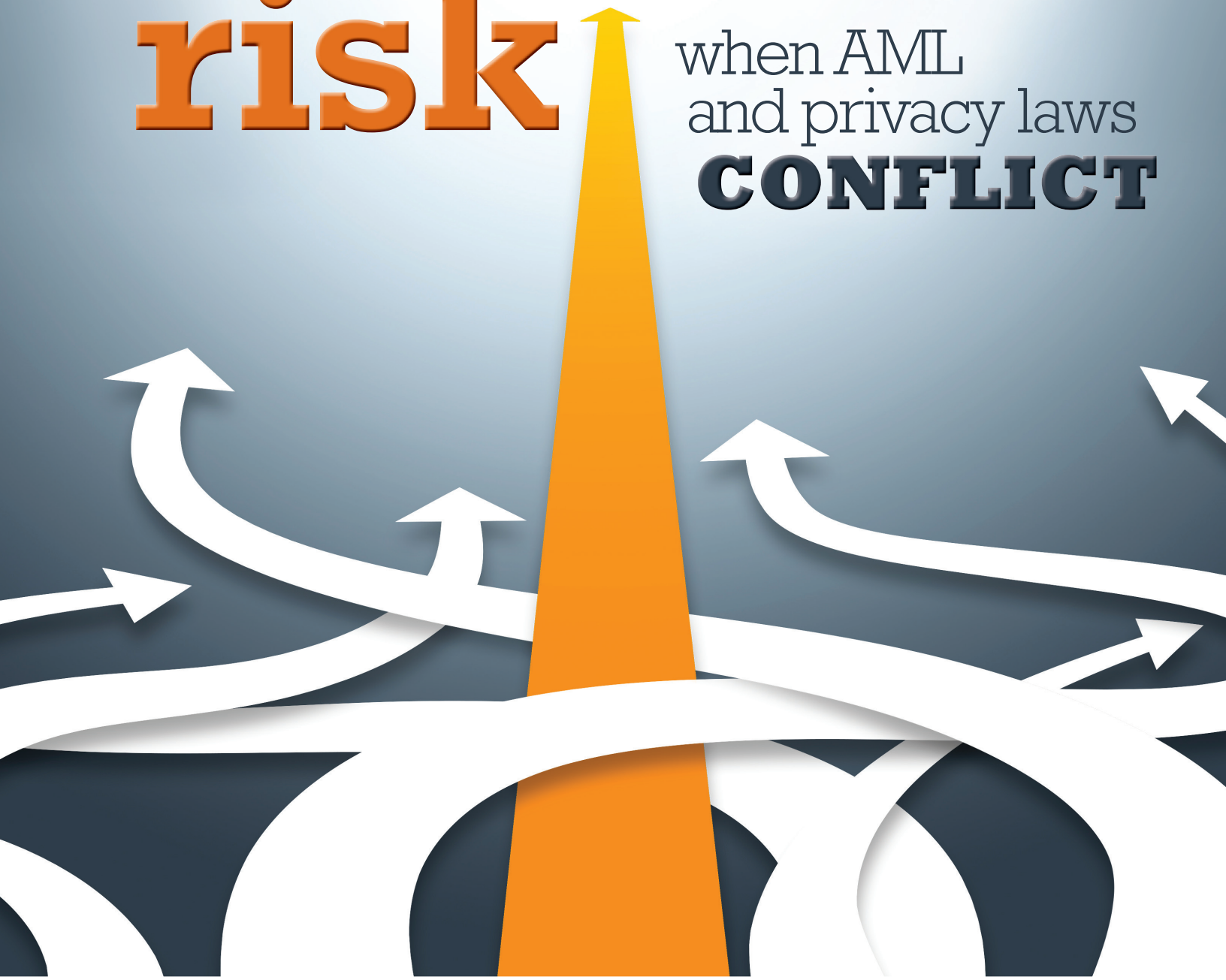
ACAMS® TODAY

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

Achieving enterprise risk when AML and privacy laws CONFLICT



SBS SAFE BANKING SYSTEMS

Reprinted with permission from the September–November 2016, Vol. 15 No. 4 issue of *ACAMS Today* magazine, a publication of the Association of Certified Anti-Money Laundering Specialists

ACAMS® | Advancing Financial Crime Professionals Worldwide®

Enterprise risk is a familiar but challenging topic within the anti-money laundering (AML) and compliance community. In order to deliver value to customers and shareholders, an institution must understand and manage the risks it faces across the entire organization. Risks are inherent to any business and are often categorized as strategic, operational, compliance and financial/reporting. An enterprise view of risk captures all the elements of business and how they intersect to deliver value and drive success. It also identifies potential events that may affect an institution so that the associated risks can be properly managed. Identifying and managing risk is especially important in today's heightened regulatory environment where Bank Secrecy Act/anti-money laundering (BSA/AML) programs have come under intense scrutiny resulting in some very high profile enforcement actions and fines in the last few years.

The challenges ahead

Financial and other regulated institutions face tremendous challenges when trying to view risk across the enterprise. Inconsistent data quality, business silos, disparate systems and massive amounts of changing information make it difficult for organizations to easily gather the intelligence they need to identify, assess and manage enterprise risk. Add to that mix, the myriad laws governing transnational financial data that comes with globalization. For multinational enterprises, satisfying regulatory requirements while meeting different jurisdictional privacy laws further complicates their ability to achieve an enterprise view of risk.

In a SWIFT Institute working paper titled "Multinational Banking and Conflicts Among U.S.-EU AML/CTF Compliance and Privacy Law: Operational and Political Views in Context," Dr. Michelle Frasher, Ph.D., indicates that "financial data is both commercial and a source of intelligence and is governed by two often opposing legal regimes."[1] Published July 1, 2016, the paper analyzes U.S. and EU anti-money laundering/counter-terrorist financing (AML/CTF) and data protection laws and identifies 19 compliance areas that pose a challenge to multinationals as they integrate privacy into their AML/CTF operations. These include compliance-related activities with the potential for regulatory and/or reputational risk such as:

- Data requests by local authorities
- The collection of sensitive data
- Transfers involving politically exposed persons, family members and associates
- Vendor compliance with U.S.-EU Privacy Shield
- Prohibition of the use of know your customer (KYC) data on EU data subjects for commercial purposes

Dr. Frasher points out how the EU's Fourth AML Directive "promotes enterprise-wide compliance programs with data protection across the group," while U.S. law "restricts data due to confidentiality concerns and does not require privacy in compliance programs."[2] Thus, in a globalized world the concept of an enterprise view of risk becomes a greater challenge when multijurisdictional privacy standards must be upheld.

Many countries have laws that make it illegal for entities—such as banks with foreign branches—to share certain types of information across borders. This begs the question: Are regulatory expectations realistic and is an enterprise view of risk even possible for global banks?

Privacy issues

The dichotomy of AML and privacy is a common conundrum for global institutions. When operating in foreign markets, failure to understand local data and regulatory requirements increases the risk and potential for large fines. Whether an organization chooses to implement a consolidated BSA/AML program or follow one in which some or all compliance controls are managed solely within affiliates, subsidiaries or business lines, regulators (especially those in the U.S.) continue to demand full transparency despite privacy laws and the cultural differences of other countries. The Federal Financial Institutions Examination Council's BSA/AML Examination Manual provides very specific instructions to examiners for assessing the adequacy of a U.S. bank's systems to manage the risks of its foreign branches and offices. It also provides specific instructions for assessing a bank's capability to implement effective monitoring and reporting systems. Examiners understand that privacy laws in a foreign jurisdiction may prevent a branch or subsidiary from sharing information with its U.S. parent. Nevertheless, they expect that compliance oversight of foreign branches and subsidiaries will ensure that adequate policies, procedures and processes are in place to protect against money laundering and terrorist financing risks.

The dichotomy of AML and privacy is a common conundrum for global institutions

Although U.S. federal, state and local governments have implemented laws to protect many aspects of Americans' privacy, some areas of processing personal data remain unregulated. The Gramm-Leach-Bliley Act provides for the protection of personal financial information such as name and account number. However, there is limited regulation over the collection of information. By contrast, the EU views privacy as a human right and therefore regulates the collection and handling of personally identifiable information. The "European Union Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data" (EU Directive) provides a framework for data privacy across Europe. Still, each EU member state must enact its own local privacy law

[1] Dr. Michelle Frasher, Ph.D with Brian Agnew, MPP, "Multinational Banking and Conflicts Among US-EU AML/CTF Compliance and Privacy Law: Operational and Political Views in Context," SWIFT Institute Working Paper No. 2014-008, July 1, 2016, http://www.swiftinstitute.org/wp-content/uploads/2016/07/SIWP-2014-008-Conflicts_US_EU_AML_CTF_FINAL-1.pdf

[2] Ibid.

based on the directive, so laws vary among EU members. This inconsistency makes it difficult for a global institution to gather and process information centrally in order to assess and manage risk across the enterprise. Cross-border privacy issues have also caused compliance and legal conflicts of law. In Asia-Pacific, financial institutions must deal with regulators in different jurisdictions that are completely autonomous. There is no framework like the EU Directive to provide guidance on privacy laws, resulting in little or no overlap and regulations which are not always documented in English.

Obtaining a workable balance

The issues posed by the conflict of data protection and bank secrecy laws can only be resolved if harmony exists between regulatory and data requirements. In the absence of harmony, both banks and regulators must strive to address these issues. While the Federal Trade Commission and Department of Commerce have initiated efforts to develop a uniform privacy policy for the U.S., it is expected to take several years to implement. Therefore, it is incumbent on banks to build privacy requirements up front when designing global operating models and information technology systems. By embedding privacy into the design of everything that comes in contact with personal information, the organization creates a default mode of operation. On the business side, consent clauses in customer agreements will allow the use of customer data to support AML surveillance. On the technology side, strict user permissions ensure data is accessed and viewed on a needs-to-know basis. While compliance departments need systems that optimize operational efficiencies, conforming to privacy standards is also required. This brings the management of personal information and its risks into the broader, strategic enterprise risk management environment, which is the ultimate goal.

Across the EU and elsewhere, we are beginning to see some developments moving in the right direction. In January 2016, SWIFT announced that over 2,000 financial institutions in over 200 countries and territories had signed up for their KYC Registry.[3] This centralized repository maintains a standardized set of KYC information for correspondent banks, fund distributors and custodians. Standardized, community-driven solutions such as this can move us closer to information sharing and a more workable balance between privacy and AML requirements.

In October 2014, the Financial Action Task Force issued its guidance on "Transparency and Beneficial Ownership." To facilitate a practical level of international cooperation, the guidance included specific requirements documented in Recommendations 24 and 25.[4] Further measures on beneficial ownership were taken in 2016 when the U.S. Department of the Treasury's Financial Crimes Enforcement Network published a final rule on customer due diligence. Often called the "fifth pillar" of BSA/AML, financial institutions are now required to identify and verify the identity of beneficial owners of a legal entity at the time the legal entity opens a new account, as well as develop risk profiles and conduct ongoing monitoring of customers.

It is encouraging to see that some privacy laws are being reassessed in certain EU jurisdictions because governments, institutions and law enforcement are recognizing that they are an impediment to identifying money laundering activities. A draft law drawn up by Germany's justice ministry allows authorities to confiscate goods suspected of being purchased with ill-gotten funds and reverses the burden of proof by forcing people under investigation to prove assets were acquired legally.

This law could be a milestone in curtailing mafia activities in Germany, which is well-known as a haven for mafia investment. It could also be a big win for the good guys if current privacy laws are amended.

Achieving enterprise risk

Is an enterprise view of risk possible in the current environment? The answer is yes. But, it is slow going and requires cooperation among jurisdictions and governments as well as regulations in harmony with privacy laws. In addition, it requires technology solutions capable of handling cross-border risk and with flexible delivery options (e.g., hosted, onsite and hybrid deployments) to accommodate jurisdictional differences.

To achieve a broad view of risk, institutions should look for solutions with robust features and functionality such as:

- Scalability to handle massive stores of customer and reference data
- Ongoing surveillance to capture constantly changing information
- Consistency and standardization across lines of business to break down silos and facilitate sharing of information
- Cutting-edge technology that employs machine learning, artificial intelligence, data visualization, rotational alignment in name matching to facilitate entity resolution and comprehensive alert prioritization and management
- Advanced link analysis tools that can identify relationships across jurisdictions without violating local privacy laws

Conclusion

As long as AML requirements and privacy laws remain pitted against each other, the ability to proactively identify and manage risk across the enterprise will continue to be a challenge especially for global institutions. Fortunately, cooperation among governments, law enforcement, regulators and other entities and more powerful technology are helping to bring an enterprise view of risk within grasp.

Carol Stabile, CAMS, senior business manager, Safe Banking Systems, Mineola, NY, USA, carol.stabile@safe-banking.com

[3] "SWIFT's KYC Registry surpasses 2,000 financial institutions," January 19, 2016, https://www.swift.com/insights/press-releases/swift_s-kyc-registry-surpasses-2_000-financial-institutions

[4] FATF Guidance, "Transparency And Beneficial Ownership," October 2014, http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-transparency-beneficial-ownership.pdf