protiviti®

Face the Future with Confidence

The Challenges of Managing a Global AML Program

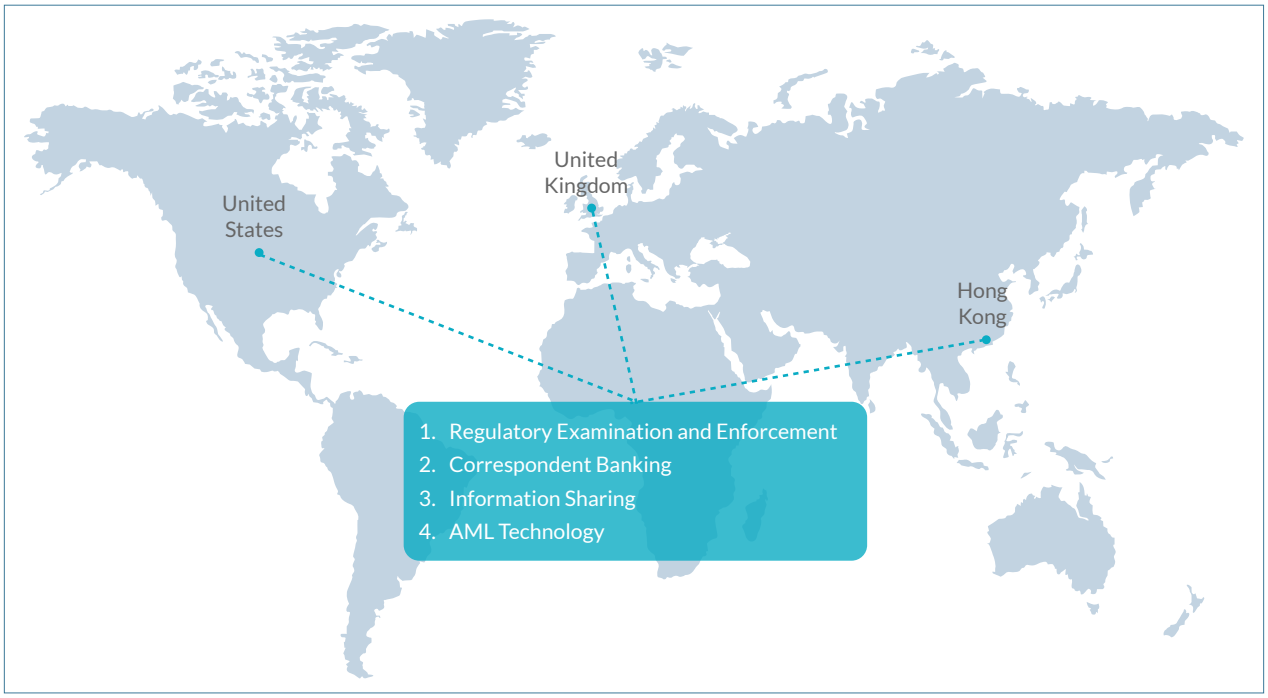
Distinctions Across the United States, the United Kingdom and Hong Kong

Internal Audit, Risk, Business & Technology Consulting

Executive Summary

The three global financial centers — New York, London and Hong Kong — may vary considerably in terms of their strategic focus, but there is a high degree of commonality to the principles of regulation for depository institutions across all three jurisdictions.

Four Areas of Difference in AML Requirements



But as any seasoned compliance officer will tell you, common principles don't necessarily mean common implementation or enforcement. What may seem like small nuances among the regulatory regimes of different jurisdictions can be minefields for an institution trying to establish and maintain an effective, global compliance program. This is certainly true in the case of compliance with anti-money laundering (AML) regulations.

A number of nuances exist in the way AML requirements apply across the United States, the United Kingdom and Hong Kong. This paper examines four areas: regulatory examination and enforcement, correspondent banking, information sharing, and AML technology. It also considers the implications of these differences for financial institutions seeking to implement a global AML program and provides advice on how firms can more efficiently implement a compliant AML program that is cost-effective and provides more value to the business.

Regulatory Examination and Enforcement

The main regulatory bodies for global depository institutions operating in the United States, the United Kingdom and Hong Kong are summarized in the following table.[1]

Key Banking Regulatory Roles	United States	United Kingdom	Hong Kong
Promulgating Rules and Regulations	FinCEN	FCA/PRA	HKMA
Issuing Guidance	FFIEC	JMLSG	HKMA
Receiving SARs/STRs	FinCEN	NCA	JFIU
Examination	FRB, OCC, FDIC, NCUA,[2] state banking regulators	FCA	HKMA
Enforcement Actions	FinCEN, FRB, OCC, FDIC, NCUA, DOJ, state banking regulators	FCA	HKMA
Fines	FinCEN, FRB, OCC, FDIC, NCUA, DOJ, state banking regulators	FCA	HKMA

Regulators in each country have different examination approaches and often change the areas of focus for AML compliance reviews. Accordingly, compliance teams need to be mindful of these factors in order to support the organization adequately, as well as deliver value and benefits to the business.

United States

Regulators in the United States apply a generally consistent and comprehensive level of examination regardless of the size and complexity of a bank and take a detailed, requirements-based approach to examinations. Of the three jurisdictions, the United States is unique in that it has an interagency regulatory body, the Federal Financial Institutions Examination Council (FFIEC), which provides an overarching AML examination framework used by all depository institution regulators, both federal and state.

Examinations are undertaken by a firm's designated primary regulator using the detailed guidance set forth in the *FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual*. Additionally, to date, the United States has taken the most strict and punitive approach to enforcement, going beyond just requiring corrective actions to include large financial penalties, some of which have been imposed directly on AML compliance officers in the asset management and money transmitter industry segments.

[1] Please see Appendix A for full names and descriptions of referenced regulatory bodies.

[2] The National Credit Union Administration (NCUA) charters and supervises credit unions. Although credit unions do not have international offices, their products (e.g., ATM cards) can be used internationally.

Hong Kong and the United Kingdom

In Hong Kong and the United Kingdom, the regulatory landscape is slightly less complicated, and there is no equivalent body to the FFIEC. The regulators that supervise financial institutions — the Hong Kong Monetary Authority (HKMA) and the United Kingdom's Financial Conduct Authority (FCA), respectively — have responsibility both for determining what is required under the rules and for examining banks to ensure that the rules have been properly implemented.

It is worth noting that the wider AML regime in the European Union (EU) is being aligned and standardized through the EU's Anti-Money Laundering Directives. The Fourth Anti-Money Laundering Directive came into effect on June 25, 2015, and member states have two years to implement changes to their respective legislation; this will also be the case for the United Kingdom.

There is no overarching equivalent to the FFIEC's manual for each regulator to follow. Regulators, therefore, tend to tailor their approach to examinations according to particular circumstances, and the examinations are relatively more risk-based. Guidance documents are in place that set out regulatory expectations for the AML standards, however.

To counterbalance the relative lack of specificity on examination procedures, regulators in the United Kingdom and Hong Kong are very active in alerting financial institutions to what they can expect from an examination. Enforcement actions by both regulators are usually less severe in comparison to those in the United States, and while the value of levied financial fines has significantly increased in recent years, the fines remain significantly smaller than those in the United States.

Examination Expectations

U.S. Regulatory Bodies
• Publish manuals utilized by examiners for carrying out Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and Office of Foreign Assets Control (OFAC) examinations for depository institutions (FFIEC).
• Publicize findings from examinations and enforcement actions and orders taken against institutions through regulators (Board of Governors of the FRS, FDIC, OCC, and NCUA).
• Publish advisories, bulletins and fact sheets on AML-related trends and emerging AML topics.
The Financial Conduct Authority
• Publishes plans for future thematic reviews.
• Publishes feedback from industry consultations, key observations and findings from its thematic reviews, or summaries of main control failings following regulatory enforcement actions. These methods provide market participants with a detailed feedback loop on current regulatory considerations.
• Sets expectations as to how examinations will be conducted, identifies key findings and publicizes enforcement actions taken through the following strategies: — A Skilled Person Review performed on behalf of the FCA through powers under Section 166 of the Financial Services and Markets Act. — Systematic Anti-Money Laundering Programme (SAMLP) assessments and intrusive testing reviews of a firm's AML-control framework.

The Hong Kong Monetary Authority

- Provides statistics on the number and type of examinations, including the number of Tier 1, Tier 2 and thematic reviews.
- Publicizes the stance on enforcement actions. In a recent briefing, the HKMA said that although no penalties have yet been issued to banks under the new AML rules, more than one bank was under investigation, and penalties are being considered.[3] The agency also indicated that it would return to a four-year period for examinations.
- Highlights key areas for attention during examinations, including recent communications related to the following:
  - Not only should Suspicious Activity Reports (SARs) be filed when suspicious activity is found, but corresponding action should be taken to improve the AML program (e.g., tuning AML technology) to respond to risks identified by SARs.
  - Institutions should also be able to demonstrate that risks are owned and understood by the first line. The appropriate "tone at the middle" should be set regarding identifying and mitigating AML risks to support the "tone at the top" being set by the board and senior management. In addition, the first line should take appropriate action to respond to identified money laundering risks (e.g., taking actions on customer accounts).
  - Reviews of management compensation and promotions will be performed to ensure that individuals are appropriately incentivized to manage money laundering risk. The HKMA will seek to understand whether individuals are compensated in ways that balance goals of growing revenues and profits with an eye on management of money laundering risks.

With the help of existing overarching global guidance provided through the intergovernmental Financial Action Task Force (FATF), a number of financial regulators have taken a proactive approach in close cross-regional collaboration and enforcement activity since 2008. (One example of recent joint investigations and enforcement activities is a joint investigation by the United States and the United Kingdom of a large multinational U.K. bank.)

This strategy impacts financial institutions as regulators undertake joint enforcement activity. An institution can find itself subject to the same inquiries in multiple jurisdictions at the same time, a circumstance that was uncommon until recently. This shift in regulatory approach highlights the need for superior compliance teams to be aligned and connected regionally as well as globally.

Point of View — Regulatory Examination and Enforcement

While the FFIEC provides an overarching structure for AML examinations, this does not necessarily result in a consistent application of rules. In contrast, the less complicated regulatory environments in the United Kingdom and in Hong Kong free the HKMA and the FCA to tailor their approaches to examination according to circumstance.

Financial institutions operating across these three global locations should be aware of the varying approaches each respective regulator applies (i.e., an approach that is more rule adherence-based in the United States versus a more principles-based approach in the United Kingdom and Hong Kong).

As a result of these differences, firms should carefully consider how their regulatory liaison teams are organized. For example, they may consider having local teams track developments in each market, understand the developments in the context of AML rules and regulations in the location, and craft responses to regulators appropriately.

In addition, financial institutions should consider having teams that provide oversight at regional or global levels to check that messages are reviewed to ensure regulators receive consistent information. Other supporting tools, such as shared-reporting AML data sources and standardized templates by which responses are crafted, may also be helpful to guarantee that different teams share accurate and up-to-date information.

[3] "Regulatory Update on AML/CFT, Putting risk-based in AML — The Road Ahead," by Stewart McGlynn, September 25, 2015: www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/aml-cft/HKIB_Speech.pdf.

Correspondent Banking

Correspondent banking provides a good example of the challenges facing banks that operate globally. Correspondent banks, or correspondents, are financial institutions that provide financial services to other domestic or foreign banks known as respondents. Respondents and their customers can thus take advantage of the existing international network of the correspondent bank without having to develop their own. While there is common recognition of the risks posed and all three jurisdictions adopt Financial Action Task Force[4] (FATF) principles and the Wolfsberg Principles,[5] significant differences exist in definition and in implementation.

The definition and scope of what constitutes correspondent banking services differs from jurisdiction to jurisdiction, as shown in the chart below. Often, "correspondent banking" is used as a synonym for "correspondent clearing," but the distinction between these two terms is important.

Correspondent clearing, typically viewed as the riskiest of correspondent banking activities, involves the clearing or settlement on behalf of customers of a respondent — customers about whom the institution may have little knowledge because they may have no direct relationship with the financial institution providing the service. The risk of this activity is even more pronounced when the providing institution clears or settles transactions for "nested" relationships (i.e., downstream relationships, such as banks and money services businesses, of the respondent bank).

Definitional Differences

Correspondent Accounts: United States

The USA PATRIOT Act defines a correspondent account broadly to include "any account established for a foreign financial institution (bank, broker-dealer, securities broker-dealer, futures commission merchant, commodities broker, mutual fund, money transmitter or currency exchanger) to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution," which involves a formal relationship to provide services. This includes accounts with non-U.S. affiliates of the correspondent.

Correspondent Banking: United Kingdom and Hong Kong

In the United Kingdom and Hong Kong, AML rules apply to correspondent banking. While there is no significant difference in the type of activity covered there compared to in the United States, the definition of correspondent banking is restricted to just banks, with no equivalent specific in-depth guidance for nonbanks in the United Kingdom and Hong Kong. In the United Kingdom, correspondent banking activities are defined by the Joint Money Laundering Steering Group (JMLSG) and the FCA specifically to include exchanging methods of authenticating instructions — e.g., by exchanging SWIFT (Society for Worldwide Interbank Financial Telecommunication) keys.

Another definitional difference is that both United States and Hong Kong guidance make specific arrangements for domestic correspondent relationships, whereas the U.K. guidance does not distinguish between different domestic and international correspondent requirements. This creates further organizational and operational challenges for institutions.

[4] The FATF is an independent intergovernmental organization that develops policies to manage money laundering, terrorist financing and financing of proliferation of weapons of mass destruction risks. FATF Recommendation 13 includes guidance on due diligence that should be performed for cross-border correspondent banking relationships.

[5] The Wolfsberg Principles are a set of guidance documents formulated by members of the Wolfsberg Group on the establishment and maintenance of foreign correspondent banking relationships. (The Wolfsberg Group consists of 13 global banks whose aim is to develop frameworks and guidance for managing financial crime risks.) The principles are designed to help manage the risk of these types of relationships and prevent the use of Wolfsberg Group member operations by criminals.

Record-Keeping Requirements

A certification process exists in the United States through which correspondent banks obtain due diligence information from respondent banks in order to ensure compliance with the USA PATRIOT Act's[6] record-keeping requirements.

Supporting controls need to capture all regulatory requirements, while also being cost-efficient and value-adding to support the respective business. In addition, these controls should be built with an eye toward the future to ensure sustainability of the operating model.

— Suneet Gorawara, Managing Director in Protiviti's Risk & Compliance Practice, Hong Kong

U.S.-based correspondents must maintain records identifying the foreign bank's ownership structure and the name and contact information of a person located in the United States who has agreed to be the principal agent. This policy helps ensure that correspondent relationships are not opened with foreign shell banks.[7]

There is no equivalent of this record-keeping and certification process in Hong Kong or the United Kingdom. While correspondent banks in those locations are subject to the same prohibitions on shell banks as in the United States, no explicit certification requirements exist. However, U.K. regulators expect correspondent banks to ensure that their respondents are neither shell banks nor offering services to shell banks. This requirement is usually fulfilled through the customer due diligence process on respondents, including site visits for higher-risk relationships. Large U.S. and U.K.-based correspondent banks have now extended these U.S. and U.K.-driven certification requirements globally across all jurisdictions where they operate.

Enhanced Due Diligence (EDD) Requirements

All three jurisdictions require correspondent banks to take the risks associated with correspondent relationships into consideration when deciding whether to apply enhanced due diligence in the form of more thorough assessment of a customer's profile and exposure to money laundering risk. However, on top of that, the United States and the United Kingdom have more prescriptive requirements in certain areas. For example:

- The United States specifically requires that EDD be performed for offshore-licensed banks, banks licensed in jurisdictions that are noncooperative with FATF, or banks designated as warranting special measures.[8]
- The U.K. correspondents are required by Regulation 14(3) of the Money Laundering Regulations of 2007 to perform EDD on respondents from non-European Economic Area (EEA) states, and should consider conducting EDD on those respondents identified to pose increased money laundering risks.

Hong Kong is less prescriptive, indicating only that EDD will be required if the respondent is incorporated in a jurisdiction that insufficiently applies FATF recommendations.

[6] The USA PATRIOT Act was signed into law in 2001 to deter and punish terrorist acts by enhancing law enforcement tools for detecting and reporting money laundering and financing of terrorism.

[7] A shell bank has no physical presence in any country and is not a regulated affiliate of the correspondent bank to which it is a respondent. Correspondent banks are prohibited from maintaining accounts for foreign shell banks, either directly or as a nested relationship in all three jurisdictions.

[8] Section 312 of the USA PATRIOT Act: www.fincen.gov/statutes_regs/frn/pdf/31_CFR_Part_103_312_EDD_Rule.pdf.

All three jurisdictions require that firms recognize payable-through accounts (PTA),[9] which expose correspondent banks to a heightened risk of money laundering. However, U.S. regulators go further by specifying under Section 312 of the USA PATRIOT Act that special due diligence be performed. This means obtaining and considering information about any person who has authority to direct transactions through the PTA (including the source of funds and beneficial owners).

In Hong Kong, however, the HKMA only expects that PTAs be identified and that assurance be obtained from the respondent bank that it has verified and continuously monitors underlying customers who have direct access. Again, the guidance in the United Kingdom is principles-based and expects that when a respondent's customers have direct access to a PTA, the respondent has conducted sufficient due diligence on the underlying customer and is able to share due diligence information on request.

Finally, nested or downstream correspondent banking relationships also carry additional EDD requirements. In the United States, when the need to perform EDD is established, the correspondent bank must establish the existence of nested relationships and obtain relevant information to assess and mitigate the risk. This information must include the identity of the nested relationship itself, unless the correspondent bank can demonstrate that it is inappropriate to reveal the information.

In Hong Kong and the United Kingdom, the rules are more principles-based and put the onus on the correspondent bank to collect sufficient information about the respondent to enable it to understand fully the nature of the respondent's business.

Extraterritorial Application of Correspondent Banking Requirements and Restrictions

Foreign banks without any physical presence in the United States are also subject to regulatory risk if they maintain correspondent relationships with U.S.-based banks. Section 319 of the USA PATRIOT Act allows federal authorities to seize money from the foreign bank's correspondent account if they can convince a judge that the money deposited overseas at the bank was obtained illicitly.

The United States may also, under Section 311 of the USA PATRIOT Act, prohibit the opening or continued operation of the account. These measures were established following specific investigative evidence following the September 11, 2001, terrorist attacks, while other countries follow more general regulatory best-practices guidance.

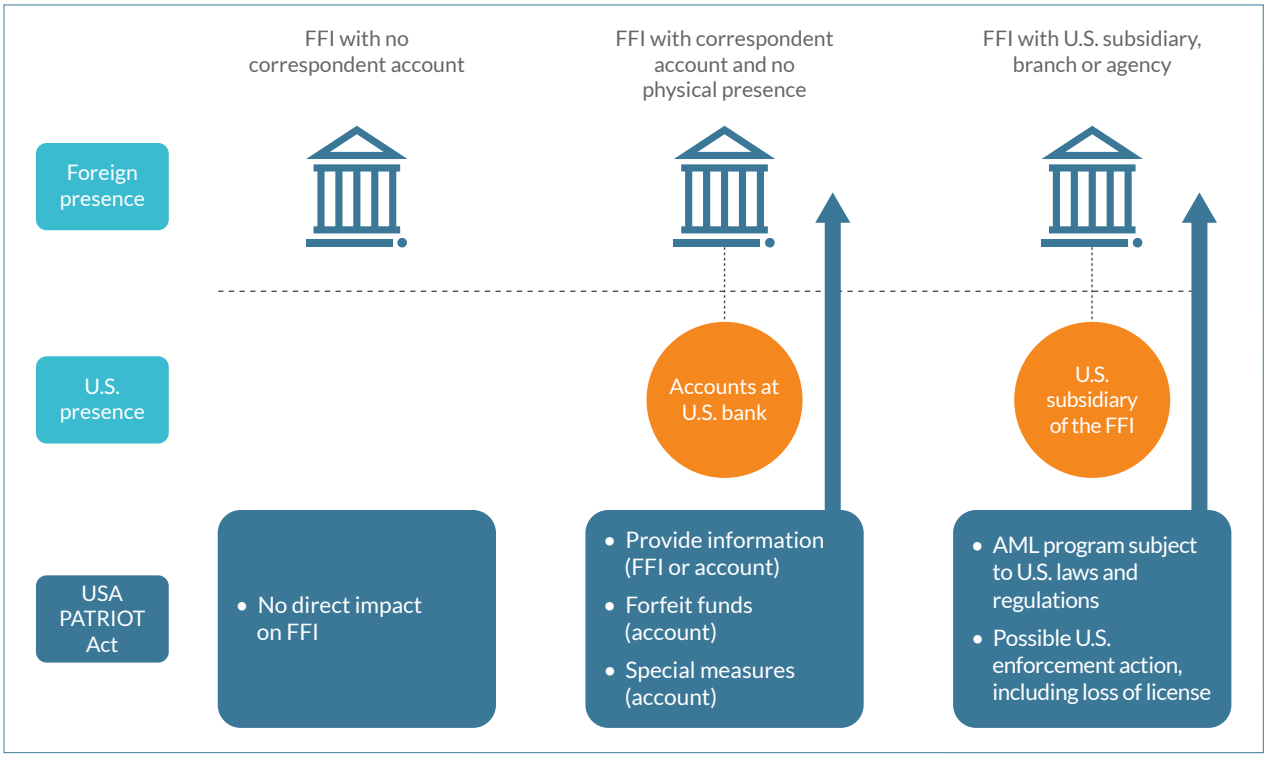
Non-U.S. offices of U.S.-chartered financial institutions are expected to comply with the stricter of U.S. or host country laws and regulations.

With the approval of the European Union's Fourth Anti-Money Laundering Directive, one area of change resulting from its implementation in national legislation, including in the United Kingdom, is that firms have to conduct a risk assessment for each of their customers. Firms will need to determine and justify cases where simplified or enhanced due diligence is applicable. The previously acceptable practice of applying blanket approaches to certain customer groups — for example, publicly listed companies — will no longer apply.

— Bernadine Reese, Managing Director in Protiviti's Risk & Compliance Practice, United Kingdom

[9] A PTA is an account maintained for a respondent bank that allows the respondent's customers to use the account directly (e.g., to make deposits or pay away).

Impact of U.S. AML Rules on Foreign Financial Institutions (FFIs)



The position is different in Hong Kong. While the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) does require all Hong Kong–incorporated financial institutions to implement group AML policies covering their overseas branches or subsidiaries to ensure that they operate to a standard that meets Hong Kong regulatory requirements, it is not the same as requiring all affiliates in the group to meet Hong Kong standards.

While requirements exist for correspondent banks to assess the AML frameworks of respondents, including affiliates, the HKMA does not appear to be intensely scrutinizing foreign subsidiaries of Hong Kong–based institutions unless there is a major concern. Also, there is a different tone and approach from the regulator regarding the ability to operate in Hong Kong, and no institutions, so far, have been under a serious license-withdrawal threat for AML violations.

In the United Kingdom, the FCA has Section 166 reviews and thematic reviews, which include an in-scope review of other jurisdictions within the particular bank's geographic footprint. To date, the general informal expectations from the FCA have been around AML internal control frameworks in the respective countries matching those of the head office.

Similar to Hong Kong, the United Kingdom's FCA has been less focused on entities in foreign jurisdictions and mainly focused on regulatory enforcements and fines at entities within the country. The FCA is likely to take a more active role in oversight of foreign subsidiaries, starting with large international U.K.-based banks for which it is the lead regulator. The outlined challenges and regional differences are applicable also to smaller and regional banks, which need to adequately manage these issues in a cost-effective and value-adding manner.

Point of View — Regulatory Examination and Enforcement

Care must be taken to address each country's regulatory requirements and expectations regarding correspondent banking related to AML controls, as merely following a risk-based approach will not fully satisfy all stakeholders. Protiviti has observed its clients facing issues in some of the following areas:

Assessing and understanding applicable legislation and regulation

- Abiding by the USA PATRIOT Act's certification requirements
- Abiding by requirements noting that EDD is obligatory, not risk-based, in certain circumstances (e.g., for banks that have an offshore license or in jurisdictions noncooperative with FATF or listed as warranting special measures)
- Having oversight and understanding of correspondent relationships
- Having awareness of inherent risk exposure from correspondent relationships
- Lacking awareness of the requirement to collect names of nested bank relationships
- Having a suitable framework to ensure that relevant regulatory requirements have been fulfilled

What singles out the United States from other jurisdictions is the desire to apply its regulatory requirements to foreign institutions through their use of the U.S. dollar, thus making U.S. rules the de facto minimum standard for a global bank.

To avoid unnecessary costs and duplication, firms should tailor their internal controls to ensure domestic compliance while being mindful of U.S. compliance requirements that may impact their institution. For example, correspondent banks seeking to clear U.S. dollars may also have to comply with certain U.S. requirements despite the fact they do not have a physical presence there.

Information Sharing

While the information-sharing processes between law enforcement agencies and banks are broadly similar across the three jurisdictions, there are differences in the way information is shared between banks and other financial institutions.

Information Sharing Between the Industry and Law Enforcement

Financial intelligence units in all three jurisdictions are empowered to obtain information on a person of interest:

- In the United States, Section 314(a) of the USA PATRIOT Act allows for law enforcement agencies to submit information requests through the Financial Crimes Enforcement Network (FinCEN), which then requires a financial institution to search its records to determine whether it maintains or has maintained an account for the named party within the past 12 months and to identify when transactions were conducted by or on behalf of the named party outside of the account during the preceding six months.
- A positive response is required within 14 days if there is a match; otherwise, no other information is required to be provided. Law enforcement agencies may also obtain information via other means, such as subpoenas and National Security Letters.
- In Hong Kong, the Joint Financial Intelligence Unit (JFIU) is given a range of powers under the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROPO), the Organized and Serious Crime Ordinance (OSCO) and the Police Force Ordinance (PFO) to obtain information from financial institutions on a particular person of interest and other information. These powers may be used to obtain additional information after a Suspicious Transaction Report (STR) has been submitted, but also may be used in other circumstances.
- In the United Kingdom, under Part 8 of the Proceeds of Crime Act (POCA), law enforcement has the authority to apply for production orders, customer information orders and account monitoring orders. Under POCA, financial institutions are required to respond to and provide the requested information to law enforcement within the time specified in the orders themselves.

It is important to note that financial institutions do not have protection against self-incrimination under POCA with production orders or search warrants. Furthermore, financial institutions are also required to seek consent from the National Crime Agency (NCA) on certain transactions the institution believes to be suspicious. The NCA will respond, typically within seven days, with consent to proceed with the transaction or an indication to block or hold it.

Information Sharing Among Banks and Other Financial Institutions

The formality of information-sharing arrangements between financial institutions varies by jurisdiction. For example, the United States has a formal scheme outlined in Section 314(b) of the USA PATRIOT Act, the United Kingdom has successfully piloted a formal scheme as part of the Joint Money Laundering Intelligence Taskforce (JMLIT), and the arrangements in Hong Kong remain relatively informal.

Section 314(b) of the USA PATRIOT Act provides the basis for a voluntary information-sharing program for U.S.-based financial institutions to exchange, under safe harbor protection, certain information about a customer. The underlying basis of a Section 314(b) request must be grounded in a legitimate AML concern. The process should not be used as a fishing expedition; an AML concern is a must.

After registering with FinCEN as a 314(b)-eligible institution, a financial institution can send and provide information from requests to other 314(b)-registered institutions. Information cannot be shared across international borders, and the sharing of SARs or knowledge of the existence or nonexistence of a SAR is not allowed.

However, responding to 314(b) requests is optional, and the process in practice is not quite as clear-cut as envisaged. Despite encouragement from regulators, financial institutions experience mixed results, ranging from prompt responses to requests, at best, to requests that are never addressed, at worst. Section 314(b)-designated individuals note that developing relationships with peers at other institutions provides for more effective results for 314(b) requests.

Two international information-sharing challenges were recognized by FinCEN's director, Jennifer Shasky Calvery, in May 2015: "lack of sufficient access by many FIUs to relevant national information and legal limitations preventing financial institutions from providing their multinational view of terrorist-financing networks to all affected jurisdictions."

In the United Kingdom, there is no formal scheme similar to Section 314(b). However, the JMLIT, a 12-month pilot program, was launched in February 2015, setting up a single hub through which intelligence on specific money laundering threats is shared between law enforcement and 10 of the United Kingdom's largest banks. The U.K. government has recently commented that this successful pilot scheme has demonstrated the clear benefits of partnership working between law enforcement agencies and the financial sector. With the JMLIT having formally come to an end as a pilot program, the U.K. government plans to build on the experience gained to put the taskforce on a permanent footing and make it an integral part of its anti-money laundering and counter-terrorist financing regime. The United Kingdom is seeking to increase its scale and capabilities, in order to tackle economic crime threats, including money laundering linked to corruption, trade-based finance, high-priority crimes and terrorist finance. A recent government paper suggests that the membership of the JMLIT should be expanded to include more banks and other financial services firms.[10]

There is also no formal scheme in Hong Kong and no explicit safe harbor from civil liability related to the sharing of information across financial institutions, so banks share information on a relatively ad hoc basis. Some financial institutions are wary of giving away information, especially to competitors. However, others capitalize on their size and commercial strength to be able to exchange information with other banks. For example, a large correspondent bank may be able to leverage its arrangement with a smaller respondent to share certain information about customers. The extension of a bank's ability to share and exchange information with other banks on financial crime-related matters is expected to help the entire sector in better managing these risks. However, given differing data privacy laws and regulations, this remains a challenge in most countries and jurisdictions due to data privacy law superiority.

[10] *The United Kingdom's Home Office and Her Majesty's Treasury's Action Plan for Anti-Money Laundering (AML) and Counter-Terrorism Finance (CTF)*, April 2016: www.gov.uk/government/uploads/system/uploads/attachment_data/file/517992/6-2118-Action_Plan_for_Anti-Money_Laundering__web_.pdf. See also Protiviti's Flash Report: *UK Outlines New Action Plan for Anti-Money Laundering and Counter-Terrorist Finance*, May 2016: www.protiviti.com/UK-en/insights/uk-outlines-action-plan-anti-money-laundering-and-counter-terrorist-finance.

SAR or STR Sharing

When is it acceptable to disclose, or share information about, a SAR or STR filing in one of these jurisdictions? The answer is almost never. All three jurisdictions demand strict confidentiality about SAR and STR filing and prohibit disclosure to the subject of the SAR or STR. However, there are obligations relating to the sharing of information within the organization, and these obligations differ across the three jurisdictions, therefore having an impact on how global banks can share this information internally among their hubs.

The following table displays how SARs can be shared within the organization in each of the three jurisdictions.

Intra-Organization SAR and STR Sharing Obligations — Country Comparison

United States
• SARs can be shared with the head office or controlling company of the financial institution making the SAR filing, regardless of whether they are based in the United States, but only if a confidentiality agreement is in place.
• SARs can be shared with any U.S. subsidiaries and affiliates under the same common control as the sharing institution and subject to U.S. SAR reporting rules. Foreign subsidiaries and affiliates fall outside this group.
• The sharing of SARs and the existence of SARs is not permitted under the USA PATRIOT Act Section 314(b) information-sharing scheme between U.S. financial institutions.
• Recipients of the information must be made aware of the confidentiality requirement and the risk of prosecution if disclosed to the client.
United Kingdom
• Sharing can be performed with any employee, officer or partner of the same firm.
• SAR information can be shared with related firms if they both belong to the same group and the firm is within a European Economic Area (EEA) state or country with equivalent money laundering requirements.
• SARs can be shared with outside entities if the report involves a customer or a transaction that is common to both firms, if both are within the EEA and subject to equivalent money laundering requirements, and if both are subject to protection of personal data duties equivalent to the POCA Section 333C and Terrorism Act's Section 21F.
Hong Kong
• Independent interpretation of what is appropriate disclosure within the organization is determined by the institution; the money laundering reporting officer (MLRO) decides when escalation to senior management is necessary to determine how to handle the relationship.

After reviewing laws and regulations in each country, the global Egmont Group of Financial Intelligence Units developed approaches to encourage increased sharing of SARs and STRs. While increased sharing does risk the confidentiality of the SARs and STRs, as well as their underlying investigations, and privacy can be compromised, there are benefits, such as more effective customer due diligence, transaction monitoring and law enforcement investigation efforts.

Increased sharing makes it harder for money launderers to hide behind the walls created when financial institutions cannot share information on suspicious individuals or entities. For example, money launderers are able to open new accounts more easily in different jurisdictions because institutions are unaware of previous suspicious activities.

Point of View — Information Sharing

On the surface, the schemes in the United States and the pilot schemes in the United Kingdom provide better approaches for information sharing between financial institutions, with explicit protection from civil liability. However, so long as participation is still optional, institutions are still able to ignore requests if they choose to do so.

In all three jurisdictions, tipping off[11] is a criminal offense under local laws. However, it is vital to recognize that the different regimes require that banks be careful when developing processes and controls for sharing information, SARs and SAR-related information. An acceptable practice in one country may lead to AML and data protection violations in other countries, which, despite best intentions, may leave the institutions open to legal proceedings.

To establish an AML information-sharing policy that is applicable cross-jurisdictionally, a bank should first understand the requirements in each jurisdiction in which it operates. While it may be tempting to select the most conservative requirement and apply it across the bank as a way to limit potential violations, a bank may be able to implement more effective AML programs if there are customized information-sharing processes developed within the bounds of applicable laws and regulations for each jurisdiction. The increased information flows will allow the bank to more effectively meet its responsibilities for money laundering detection.

[11] Under POCA Section 333A, tipping off is committed when a person reveals information gained through work in the regulated sector that a disclosure has been considered or made to an official, and when that information is likely to prejudice an investigation resulting from that disclosure.

AML Technology

Regulators in all three jurisdictions understand the important role AML technology plays in an AML control framework. Such technology includes software used to detect potentially suspicious transactions and to screen customers and payments against watch lists, as well as technology used to rate customer risk.

All have long been areas of focus during examinations of banks in the United States and the United Kingdom. More recently, the HKMA has put the issue, specific to transaction monitoring, under the spotlight in Hong Kong. Hong Kong Monetary Authority deputy chief executive Arthur Yuen Kwok-hang commented that "some banks do not have a good record-keeping system to monitor suspicious transactions for reporting. This may be related to some banks having not yet invested sufficient technology and manpower into the new requirements."[12]

Again, the principles are more or less the same across the three jurisdictions, but the U.S. rules are much more explicit and detailed in what they require. Some examples are discussed below.

AML Systems — Risk Model or Technology?

In the United States, the industry considers AML technology used for transaction monitoring, watch list screening and customer risk scoring as risk models subject to the requirements set out in the "Supervisory Guidance on Model Risk Management," issued by the OCC and by the Federal Reserve Board.[13] This requires an effective model risk governance program and, crucially, validation of the model by an independent party.

The independent party must assess model governance, replicate scenarios to verify that rule definitions have been implemented appropriately and give assurance that the threshold values are appropriate. This assessment must be performed by the bank's independent model validation group or a qualified third-party vendor with the required IT and quantitative and AML risk knowledge. Where such systems are run globally from a location outside of the United States, it is important to recognize that the U.S. requirements for an independent assessment still apply.

So far, the United Kingdom and Hong Kong have not gone that far and have not specifically classified AML technology as risk models requiring a model risk governance framework. For example, the HKMA, and the United Kingdom's JMLSG guidelines, are more general and require senior management to monitor development and implementation, periodic reviews to be undertaken, and parameters and thresholds to be appropriate.

The effective and efficient use of enabling technology remains a significant challenge to the financial services industry and an area of continuing regulatory criticism. For many financial institutions, this means more attention needs to be paid to the selection, configuration and maintenance of AML-related systems to justify the high level of spend on these systems.

— Carol M. Beaumier, Protiviti Managing Director, Protiviti, New York

[12] "Banks could face fines in anti-money laundering law compliance probe," South China Morning Post, June 4, 2015: www.scmp.com/business/banking-finance/article/1816065/banks-could-face-fines-anti-money-laundering-law-compliance.

[13] "Supervisory Guidance on Model Risk Management," Board of Governors of the Federal Reserve System and Office of the Comptroller of the Currency, April 4, 2011: www.occ.gov/news-issuances/bulletins/2011/bulletin-2011-12a.pdf and SR Letter 11-7: www.federalreserve.gov/bankinforeg/srletters/sr1107a1.pdf.

However, the JMLSG guidance has more specific guidelines for watch list screening than where commercially available automated screening software is implemented. Firms should understand their capabilities and limits and make sure they are tailored to their business requirements, data requirements and risk profile. Firms should also monitor the ongoing effectiveness of automated systems. Where automated screening software is used or watch list screening – where commercially available – organizations should be satisfied that they have adequate contingency arrangements should the software fail, and they should periodically check that the software is working as expected.

Examples of Concern Areas Affecting Suitability and Functionality of AML-Related Technology

This table illustrates some concerns typically expressed by regulators across the three jurisdictions in focus:

System Design and Validation

• Incomplete data population	• No tracking of workflow performance (e.g., backlogs, past due alerts)
• Lack of holistic customer monitoring	• Lack of independent system validations
• Incomplete customer coverage	• Poor workflow escalation capabilities (e.g., poor tracking of individual alerts and lack of timelines)
• Too many, or too few, alerts in proportion to risk and/or size of operations	• Various monitoring systems not linked, causing a broken customer view (e.g., fraud/market abuse separate from AML monitoring) and potentially leading to multiple cases on same/similar customer activity
• Undefined validation schedule	• Insufficient management information (MI) capabilities
• Inadequate deployment of transaction monitoring scenarios (e.g., not risk-based, insufficient coverage)	• Inaccurate/inconsistent MI reports generated from disparate systems

Point of View — AML Technology

Whether mandated by local regulations or not, considering AML technology systems risk models, and applying all the relevant disciplines that implies, is likely to result in greater efficiency and effectiveness.

With large correspondent banks under regulatory pressure from their home supervisors to enhance their AML technology capabilities, it is only a matter of time until similar requirements are extended to less proactive jurisdictions through U.S.- or U.K.-based correspondent banks serving these markets.

Additionally, it is expected that financial institutions will continue making cost reductions and efficiency gains, both of which can be achieved through deployment of suitable and fit-for-purpose AML technology.

Efficiency gains can be achieved in areas such as transaction monitoring through deployment of new AML technology delivering more effective scenario deployment, enhanced workflow capabilities and improved MI generation.

Summary

While there are many areas of commonality across the United States, the United Kingdom and Hong Kong, there are also several instances where the details behind the regulatory requirements and expectations differ, therefore creating challenges for managing a global AML compliance program.

Firms will be able to leverage a large proportion of their AML controls globally across these three key financial services hubs; however, at the same time, there will be areas that will require a regional or national approach to allow global institutions to meet all local regulatory expectations. This requires firmwide controls to be global in application yet carry a degree of flexibility to allow for regional variations — a balance difficult to strike.

Appendix A

Regulatory Body	Full Name and Description
DOJ	The United States Department of Justice (DOJ), also known as the Justice Department, is a federal executive department of the U.S. government, responsible for the enforcement of the law and administration of justice in the United States, equivalent to the justice or interior ministries of other countries.
FinCEN	The Financial Crimes Enforcement Network, a bureau of the U.S. Treasury Department, is the financial intelligence unit for the United States interfacing with law enforcement agencies. It also provides guidance on implementation of AML regulations.
FCA	The Financial Conduct Authority, whose responsibilities include maintaining financial market integrity, is a financial regulatory body that operates independently of the U.K. government.
PRA	The Prudential Regulatory Authority, created in 2012 with the FCA, is responsible for the prudential regulation and supervision of around 1,700 banks, building societies, credit unions, insurers and major investment firms.
HKMA	The Hong Kong Monetary Authority is the government authority in Hong Kong with responsibility for maintaining the integrity of the banking system and Hong Kong's status as an international financial center. There is a specialist AML function within the banking-supervision division.
FFIEC	The Federal Financial Institutions Examination Council is an interagency body in the United States, including, for example, representatives of the FRB and the OCC. It is empowered to prescribe uniform principles, standards and report forms and to promote uniformity in the supervision of financial institutions.
JMLSG	The Joint Money Laundering Steering Group is composed of the leading U.K. trade associations in the financial services industry. Its aim is to promulgate good practice in countering money laundering and give practical assistance in interpreting the United Kingdom's Money Laundering Regulations.
NCA	The National Crime Agency operates the United Kingdom's financial intelligence unit.
JFIU	The Joint Financial Intelligence Unit operates Hong Kong's financial intelligence unit.
FRB	The Federal Reserve Board is responsible for supervision of bank holding companies and state member banks and maintains oversight of foreign banking organizations operating in the United States.
FDIC	In addition to administering the deposit insurance system in the United States, the Federal Deposit Insurance Corporation is responsible for supervising state nonmember banks.
OCC	The Office of the Comptroller of the Currency authorizes and supervises all federally chartered and licensed banking organizations in the United States.
NCUA	The National Credit Union Association charters and supervises federal credit unions.

It is important to note that the United States operates under a dual banking system under which depository institutions may opt for either federal or state charters or licenses. State banking authorities have authority to grant state charters or licenses and, along with their federal counterparts, supervise state-chartered, state-licensed organizations.

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

CONTACTS

Carol Beaumier
+1.212.603.8337
carol.beaumier@protiviti.com

Michael Brauneis
+1.312.476.6327
michael.brauneis@protiviti.com

Suneet Gorawara
+852.2238.0486
suneet.gorawara@protiviti.com

Bernadine Reese
+44.20.7024.7589
bernadine.reese@protiviti.co.uk

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
Sao Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City

PERU*

Lima

VENEZUELA*

Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

SAUDI ARABIA*

Riyadh

SOUTH AFRICA*

Johannesburg

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

INDIA*

Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

protiviti®