# Know your customer: Enhanced requirements

Know your customer/customer due diligence (KYC/CDD) requirements have been the focus of regulatory revision processes both in the U.S. and the EU in 2016, leading to a changed understanding of the KYC/CDD requirements and the approaches and tools needed to meet these requirements.

These developments are the result of shortcomings in KYC/CDD processes and procedures, which have resulted in numerous enforcement actions across the banking sector in recent years, but also due to the increased threats emanating from terrorist activities. KYC/CDD processes act as a link between all financial crime areas, including the new topics of increased international focus—namely targeted sanctions and anti-human trafficking.

An increased focus has been placed on risk assessment, high-risk countries politically exposed persons (PEPs), beneficial ownership and on actually identifying and verifying customers, their business—and if relevant—the customer's customer. The point here is to understand not only who the legal owner of the business or account is, but who actually controls the entity. With regards to PEPs, there are cases where PEPs are not registered as owners of an entity, but are indeed controlling the business. The purpose and nature of the customer has to be understood in order to determine the purpose for the account. Source of funds and source of wealth must also be determined.

It is widely recognized that a holistic and enterprise-wide approach to KYC/CDD is required in order to effectively manage the increased requirements vis-à-vis KYC/CDD risk attached to customers. This requires not only improved training in this area at various levels within the organization, but also investment in technological solutions, which will enable this goal to be achieved.

The following article outlines some of the recent regulatory changes in relation to customer due diligence (KYC/CDD) requirements both in Europe and the U.S. with a particular focus on PEPs and beneficial ownership. The topic of KYC/CDD sits at the heart of this discussion.

## KYC/CDD: Stepping up the pace

At the 2016 ACAMS' *12th Annual AML and Financial Crime Conference* in London, Rick McDonell, former FATF executive secretary, spoke of "reinvigorated determination" on behalf of regulators who are committed to strengthening and deepening the regulatory framework in order to more effectively combat financial crime. Although the leak of the Panama Papers and the terror events in 2015 and 2016 have increased the drive to pass adequate legislation and amend existing legislation quickly, the discussions around making KYC/CDD policy a requirement has been ongoing for some time.

European regulators and those across the globe can be seen unifying efforts against the existing and emerging global threats. For example, in June 2016, the regulator in Singapore stepped up its efforts to enforce better KYC/CDD standards, and as recently as July 2016, the Indian regulator fined its state-owned banks and advised them to "put in place appropriate measures and review them from time to time to ensure strict compliance of KYC/CDD requirements and FEMA provisions on an ongoing basis."[1] Although terrorist financing does not appear to be the driver, it may be viewed more as the accelerator of these developments.

**The purpose and nature of the customer has to be understood in order to determine the purpose for the account**

## KYC failings: Enforcement actions and sanctions

Financial institutions in the U.S., Europe and Asia have been at the heart of a number of large-scale investigations resulting from failings in their AML and in particular, their KYC/CDD policies and procedures.

Consequences of KYC/CDD noncompliance keep growing. In 2014, the U.K. regulator alone issued 1.5 billion pounds in fines—in 2013 the figure was 474 million pounds. Worldwide since 2013, financial institutions failing to meet anti-money laundering (AML) rules for KYC have been fined more than $10 billion.[2]

From 2004 to 2010, 110 financial institutions in the U.S. "were fined for AML failures, including lack of training. The most commonly publicized penalties for compliance failure are monetary fines. There has been no shortage of media coverage of major financial institutions such as HSBC ($1.92 billion) and Standard Chartered ($327 million) in 2012, and BNP Paribas ($8.9 billion) in 2014. Many other institutions have also been fined for smaller amounts over the years as well."[3]

In 2014, Standard Chartered was fined 7.5 million pounds for failures in its AML controls and KYC/CDD procedures. In 2015, Barclays was fined a staggering 72 million pounds by the U.K. regulator for poor handling of financial crime risks. The clients involved were PEPs and should therefore have been subject to enhanced levels of due diligence and monitoring.

In Germany over the past year, there have been $1.45 billion in penalties imposed on Commerzbank to settle sanctions and money laundering related charges. Recently, the case against Deutsche Bank and its sanctions violations saw the bank being fined $258 million.

In August 2016, New York's state bank regulator (DFS) fined Mega International Commercial Bank of Taiwan $180

[1] "RBI Penalizes 13 Banks for Violating KYC Norma," Reserve Bank of India, July 27, 2016, https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=37618

[2] Steve Pulley, "Regulatory Changes and Stiffer Fines are a Call to Action for Smarter KYC & AML Compliance," Thomson Reuters, September 15, 2016, http://blog.financial.thomsonreuters.com/regulatory-changes-and-stiffer-fines-are-a-call-to-action-for-smarter-kyc-aml-compliance/

[3] "What happens when businesses don't comply with AML/KYC regulations?," Trulioo, February 11, 2015, https://www.trulioo.com/blog/happens-businesses-dont-comply-amlkyc-regulations/

million for deficiencies in their CDD/KYC risk assessment. As recently as August 2016 and as of November 2016 the DFS fined the Agricultural Bank of China $215 million for violating anti-money laundering and sanctions laws involving Russia, China and Afghanistan, amongst others.[4] These are some examples of the fines presented by the DFS since 2015.

**For each new customer, a financial institution or obliged entity must identify and verify the ultimate beneficial owner**

## FinCEN's CDD Rule

On May 11, 2016, the U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) issued its Final Rule for CDD under the Bank Secrecy Act (BSA) for banks and other covered financial institutions. The rule, which came into effect on July 11, 2016, must be implemented by the following organizations by May 11, 2018: banks, broker-dealers, mutual funds, futures commission merchants and introducing brokers in commodities. All obliged entities will have to identify and verify the identity of their entities' beneficial owner.

The CDD Rule has been termed as the fifth pillar created to support compliance programs. Prior to this, financial institutions have operated under an effective BSA/AML compliance program, which includes the following four pillars: policies and procedures, appointing a designated AML compliance officer, independent testing of the institution's AML program, and the implementation of an adequate employee training program. The fifth pillar now underlines the importance of a risk-based, CDD procedure.

For each new customer, a financial institution or obliged entity must identify and verify the ultimate beneficial owner, who might be an individual who either directly or indirectly retains a 25 percent stake in the company or an individual who controls/manages a legal entity. Exclusions to the rule also exist and must be taken into consideration in this regard also.

## EU Fourth AML/CTF Directive: EBA KYC guidance

"The EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing—more commonly known as the Fourth EU AML Directive—was passed by the European Parliament on May 20, 2015, and came into force on June 25, 2015."[5] The European Banking Authority drafted guidelines on risk factors and simplified and enhanced customer due diligence.[6] The guideline underlines that firms should put in place systems and controls which enable them to identify and assess emerging money laundering/terrorist financing (ML/TF) risks and to incorporate these in their business-wide and individual risk assessments. With regard to KYC requirements the document differentiates broadly between simplified due diligence (SDD) and enhanced due diligence (EDD). The following main points are set out in the guideline:

### *Simplified due diligence*

In line with national legislation and in the context of the risk-based approach, obliged entities can apply SDD measures in situations where the ML/TF risk associated with a business relationship is low. Nonetheless the quality of the information on which this decision is based must enable the firm to "be reasonably satisfied that the risk associated with the relationship is low" and provide "enough information about the nature of the business relationship to identify any unusual or suspicious transactions."[7]

### *Enhanced due diligence*

Where firms are faced with higher AML/CTF risks, EDD measures must be undertaken in situations to manage and mitigate those risks appropriately. The guideline refers to Directive (EU) 2015/849, which lists the following specific high-risk situations that firms must always treat as high risk:

- Where a customer or a customer's beneficial owner is a PEP, firms must a) "take adequate measures to establish the source of wealth and source of funds to be used in the business relationship," b) "obtain senior management approval for entering into or continuing a business relationship with a PEP" and c) "apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship."[8] Firms must apply all of these measures to PEPs, their family members and to known close associates and should adjust the extent of these measures on a risk-sensitive basis.
- Where a firm enters into a correspondent relationship with a respondent institution, firms must take specific EDD measures where a cross-border correspondent relationship with a respondent who is based in a third country exists. Firms

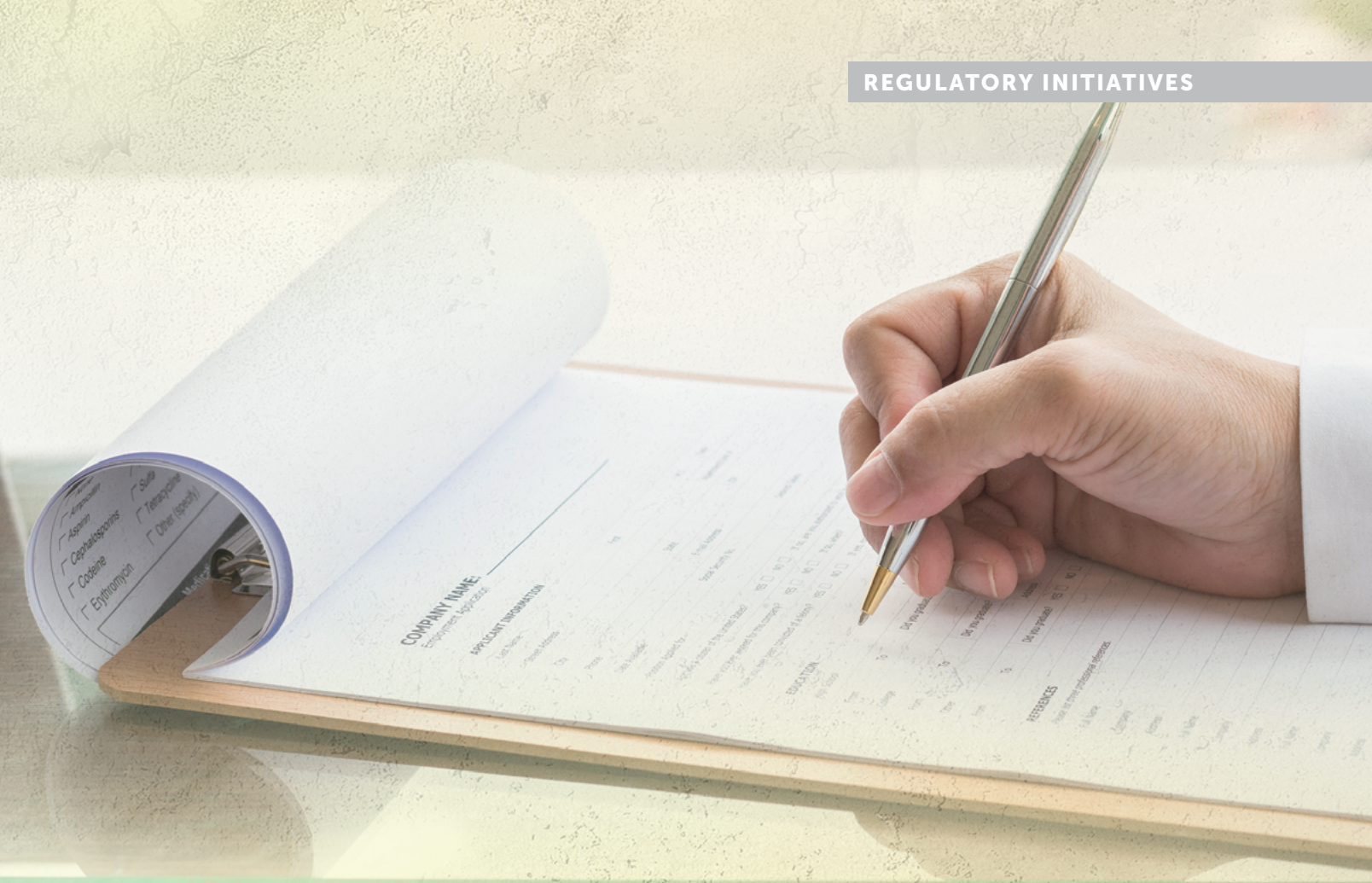
[4] "New York fines Chinese bank US$215m for money laundering violations," *HKFP*, November 5, 2016, https://www.hongkongfp.com/2016/11/05/new-york-fines-chinese-bank-us215m-money-laundering-violations/

[5] Jennifer Hanley-Giersch, "The Fourth EU AML/CTF Directive: A Holisitc Risk-Based Approach," *ACAMS Today*, September-November 2015, http://www.acamstoday.org/fourth-eu-aml-ctf-directive/

[6] "Joint Consultation Paper," Join Committee of the European Supervisory Authorities, October 21, 2015, https://www.eba.europa.eu/documents/10180/1240374/JC+2015+061+%28Joint+Draft+Guidelines+on+AML_CFT+RFWG+Art+17+and+18%29.pdf

[7] Ibid.

[8] Ibid.




must apply all of these measures and should adjust the extent of these measures on a risk-sensitive basis.

- Where a firm deals with natural persons or legal entities established in high-risk third countries.

## Summary

Both in the EU and in the U.S. we have seen updates on the regulatory level in relation to KYC/CDD requirements. The European Commission (also under pressure following the tragic events in Paris and Brussels) published their outline on how they plan to deliver on the European Agenda on Security to combat terrorism, and started to discuss the shortcomings in the Fourth EU AML/CTF Directive with the topic of enhanced KYC at the top of the list, in preparation for the Amendment to the Fourth EU AML Directive to be passed in early 2017.

Not only is the changing regulatory landscape demanding that firms review their KYC/CDD procedures, but equally important are the numerous fines which indicate the great challenges in putting in place effective KYC/CDD systems and procedures.

Besides understanding the nature and purpose of the relationship, as well as the ultimate beneficial ownership of entities, it is important to remember that KYC/CDD risk assessment is a dynamic and ongoing process, which is also recurring due to the ongoing monitoring requirements. In order to strengthen organizations' processes and procedures, the following can be recommended:

- Establishing robust protocols for onboarding, identifying beneficial owners and risk rating clients
- Boosting client identification accuracy with EDD policies
- Formalizing policies for regular risk reevaluation and when to escalate for EDD review

If organizations succeed in not only identifying the ultimate beneficial owner and locating KYC/CDD information when required, but also succeed in getting the business to understand and own the risks identified, they will be able to install effective and solid KYC/CDD processes and procedures, which will not only meet regulatory requirements, but also add value to the business overall.

*Jennifer Hanley-Giersch, CAMS, managing partner, Berlin Risk Ltd., Berlin, Germany, jennifer.hanley@berlinrisk.com*