

# ACAMS TODAY

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

## NAVIGATING FATF Recommendation 16



amid concern about the rise of terrorist organizations and other criminal bodies, banks are being asked to step up their role in monitoring international payments. While much attention has been paid to issues such as know your customer (KYC) deficiencies and sanctions violations—and the sizeable penalties imposed as a result of these issues—the more fundamental issue of data quality is beginning to attract more focus.

This is underlined by the Financial Action Task Force's (FATF) 2012 recommendations—particularly Recommendation 16—which specifies the need for financial institutions to provide information not just about the originator of a payment, but also the beneficiary. Under this recommendation, banks will also have a more explicit obligation to monitor the quality of data in the transactions they receive. The EU and Singapore have already issued regulations that reflect Recommendation 16, and other FATF members—including the U.S.—are expected to follow.

Complying with the new requirements will present some significant operational and compliance challenges for banks. However, by taking the steps needed to improve data quality, banks can also expect to see considerable benefits from the more effective use of sanctions filters to greater insights from business intelligence.

### Background

Knowing who is sending and receiving money is an essential part of tackling money laundering, terrorist financing and other forms of financial crime. Recommendation 16 aims to improve the traceability of transactions, with the intention of preventing and detecting terrorist financing and other illicit activities.

The new requirements come as part of a wider focus on improving KYC procedures as a means of preventing money laundering and terrorist financing and in the context of new regulations, such as the EU Fourth Anti-Money Laundering Directive. While understanding an entity's ultimate beneficial owner (UBO) has been a critical element of KYC for years,

developments in the last few months have intensified focus on this area. "Recent events such as the publication of the Panama Papers has helped to speed up the release of proposed and final rules in the U.S. and the U.K. on formalizing UBO disclosure," comments Daniel Tannebaum, a director in PwC's Financial Crimes Unit and the leader of the Global Financial Services Sanctions Practice.

At the same time, with greater importance being placed on the issue of preventing terrorist financing, banks are seen as the front line to stop funds from falling into the wrong hands. They have to balance this duty with the need of making sure that payments made for customers are as quick, efficient, cheap and seamless as possible.

"The only way to achieve this is to make sure that the data is of sufficiently high quality so that automated solutions can do their work," says Stephen Lindsay, head of standards at SWIFT. "That's why there is a push to improve the data quality at the source—so that when you are screening it for embargoed countries or sanctioned customers, you can do so automatically, efficiently and effectively."



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  
© 2016 [www.acams.org](http://www.acams.org) | [www.acamstoday.org](http://www.acamstoday.org)

**ACAMS**® Advancing Financial  
Crime Professionals  
Worldwide

## What is changing?

The FATF Recommendations, published in 2012, consists of 40 recommendations. These are intended to provide a framework enabling countries to combat money laundering and terrorist financing in a consistent way. Many FATF member countries—and the EU (which is also a FATF member)—are in the process of incorporating the FATF recommendations into their own regulations and requirements.

Recommendation 16 applies to both cross-border and domestic wire transfers. The objective of the recommendation, as set forth in the FATF Recommendations, is to prevent “terrorists and other criminals from having unfettered access to wire transfers for moving their funds, and for detecting such misuse when it occurs.”<sup>1</sup>

Parts of Recommendation 16 are already stipulated by FATF’s previous guidelines on this topic, Special Recommendation 7 (SR7), and by the Travel rule in the U.S., which requires banks to transmit certain information to other banks. While these rules focus on originator information, Recommendation 16 requires both originator and beneficiary information to be included in some financial messages for wire transfers.

- For cross-border wire transfers, the name and account number of the beneficiary must be included in the financial message and must travel with the transfer. Transfers should also include the originator’s name, account number and address, or other information to aid identification, such as their national identity number, customer identification number, and date and place of birth.
- For domestic transactions (regardless of country), which are easier to trace, the requirements are less onerous, with the provision that full information must be provided to the beneficiary institutions and appropriate authorities by other means when requested.



## Monitoring and reporting

As well as stipulating the information that needs to be included in wire transfers, Recommendation 16 sets out the need for banks to monitor the transactions they receive. Banks will need to ensure that the required data is provided and take the necessary steps if it is not.

Banks are expected to take a risk-based approach regarding missing originator and beneficiary information. This could include talking to the relevant bank and encouraging it to improve its standards. Such follow-up may now be getting more robust, with some financial institutions saying that if the data quality from certain counterparties does not improve, they will look to terminate those relationships. This could have a particular impact in developing markets, where financial regulations are less stringent and the countries themselves are not members of FATF.

Meanwhile, under Recommendation 16 the obligations for banks to monitor data are made much clearer. Financial institutions “should have effective risk-based policies and procedures for determining when to execute, reject, or suspend a wire transfer lacking required originator or required beneficiary information; and the appropriate follow-up action.”<sup>2</sup> Individual countries can be even more stringent, and EU regulation talks about terminating relationships in the face

of repeated noncompliance with originator and beneficiary information requirements.

## Adopting FATF Recommendation 16

Although the FATF Recommendations were published in 2012, they are still being implemented in various countries. As such, some jurisdictions have made more progress than others in adopting the new guidelines. The EU published its relevant legislation, the Funds Transfer Regulation (*Regulation (EU) 2015/847 of the European Parliament and of the Council on information accompanying transfers of funds*) in June 2015; however, enforcement will not begin until June 2017. Singapore has also included the new rules in MAS Notice 626.

Complying with the new regulations is likely to place some significant challenges on the industry. Good quality data will need to be captured at the source and banks should invest in sophisticated quality checking systems which can deal appropriately with formatting challenges. Rather than adopting a ‘firefighting’ approach and tackling issues message by message, banks should take an analytical approach in order to find patterns and offenders and resolve issues at source.

Indeed, complying with the existing requirements for originator information under SR7 is not necessarily straightforward, mainly because the data provided is unstructured.

<sup>1</sup> “Recommendation 16: Wire Transfers,” <https://www.fatf-gafic.org/index.php/documents/fatf-40r/382-fatf-recommendation-16-wire-transfers>

<sup>2</sup> Ibid.



“This is something that institutions have struggled with for years,” says Tannebaum. “For one thing, there have been limited penalties related to travel rule-like requirements, even though there has been legislation in place for a number of countries mandating certain information to travel with the transaction. Technology limitations have also been a big challenge. Many institutions simply do not have controls in place to detect incorrect or missing information in certain required fields.”

Tannebaum says ‘what we’ve seen in many banks are challenges relating to systems glitches where fields are populated with incorrect data, for example an institution’s own address instead of the actual transaction originator’s address.



## Collaboration can play an important part in improving consistency across the industry



A further obstacle is the inconsistencies that may arise between different bank approaches to capturing data from customers. Some banks require full data for both originator and beneficiary, while others do not. “That inconsistency can certainly slow international cross-border transactions,” says Tannebaum. “One bank may have laxer standards than a downstream correspondent. This might mean that a transaction is stopped because of a lack of information that the upstream bank is not required by law or policy to collect,” he adds.

Collaboration can play an important part in improving consistency across the industry. Compliance with Recommendation 16 is one of the issues being discussed by the Payments Markets Practice Group (PMPG), which works to improve market practices in conjunction with the correct use of standards. To that end, PMPG has published specific guidelines for Recommendation 16 compliance

using SWIFT MT messages.<sup>3</sup> Critical market infrastructures, as well as transnational industry organizations such as SWIFT, can play a leadership role in helping financial institutions work together to address these challenges.

## What banks need to do

First and foremost, banks need to ensure that they understand the changes. This should include talking to other banks, industry groups and regulators in order to understand the new rules and find out how others are responding.

In light of the new requirements, there is a clear need for banks to adopt more explicit policies—both to ensure the accuracy of their own data and to monitor the data provided by other banks. Internal controls should be enhanced to make sure that certain fields are populated with the right information. Controls should also be in place to root out ‘dummy data’—for example, when fields are populated with strings of numbers instead of strings of letters.

At an operational level, banks should consider whether they will need to purchase new software. They should also make sure they have an overview of all of the payment systems in place across the group, as well as assurance that every part of the group is following the same approach. They will also need to ask whether they need to do real-time monitoring or post-fact monitoring, and build suitable processes and procedures around these points.

However, the main challenge for banks is to focus sufficient attention to this area, which can be difficult with so many competing priorities. As Tannebaum comments, “Many banks operate under a triage-based approach, so wherever the regulator or auditors are shouting the loudest tends to be where resources are directed.”

## Beyond FATF Recommendation 16 compliance

There is more to data quality than achieving compliance. While complying with Recommendation 16 is the main catalyst

for banks to tackle this area, it is also important to note that improving data quality brings additional benefits, such as the more effective use of sanctions-related systems.

This is true because sanctions filters and systems are being fed data that goes back to the quality of the payments themselves. If banks look at the quality of the data and fix any issues before the data hits the sanctions screening, transaction monitoring, KYC or anti-money laundering systems, then those systems will be able to operate much more effectively.

“Increased consistency in the reduction of errors or missing data fields will do nothing but speed up transactions,” says Tannebaum. “If you have a greater confidence in the data in the field that you are passing through your sanctions screening filters, you will have greater confidence in your ability to comply with the mandate of the program in question,” he adds.

Other spinoff benefits may include improved straight-through processing (STP) and improvements in transaction monitoring processes. In addition, improved data quality may enable banks to use their own data more effectively from a business intelligence point of view. A bank’s payment flows represent a rich source of business intelligence on areas such as which relationships are the most profitable, which countries the bank is most exposed to and where their business is coming from. The better quality data a bank has about the originators and beneficiaries of these payments, the more usable that information is.

In conclusion, data quality may not have attracted as much focus in the past as some other topics. However, the adoption of Recommendation 16 is pushing this issue higher up the priority list—and despite the challenges involved, improving data quality will also bring considerable benefits beyond regulatory compliance. **■**

*Simon Muir, lead product manager, Financial Crime Compliance Services Division, SWIFT, Brussels, Belgium, [simon.muir@swift.com](mailto:simon.muir@swift.com)*

<sup>3</sup> See [www.pmpg.info](http://www.pmpg.info)

