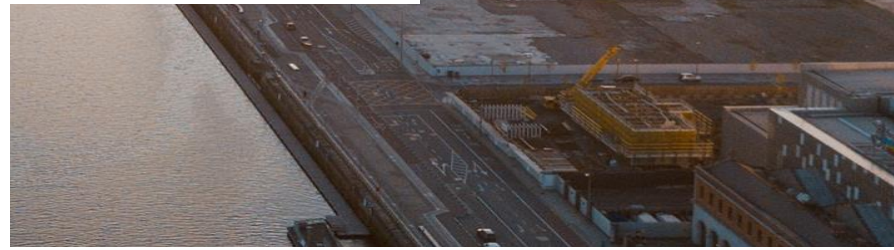
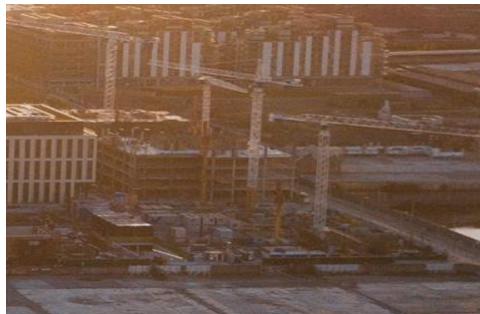
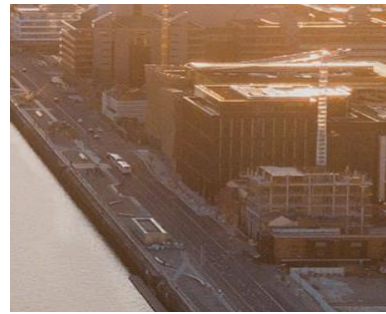


Financial Crime Update - May 2022



Introduction

Welcome to the latest edition of our new Financial Crime update, which outlines all of the latest news and regulatory updates across the world of Financial Crime.

From a European perspective, in March, the European Banking Authority issued a report on Competent Authorities approaches to AML / CTF supervision of banks. They also launched their central database for AML/CTF in January.

In Ireland, the Central Bank published further guidance in April on the latest amendments to the new list of Pre-approved Controlled Function roles, including the new PCF-52 - the “Head of Anti-Money Laundering and Counter Terrorist Financing Compliance”. They also noted in a speech in March that AML/CTF will continue to be “an area of core focus this year, and indeed for the foreseeable future”.

In April, PwC hosted an AML webinar addressing the evolution of AML Operating Models, leveraging technology. If you missed it, you can listen back here:

https://event.webcasts.com/starthere.jsp?ei=1511256&tp_key=bf7612e84e

We hope you enjoy reading this newsletter, which contains further details on the issues outlined above, and more!

Sinead Ovenden

Partner, FS Risk and Regulation

Contents

- Irish Financial Crime Updates
 - Amendments to the list of Pre-approved Controlled Functions
 - Central Bank of Ireland updates
 - Department of Justice officials to have power to issue fines for minor money laundering breaches
 - Regulation on a central database on safe-deposit boxes and bank and payment accounts published
- European & UK Financial Crime Updates
 - EBA statement on financial inclusion in the context of the invasion of Ukraine
 - European Banking Federation's Position on Proposal for a Regulation Establishing a new AML/CTF Authority
 - EBA launches 'EuReCA:' the EU's central database for AML / CTF
 - Cayman Islands added to EU AML Blacklist
 - EBA alerts on the detrimental impact of unwarranted de-risking and ineffective management of ML/TF risks
 - EBA report on competent authorities' approaches to AML/ CTF supervision of banks
 - EBA concludes its Luanda leaks investigation
 - FCA review finds weaknesses in some new banks' financial crime controls
- Global Financial Crime Updates
 - Wolfsberg Group publish guidance on Digital Customer Lifecycle Risk Management
- FATF Insights
 - Report on the State of Effectiveness and Compliance with the FATF Standards

3

8

17

19



IRISH FINANCIAL CRIME UPDATES

1

Amendments to the list of Pre-approved Controlled Functions

In September 2021, the Central Bank of Ireland (CBI) published their intention to amend the current PCF list - which included the introduction of PCF-52 - "The Head of Anti-Money Laundering and Counter-Terrorist Financing", replacing the previous PCF-15 ("Head of Compliance with responsibility for Anti Money Laundering and Counter Terrorist Financing Legislation"). In April 2022, further guidance was published around these new PCF roles, where a number of points were clarified by the CBI:

- The CBI confirmed that the new PCF-52 role is specifically an AML compliance role, and the title has been amended to reflect this to the "Head of Anti-Money Laundering and Counter Terrorist Financing Compliance"
- This new PCF does not in and of itself require the appointment of separate individuals to PCF-12 and PCF-52 but it will be up to individual regulated entities to assess the roles and determine the appropriate appointments for their business.
- Where it is not appropriate or applicable for an organisation to redesignate a current PCF-15 to PCF-52, the regulated entity must review its functions to determine whether any of them would meet the Head of AML and CTF Compliance role. If it is determined that no current roles fit the PCF-52 designation, the regulated entity is not required to create a new PCF role in order to comply with obligations under the Fitness & Probity regime. However, they will be required to review their assessment under Section 21 of the Central Bank Reform Act 2010 in respect of individuals in-situ and submit confirmation of such an assessment to the Central Bank.

In relation to timelines for these changes, in-situ PCF-15 designations will be end-dated and firms will be required to notify the Central Bank of the appropriate PCF designation of the individual by 3 June 2022, either PCF-12 or PCF-52



Central Bank of Ireland updates

Warning on Crypto Assets

In March 2022, the Central Bank of Ireland (CBI) issued a warning on the risks of investing in crypto assets, as part of a wider European campaign led by the European Supervisory Authorities. The CBI emphasised that crypto assets are highly risky and speculative, and may not be suitable for retail customers. They also noted that people need to be alert to the risks of misleading advertisements, particularly on social media, where influencers are being paid to advertise crypto assets.

In addition to this warning, the European Security Authorities have also recently highlighted that these assets are not suited for most retail consumers as a means of payment or as an investment asset, and highlighted the fact that there is little recourse or consumer protection available as these products and services typically fall outside existing protective regulation.

The CBI has published a plain English explanation for consumers on cryptocurrencies, which can be found here: <https://www.centralbank.ie/consumer-hub/explainers/what-are-cryptocurrencies-like-bitcoin>.

AML remains a priority for the CBI

In March 2022, Director General of the Central Bank of Ireland (CBI), Derville Rowland, set out the priorities of the CBI for the year ahead during a speech delivered at FSI Executive Board engagement. Amongst these priorities, Ms Rowland outlined that “Anti-money laundering and countering terrorist financing will be another area of core focus this year, and indeed for the foreseeable future”. She noted that the CBI will work closely with their European counterparts “to help shape and implement the Package and the new single Anti-Money Laundering (AML) authority, which will mark a structural sea-change in the European approach to combating this problem”.

Mrs Rowland noted that there were currently numerous products and services, particularly cryptocurrencies and assets, which fell outside of current AML/CTF regulation but that this was a gap which European authorities were working to close. It was highlighted that the European regulatory framework must be strengthened to prevent fraud risk to investors, particularly retail investors



Department of Justice officials to have power to issue fines for minor money laundering breaches

While the Central Bank of Ireland is the supervisor and competent authority for the financial service industry, the Department of Justice are the Competent authority for non-Financial Services designated bodies. Under Government plans announced in January 2022, the Department is set to be given the power to issue fines for breaches of money laundering laws. The current legal environment only allows for a criminal prosecution. This move follows a request from Justice Minister Helen McEntee to expand the regulatory enforcement powers of the Department's Anti-Money Laundering Compliance Unit (AMLCU).

The new powers will enable officials in the AMLCU unit to implement obligations under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. A new heads of bill is to be drafted to give a legislative basis to the new powers. The level of administrative fines that the AMLCU will be able to issue, and the strict liability offences to which those fines will apply, are to be considered further as part of the drafting of the legislation.





Regulation on a central database on safe-deposit boxes and bank and payment accounts published

A new regulation authorising the CBI to establish and maintain a register of information on safe-deposit boxes and bank and payment accounts was published in Ireland in February 2022: The EU (Anti-Money Laundering: Central Mechanism for Information on Safe-Deposit Boxes and Bank and Payment Accounts) Regulation 2022.

Under this regulation, credit institutions may have to provide certain prescribed information to the CBI, which will be held for a minimum of 5 years after an account is closed or a safe-deposit box has expired. Access to the data will only be made available to FIU Ireland, who may in turn share it with other FIUs throughout the EU.

The information which credit institutions will have to provide relates to individuals' personal details and those of corporate entities, as well as bank/payment and safe deposit account details. The CBI is yet to communicate a timeline for credit institutions to comply with this regulation, and have indicated that they are still finalising the technical details.

EUROPEAN & UK FINANCIAL CRIME UPDATES

2

EBA statement on financial inclusion in the context of the invasion of Ukraine

On 27 April 2022, the European Banking Authority (EBA), issued a statement on financial inclusion in the context of the invasion of Ukraine, the large number of people who have now found refuge in EU member states and their need for access to basic financial products and services to participate in society.

In this statement, the EBA outlined what financial institutions and regulators can do in order to provide access to the EU financial system to refugees. The statement references the Temporary Protection Directive, which was activated by the EU on 4 March 2022. This Directive has provided temporary EU residency and a right to access and use of a payment account with basic features to all refugees from Ukraine.

The EBA outlined that whilst institutions must continue to comply with their regulatory obligations in respect of AML, they should do so within the flexibility permitted by the directive and apply simplified due diligence where there is a reduced risk of money laundering. For example, where a product's functionalities are limited or only available to customers meeting a set of narrowly defined criteria. Consequently, in these circumstances, firms may not need a passport to verify a customer's identity but can instead look to alternative independent documentation, such as evidence that an individual is a refugee coming from Ukraine. Institutions may also postpone initial onboarding identification to a later date, where the conditions in Guidelines 4.41, 9.15, 10.18 of the EBA's ML/TF Risk Factors Guidelines are met.

The EBA's statement also alerts institutions to signs of potential indicators that refugee customers are being exploited. This can include signs such as recurring payments for wages at unusually low amounts or unusual patterns of transactions. Given the heightened risk of human trafficking and exploitation that such a humanitarian crisis can cause, the EBA encourages financial institutions to remain vigilant and monitor customer activity for these signs.

Finally, in addressing the expanding EU sanctions regime, the EBA noted that financial institutions should pay particular attention to apparent attempts by customers to obfuscate relationships with sanctioned persons and those who are at risk of being sanctioned, or to conceal the ultimate beneficial owner, through for example, sudden changes in the customer's ownership or control structure.



European Banking Federation's Position on Proposal for a Regulation Establishing a new AML/CTF Authority

In January 2022, The European Banking Federation ("EBF") provided feedback to the European Commission's proposed AML Package. The EBF supports the objectives of this package which aims to strengthen the fight against financial crime in Europe. In announcing its position on the package, feedback was provided by the EBF across various areas, including:

AML Authority (AMLA) Supervision:

- The EBF stressed that the criteria for the selection of entities subject to supervision from the new AML Authority (AMLA) is a key element of effective European supervision and they believe that the methodology for selecting these entities should be based on the net AML/CTF risk presented by an entity and not the inherent risk, noting that the largest entities are not necessarily the ones carrying the largest AML/CTF risk.
- The EBF believes that the scope and competencies of direct supervision of selected entities should be properly calibrated to avoid overlaps and duplications with national supervisors. The concern about duplications also includes the payment of supervisory fees. The EBF believes the current situation, with several different disconnected supervisory authorities, seems ineffective, cumbersome and expensive.
- The EBF outlined that in the case of both selected and non-selected entities, coordination between the AMLA and national supervisory authorities should be ensured in order to avoid differences in secondary legislation and supervisory fragmentation that may impede harmonisation.

Financial Intelligence Units:

- The EBF particularly welcomes the legislative efforts aimed at fostering a secure information exchange between FIUs, including through hosting FIU.net (as set out in Article 37).
- The EBF calls for entrusting AMLA with a mandate to conduct an assessment covering ineffectiveness in SAR filing processes focusing on the high false positive ratio.
- They also suggested analysing the usefulness of feedback received from FIUs.

Common Instruments:

- The EBF highlighted that the AMLA should ensure that future Regulatory Technical Standards (RTS) drafted by them do not dilute the regulatory standards already foreseen in the Anti Money Laundering Regulation (AMLR) by being too broad or imprecise in nature. The EBF believes that this could undermine the goal of the AMLR, leading to discrepancies within Member States and eventually to legal uncertainty.
- The EBF notes that further clarity would be required on how the AMLA's RTS relate to existing EBA RTS and guidelines, directly and indirectly concerning AML/CTF. This would also need to be understood with regard to the guidelines of national supervisors.
- The EBF believes that a distinction of powers needs to be drawn between the AMLA and the ECB in the context of the Supervisory Review and Evaluation Process (SREP) where AML/CTF has been introduced.

EBA launches 'EuReCA:' the EU's central database for AML / CTF

In January 2022, the European Banking Authority (EBA) launched its central database for anti-money laundering and counter-terrorist financing (AML/CTF). This European reporting System for material CTF/AML weaknesses, EuReCA, will be central to coordinating efforts by competent authorities and the EBA to prevent and counter money laundering and terrorist financing (ML/TF) risks in the Union.

EuReCA will contain information on material weaknesses in individual financial institutions in the EU that competent authorities have identified. As part of this reporting, general information will need to be provided which serves to identify the competent authority that reports the information and the financial sector operator that is the subject of the report. Competent authorities will also be reporting the measures they have imposed on financial institutions to rectify those material weaknesses.

Examples of material weaknesses include the lack of adequate AML/CTF policies and procedures including the absence of transaction monitoring at the group level and the absence of policies and procedures for high-risk customers, which increase the ML/TF risk associated with the financial institution.

EuReCA also includes internal audit findings identified by a prudential authority during an on-site inspection about which the management body of the senior management appeared to have been informed and decided not to remediate.

The EBA will use information from EuReCA to inform its view of ML/TF risks affecting the EU financial sector. It will also share information from EuReCA with competent authorities as appropriate, to support them at all stages of the supervisory process and, in particular, should specific ML/TF risks or trends emerge. In this regard, EuReCA will act as an early warning tool, which will help competent authorities to act before ML/TF risks crystallise.

EuReCA will not start to collect personal data until the approval of the draft RTs by the European Commission.



Cayman Islands added to EU AML Blacklist

On 21 February 2022, following the European Commission's proposal in January, a Commission Delegated Regulation was published, which places the Cayman Islands along with eight other jurisdiction on the EU's Anti-Money Laundering (AML) 'blacklist'. This blacklist is a list of third countries which have strategic deficiencies in their Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) Regimes. This Delegated Regulation came into force on 13 March 2022.

As outlined in the EU Risk factor Guidelines, one of the consequences of this change for individuals / entities connected to Cayman Island is that Enhanced due diligence (EDD) must be applied where a customer is established or resident in a jurisdiction on the AML blacklist, including putting in place enhanced ongoing monitoring measures.

The European Commission published a revised methodology for the identification of high risk third countries in May 2020, to ensure that a robust, objective and transparent process is applied. The methodology provides that the Commission will consider FATF lists as a starting point and complement this by an autonomous assessment of additional countries using a defined approach.

Cayman Islands were originally placed on the FATF enhanced monitoring list following the fourth round Mutual Evaluation Report in November 2018. In November 2021, FATF published a follow up report on Cayman Islands which noted that there are now no recommendations that are rated as "non-compliant" or "partially compliant". Based on the progress made, it is expected that Cayman Islands will be removed from the FATFs monitoring list at the next follow up review.



EBA alerts on the detrimental impact of unwarranted de-risking and ineffective management of money laundering and terrorist financing risks

In January 2022, the European Banking Authority (EBA) published its Opinion on the scale and impact of de-risking in the EU and the steps competent authorities should take to tackle unwarranted de-risking. Providing access to at least basic financial products and services is a prerequisite for participation in modern economic and social life. De-risking, when unwarranted, can cause the financial exclusion of legitimate customers. It can also affect competition and financial stability.

The EBA opinion describes de-risking as a situation where a financial institution takes a decision to refuse to enter into, or to terminate, business relationships with individual customers or categories of customers associated with higher money laundering / terrorist financing (ML/TF) risk, or to refuse to carry out higher ML/TF risk transactions. De-risking can be a legitimate risk management tool but it can also be a sign of ineffective money laundering (ML) and terrorist financing (TF) risk management, with at times severe consequences.

To assess the scale and impact of de-risking across the EU and to better understand why institutions decide to de-risk particular categories of customers instead of managing the risks associated with such relationships, the EBA reached out to all relevant competent authorities across the EU, as well as to external stakeholders. The EBA's findings suggest that de-risking, especially if it is unwarranted, has a detrimental impact on the achievement of EU's objectives, in particular in relation to fighting financial crime effectively and promoting financial inclusion, competition and stability in the single market.

The EBA encourages competent authorities to engage more actively with institutions that de-risk and with users of financial services that are particularly affected by de-risking, to raise mutual awareness of their respective rights and responsibilities of both institutions and their customers. The EBA is committed to following-up with competent authorities on the actions they have taken to tackle unwarranted de-risking going forward. This will inform the next EBA Opinion on ML/TF risks under Article 6(5) of the AMLD, which is due to be issued in 2023.

This Opinion complements the EBA ML/TF risk factors guidelines and the guidelines on risk-based supervision, both of which were revised and published in 2021. Further detail can be found here:

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20on%20de-risking%20%28EBA-Op-2022-01%29/1025705/EBA%20Opinion%20and%20annexed%20report%20on%20de-risking.pdf



EBA report on competent authorities' approaches to AML/ CTF supervision of banks

In March 2022, the European Banking Authority (EBA) published findings from its assessment of Competent Authorities' (CA) approaches to the Anti Money Laundering/Counter Financial Terrorism supervision of banks. Since the EBA began these reviews in 2019 and strengthened its Anti-Money Laundering and Counter Terrorism Financing (AML/CTF) guidance, national supervisors have started to adopt meaningful reforms to improve their AML/CTF supervision, but the EBA found that significant challenges remain in important areas such as the identification and assessment of money laundering and terrorist financing (ML/TF) risks.

The review covered seven CAs from seven EU/EEA Member States. The report produced by the EBA describes how CA's in this period's sample apply the risk-based approach set out in international standards, the AML Directives and AML/CTF guidelines issued jointly by the European Supervisory Authorities and the EBA. The EBA found that the CAs assessed had undertaken significant work to implement a risk-based approach to AML/CTF, noting that several competent authorities had made tackling ML/TF one of their key priorities. They also found from the reviews, that supervisory cooperation had become a clear focus for CAs in this year's sample, with mechanisms being put in place to exchange information with other relevant authorities at home and abroad such as memoranda of understanding and AML/CTF colleges.

However, CAs continued to face challenges in operationalising the risk-based approach to AML/CTF. Some of these challenges were unique to individual CA and related to, for example, geographical factors such as their sector's exposure to customers from higher ML/TF risk third countries. Other challenges were common challenges, which included difficulties relating to the identification and assessment of ML/TF risks associated with the banking sector and with individual banks within that sector, and taking proportionate and sufficiently dissuasive enforcement measures to correct AML/CTF compliance weaknesses, for example. The review team also found that cooperation with FIUs was not always systematic and continued to be largely ineffective in most Member States in this year's sample, though several competent authorities had started to take steps to address this.

Overall, while these challenges hampered the effectiveness of aspects of CAs' approaches to AML/CTF supervision, change was underway and the review team found that most CAs were on course to tackle ML/TF risks more effectively, holistically and comprehensively.



EBA concludes its Luanda leaks investigation and points to significant differences in competent authorities' responses to emerging money laundering and terrorist financing risk

In February 2022, the European Banking Authority (EBA) published its findings of its assessment of competent authorities' responses to the Luanda leaks. The leaks published in 2020 related to documents obtained by the International Consortium of Investigative Journalists (ICIJ) on the affairs of Isabel dos Santos and her associates, which indicated that financial institutions in the EU may be handling the proceeds of corruption.

The EBA found that competent authorities across the EU adopted significantly different approaches for identifying and tackling money laundering (ML) and terrorist financing (TF) risks highlighted by the leaks. These approaches varied beyond what the EBA would have expected under a risk-based approach.

The EBA found that more than half of competent authorities took action to assess the information provided by the leaks, and several subsequently identified institutions that had links with Isabel dos Santos and her associates. Conversely, some competent authorities took no action upon the release of the leaks, highlighting a possible risk that proceeds from corruption linked to these parties may not have been detected and continues to be laundered through the EU financial system. The EBA noted that few competent authorities took advantage of existing cooperation channels to exchange information and improve their understanding of the risks raised by this case.

This was the first occasion in which the EBA had used its investigatory powers to perform risk assessments of the strategies, capacities and resources of competent authorities to address ML and TF risks throughout the EU.



FCA review finds weaknesses in some new banks' financial crime controls

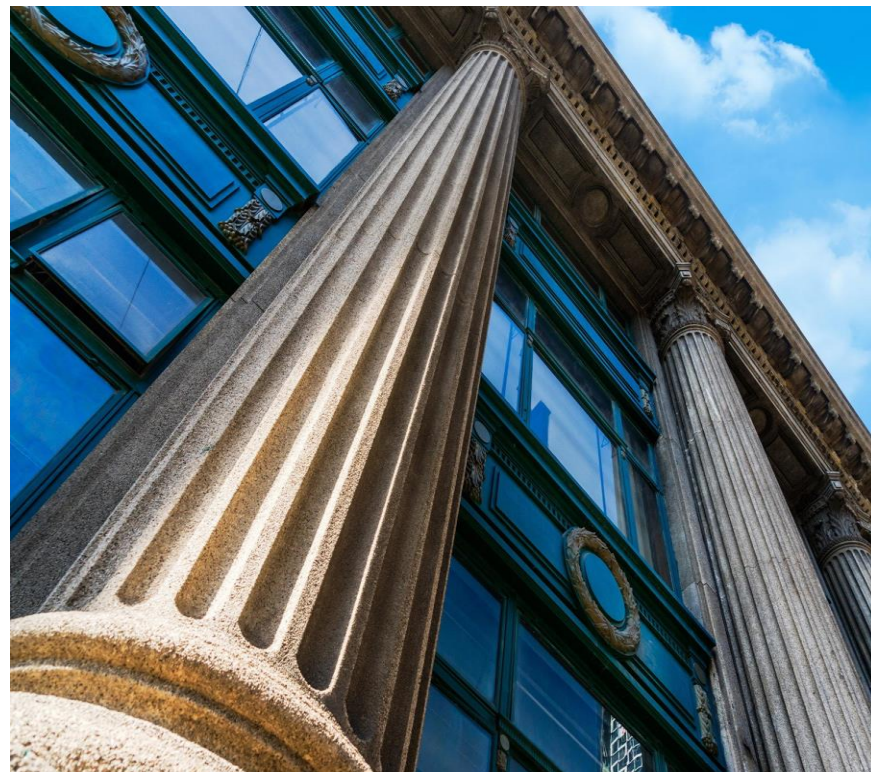
A review, published by the UK Financial Conduct Authority (FCA) in April 2022, has found that challenger banks need to improve how they assess financial crime risk, with some failing to adequately check their customers' income and occupation. In some instances, challenger banks did not have financial crime risk assessments in place for their customers.

The review, conducted over 2021, identified a rise in the number of Suspicious Activity Reports reported by challenger banks, raising concerns about the adequacy of these banks' checks when taking on new customers.

The FCA's review during 2021 found some evidence of good practice, for example innovative use of technology to identify and verify customers at speed.

The review focused on challenger banks that were relatively new to the market and offered a quick and easy application process. This included 6 challenger retail banks, which primarily consist of digital banks and covering over 8 million customers.

The Executive Director of Markets at the FCA, Sarah Pritchard, noted that "Challenger banks are an important part of the UK's retail banking offering. However, there cannot be a trade-off between quick and easy account opening and robust financial crime controls. Challenger banks should consider the findings of this review and continue enhancing their own financial crime systems to prevent harm".



GLOBAL FINANCIAL CRIME UPDATES

3

Wolfsberg Group publish guidance on Digital Customer Lifecycle Risk Management

In March 2022, the Wolfsberg Group published guidance on Digital Customer Lifecycle Risk Management. The Guidance describes the approach and challenges for Financial Institutions (FI) to effectively manage the financial crime risks associated with non-face-to-face digital engagement. In their guidance, the Wolfsberg Group outlines areas for consideration by FIs who wish to assess their digital approach to customer lifecycle risk management. These include areas such as:

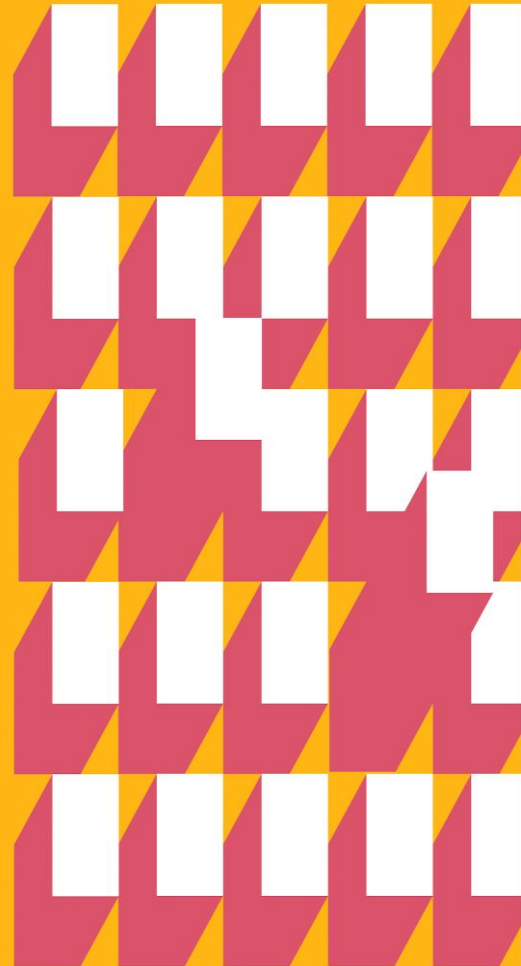
- Building a more holistic customer profile via a wider concept of identity attributes (in line with regulatory requirements);
- Leveraging the ability to detect changes and deviations in the customer profile better, so as to evolve from traditional periodic refresh cycles to a more effective trigger-based approach.
- Collaborating with governments on digital initiatives aimed at increasing access to high quality identity data, promoting interoperability, and facilitating access to financial services.

The Wolfsberg Group Guidance on Digital Customer Lifecycle Risk Management explores how non-face to-face digital engagement could be considered a standard, or even lower risk channel for an FI by further developing three core Anti Money Laundering /Counter Terrorism Financing controls:

1. Expanding concepts of identification and verification, and increasing the emphasis on the importance of authentication;
2. Building and maintaining a dynamic, more holistic customer risk profile; and
3. Shifting to a targeted, disciplined approach to on-going due diligence by refreshing customer data on a trigger (rather than periodic) basis, dedicating resources effectively to priority risks in real-time.

The guidance concludes that Technology can enable an FI to both meet customer expectations on digital engagement and prioritise resources in an effective, risk-based manner. Digital approaches to customer lifecycle risk management, if defined and calibrated responsibly, provide the FI with an opportunity to build a dynamic understanding of customer risk, refresh relevant customer information on a targeted basis, and pursue new customers without face-to-face interaction – including the financially excluded – while focusing resources to address priority financial crime threats. You can read the full Guidance paper here:

<https://www.wolfsberg-principles.com/sites/default/files/wb/Digital%20Customer%20Lifecycle%20Risk%20Management.pdf>



FATF INSIGHTS

4

Report on the State of Effectiveness and Compliance with the FATF Standards

In April 2022, FATF released their report on the “State of Effectiveness and Compliance with the FATF Standards”. This report gives a comprehensive overview of the state of global efforts to tackle money laundering, terrorist and proliferation financing, as well as results from the 4th round of mutual evaluations.

Overall, the report finds that countries have made huge progress in improving technical compliance by establishing and enacting a broad range of laws and regulations to better tackle money laundering, terrorist and proliferation financing.

In terms of laws and regulations, 76% of countries have now satisfactorily implemented the FATF’s 40 Recommendations. This is a significant improvement in technical compliance, which stood at just 36% in 2012, demonstrating the positive impact of the FATF Mutual Evaluation and Follow-up processes.

The report also highlights that many countries still face substantial challenges in taking effective action in line with the risks they face. This includes difficulties in investigating and prosecuting high-profile cross-border cases and preventing anonymous shell companies and trusts being used for illicit purposes.

The results from the report have informed the FATF’s Strategic Review, which aims to make the next cycle of FATF assessments more timely, risk-based and effective. FATF used this information to make a number of changes to how the FATF will assess countries’ actions in the 5th Round, which will include:

1. a significantly shorter mutual evaluation cycle, so that countries get assessed more frequently;
2. greater emphasis on the major risks and context to ensure that countries focus on the areas where the risks are highest; and
3. a results-orientated follow-up assessment process, which will focus on specific actions to tackle money laundering, terrorist financing and the financing of weapons of mass destruction.

The ‘FATF Methodology’ and ‘FATF Procedures’ will come into effect when the FATF commences the 5th Round of mutual evaluations and may be subject to change before the start of that next round.

The full report can be accessed here: <https://www.fatf-gafi.org/media/fatf/documents/recommendations/Report-on-the-State-of-Effectiveness-Compliance-with-FATF-Standards.pdf>

Contacts

FS Risk and Regulation - Financial Crime



Sinead Ovenden
Partner - FS Risk & Regulation
E: sinead.m.ovenden@pwc.com



Aoibheann Morgan
Senior Manager - FS Risk & Regulation
E: aolibheann.morgan@pwc.com



© 2022 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way. Please see www.pwc.com/structure for further details.