fscom
Expertise that adds value.

Brexit Planning

Whitepaper

Understanding The Anti-Money Laundering Considerations In EEA Jurisdictions

Contents

On the 23rd of June 2016, the United Kingdom voted 'Yes' to withdraw from the EU. As a result, UK- based financial services companies must consider the implications of being isolated, in some manner, from the largest customs union in the world. The following white paper aims to describe and illustrate the differing Anti-Money Laundering regimes across Europe and the unique facets each jurisdiction possesses in comparison to the MLRs 2017. Numerous areas of interest will be discussed such as CDD requirements, SAR reporting and record keeping.

The following has given careful consideration to all jurisdictions as a guide for those firms intending to establish a European entity to offset the ramifications of the United Kingdom's withdrawal from the European Union.

The following jurisdictions have been considered; Ireland, The Netherlands, France, Belgium, Germany, Luxembourg, and Lithuania. Please note, all jurisdictional legislation will be referred throughout as "[Jurisdiction] AML Legislation."

A comprehensive list of the legislation and its components is listed in the bibliography.

Overview

The following provides a brief overview of the jurisdictions that are to be covered;

Ireland

Having just recently transposed the 4th Money Laundering Directive, Ireland is making significant improvements on its AML regime. Ireland is seen as a stable and welcoming environment for upcoming firms and a suitable substitute jurisdiction given the common language shared with the UK.

The Netherlands

The Dutch implemented 4MLD in July 2018. The DNB's have recently imposed a record fine on ING Bank for various AML failings, including poor customer filings and providing inadequate resources to combat the threat of ML/TF.

Germany

The German authorities have taken a prudent approach with the implementation of 4MLD. In fact, they are the only country other than the UK thus far to have implemented the electronic online UBO register. Germany provides for an inviting post-Brexit location, with a burgeoning fintech hub in Berlin as well as Frankfurt; the emerging European Capital of Finance.

France

France's implementation of the 4MLD has been a gradual process, necessitating two implementation acts. France is stringent regarding adherence to their legislation, with the ACPR having imposed large fines to French banks such as BNP Paribas and Société Générale for significant lapses in their AML regimes.

Belgium

Belgium transposed the 4th Anti-Money Laundering Directive into national law through the Law of the 17th of September 2017. Located at the heart of the European Union and nestled between some of Europe's largest economies, Belgium would be an attractive destination for UK based firms.

Luxembourg

Recently reprimanded by the EBA for their failure to fully transpose 4MLD, Luxembourg, along with Ireland have been accused of slowly implementing the required enhancements under 4MLD. Nevertheless, they have committed to amend these shortcomings as well as ensure a robust competitive environment amongst its neighbours.

Lithuania

UK-based firms will be happy to note that the Lithuanian regime, along with Ireland, has a legally binding English version of their national law. Furthermore, the transposition of 4MLD is the most perspective and detailed of the group, ensuring that the intentions of the regulator has been clearly conveyed. Revolut are perhaps the most famous case of a UK-based firm reaching out to the Lithuanian regulators, as they have just been awarded a banking license in this jurisdiction.

Ireland

Ireland recently transposed 4MLD through the enactment of the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018 on the 14th November 2018. The updated AML law amends various provisions of the previous Statute.

The Irish AML law is closely aligned with the UK's efforts at transposition. This can be illustrated through Ireland holding the same requirements as the UK regarding the e-money exemption.

Risk Assessment

The Irish AML Legislation mandates that firms must implement a risk assessment in order to determine where resources should be focused in combating money laundering. However, firms must consider the usual requirements such as customers and products and geographical location. The Irish AML law also encourages firms to consider any other AML risk that they may perceive.

Through applying a Risk Assessment, firms must consider the purpose of the account or relationship, the level of assets to be deposited and the regularity and the duration of the transaction in order to determine the client risk profile. Furthermore, the CBI requires firms to clearly communicate both inherent and residual risks within a firm-wide framework.

Customer Due Diligence

The CDD requirements are very similar to those applied in the UK and are now in line with 4MLD with the enactment of the recent legislation.

For EDD, a higher risk of money laundering must be considered in the light of what a reasonable person would consider to be a higher ML/TF risk. The Irish AML law is also concerned with a firm's ability to implement the appropriate controls to allow for the detection of unusually large, patterned or otherwise complex transactions.

Suspicious Activity Reporting

There is an obligation, when an employee suspects or has reasonable grounds to suspect ML/TF, to report their findings to both the Garda Síochána and the Revenue Commissioners. An employee must make a report as soon as is practicable after acquiring the knowledge or forming a suspicion.

Firms may not proceed with completing the suspicious transaction unless it is impractical to stop or delay it, or if delaying the transaction in any way would result in the concerned individual becoming aware of the investigation. The authorities can also direct firms as to how to proceed with the transaction once a report has been made.

Firms wishing to apply to the CBI will not only be required to submit all necessary AML policies and procedures but will also be required to answer a specific AML Questionnaire, reference to which can be found in the Bibliography.

Record Keeping

Similar to the UK, firms must maintain records for five years following the termination of the business relationship.

The Netherlands

The De Nederlansche Bank (DNB) is the Dutch regulator and is also responsible for sanction reports. The Financial Intelligence Unit (FIU-Nederlands) is responsible for processing SARs.

The Dutch have fully implemented the 4MLD through their Implementation Decree. This, however, has not yet been fully consolidated into the main AML legislative statute.

As with most jurisdictions, the Dutch AML Legislation has been enhanced to provide greater coverage in the areas of customer due diligence and the reporting of unusual transactions.

This can be exemplified through the lowered amount that qualifies the need for CDD (€10,000 for cash payments) as well as an increase in the maximum number of fines that can be levied towards an individual (up to 20%) to deter non-compliance.

The Dutch AML Legislation also provides for a broad interpretation as to how policies and procedures must be implemented. It is stated that firms must be 'demonstratively attune,' to client risk screening, and, therefore, it is for the firms to provide evidence to the DNB.

Customer Due Diligence

CDD requirements are left for the firm to decide, so long as the verification measures are in line with international standards.

Interestingly, and what some firms may not have experienced, in the case where a natural person is acting on behalf of the client, the details of this individual must be recorded also, in line with the regulatory requirements of the client.

There is however, a prescriptive list of requirements regarding evidence to determine the source of funds. This includes details such as listing; the reason given for the source of funds, country of origin and destination, as well as a description of the product or service provided.

The Dutch AML Legislation mandates that internal procedures must be set up in a manner that allows for the constant monitoring of PEPs.

Suspicious Activity Reporting

The guidance provided for the determination and reporting of SARs is quite different than what firms are accustomed to.

The DNB Guidance provides for specific examples, within their guidance, of what employees should look out for on both an objective and subjective level. For example; subjective indicators can include the manner and behavior of the client, while objective indicators list the amount of funds presented i.e. a sum of €15,000 or more.

The Guidance also notes that employees should be mindful of their 'gut' feeling as well.

The FIU-Nederlands has an online portal for MLROs to file their SARs, with instructions as to how to register and file online.

Firms have an obligation to file the report immediately. The FIU-Nederlands must receive it no later than 14 days after the suspicion was made apparent.

Record Keeping

Similar to the UK, Dutch firms must maintain records for five years following the termination of the business relationship.

Case Study 1:
ING Group

In September 2018, Dutch bank ING, the largest bank in the Netherlands, agreed to pay €775 million in a settlement for compliance failures.

Compliance failings included missing or incomplete customer filings, a failure to exit business relationships in a timely manner, classifying customers in the wrong segments, providing a lack of resources to adequately mitigate the ML/TF threat, insufficient post-transaction monitoring and a failure to review its financial crime prevention process.

All the above failures allowed for serious breaches to occur. In fact, prosecutors are quoted as saying that, "the shortcomings identified resulted in clients having been able to use their bank accounts for, inter alia, money laundering practices for a number of years."

These findings were uncovered when the Dutch prosecutor investigated wrongdoing in four companies that held accounts with ING. Among the findings were; a $55m bribe paid to the daughter of Uzbekistan's president, a Venezuela based firm laundering $150m and a fruit-and-veg front store also used for the purposes of money laundering.

The result was another blow for the Bank as it had previously been fined $619 million for a failure to prevent sanctions breaches.

The consequences have not only been financial. Aside from the reputational impact this latest fine to ING has wrought, there have been other impacts.

The fine comes as a sign that the Dutch regulatory authorities are not hesitant to impose large fines on repeated offending. In fact, the recently implemented Dutch AML law was used to levy the fine as 10% of the Bank's annual revenue.

Also, personnel responsible for implementing the Bank's AML regime were also held to account; CFO Koos Timmermans has resigned from his position. Top executives, in a face-saving attempt, also forfeited their annual bonuses. Small acts of remediation such as these could be indicative of a wider trend in ensuring that those at the top are held accountable.

The ING case cannot be considered in a vacuum. Danske Bank are currently embroiled in perhaps the largest case of Money Laundering seen in Europe – see case Study 4.

France

The ACPR acts as the French regulator and Tracfin, the French FIU, is responsible for handling SARs.

The most recent iteration of the French AML regime came into force on 1st October and there is currently no English translation.

Customer Due Diligence

French AML legislation holds that, prior to entering a business relationship, a firm should identify and verify the client and, where applicable, the UBO/BO. Firms are obliged to practise constant due diligence throughout the business relationship.

For a natural person, firms must obtain the place of birth of the client. However, there is no obligation to provide the client's current address, an unusual facet present in the French AML Legislation. French AML Legislation sets out the methods of which a client's identification may be verified. Certain methods are unique, such as an electronic device issued as part of the French electronic verification scheme or, for a legal entity or trust, this could be an extract from the French Official Journal.

"Certain Methods are unique, such as an electronic device issued as part of the French electronic verification scheme or, for a legal entity or trust, this could be an extract from the French Official Journal"

The French AML Legislation holds that simplified due diligence may be applied whereby there is a low risk of ML/TF. This is the case when a maximum of €250 is stored electronically. Following talks at the end of 2017, ACPR aims to further reduce this to €150, with a transposition deadline of 18 months.

There is a limited amount of detail regarding EDD measures in the French legislation in comparison to other jurisdictions, the only requirements outlined expressly are sign off by the executive body regarding the continuation of the business relationship and obtainment of information regarding the origin of the assets/funds.

Reporting of Suspicious Transactions

Firms are required to report to Tracfin transactions which they know, suspect or have good reason to believe are related to ML/TF. Prior to this, however, the report must be sent to the relevant declarant/correspondent for consideration and review.

On their website, Tracfin provides a form to be completed and submitted. This can be done online, by mail or, in certain circumstances, verbally.

Tracfin may oppose the transaction for up to 10 days after receipt of the report. This timeframe may be further extended by the President of the Tribunal de Grand Instance of Paris on the request of Tracfin or the public prosecutor.

Record Keeping

Firms should maintain CDD records, transaction files and information relating to the activation, loading and use of e-money instruments for a period of 5 years.

Belgium

The Financial Services Market Authority (FSMA) is the Belgian regulator. The CTIF-CFI, the Belgium FIU, is responsible for handling SARs.The Belgian AML Legislation was adopted on the 6th of October 2017 and is unofficially translated into English.

Customer Due Diligence

The CDD regime in Belgium has several unique facets, one being that firms must identify and verify clients of which they have doubts regarding the veracity/accuracy of data that was previously obtained to identify them.

In the case of natural persons, firms are required to collect the client's place of birth whereas their current address must be obtained only to ''the extent possible''. Firms also have the discretion to increase or decrease the amount of information they collect from a client based on the ML/TF risk the client/transaction poses.

Belgian AML Legislation states that the maximum amount of money stored electronically in Belgium is €250, lower than numerous jurisdictions.

Belgian AML Legislation is less prescriptive about the risk factors to be considered when determining to apply EDD than elsewhere.

The legislation, however, lists the EDD measures that should be adopted when firms rely on third party business introducers or whereby, they establish cross border correspondent relationships with a correspondent from a third country.

Reporting Suspicious Transactions

Firms are required to report to the CTIF-CTI any transaction they know/suspect or have reasonable grounds to suspect are related to ML/TF prior to carrying out the transaction, bar certain exceptional circumstances.

The King is granted power to extend the reporting obligations set out in Belgian AML Legislation to natural/legal persons domiciled, registered or located in a country or jurisdiction whose legislation is considered insufficient or risks impeding the fight against ML/TF. On a risk sensitive basis, discretion is in place to extend these obligations.

Interestingly, the Belgian AML Legislation ensures that the staff/agent/distributor of a firm who reports an unusual transaction or reports the entity for its inability to fulfil the due diligence requirements should not face liability of any kind nor adverse discriminatory employment action.

The CTIF-CFI website has an automated online reporting system whereby firms can submit their SARs. The CTIF-CFI may take two courses of action following the receipt of these reports; it can oppose the execution of the transaction relating to the report, or may communicate to the firm, within the time it determines appropriate, any additional information it deems useful.

Record Keeping

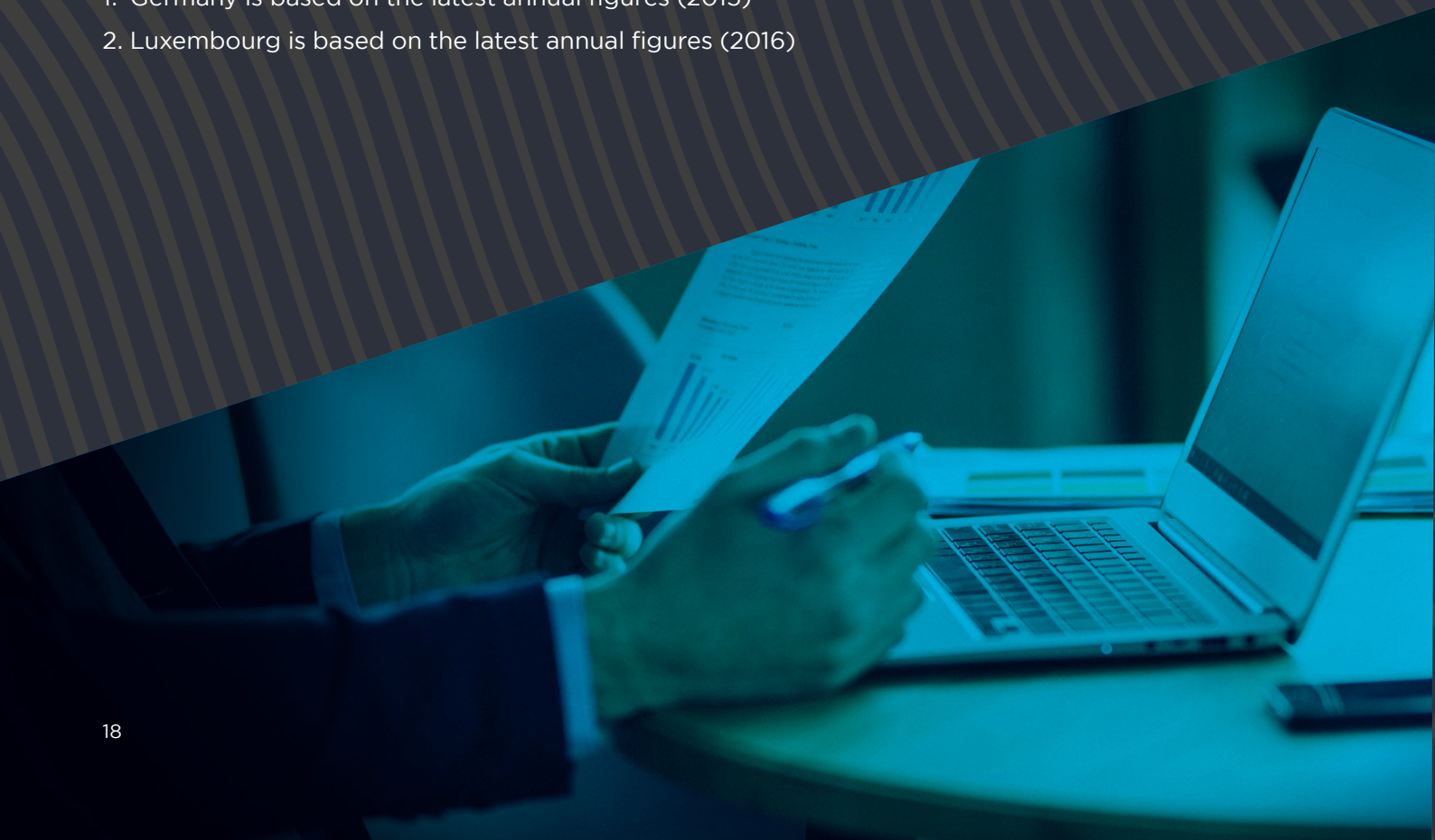
Firms should retain all relevant documentation such as identification data, transaction information and SAR reports for eight years, which is typically longer than other jurisdictions. As a matter of interest, the retention period will be increased to nine years in 2019.

The firm can substitute the retention of a copy of the records by retaining instead the reference of the records, as long as they can be produced immediately.

Case Study 2:
SAR Reports

Jurisdiction	Number of SARs reported	Number of SARs investigated	Number of SARs raised to judicial authorities
United Kingdom	460,000	–	–
Ireland	24,398	24,232	42
The Netherlands	361,015	40,456	5,898
Germany[1]	32,008	17,749	968
France	68,661	61,128	891
Belgium	31,080	10,646	1,192
Luxembourg[2]	30,710	–	545
Lithuania	833	233	23

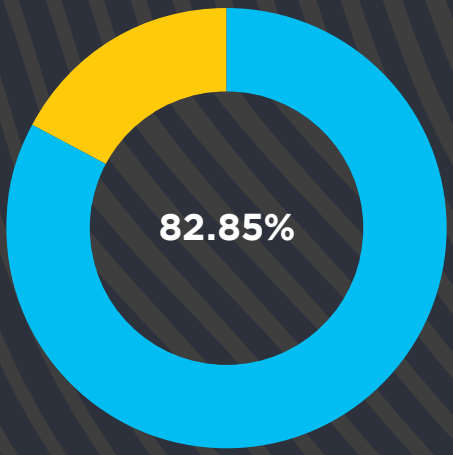
1. Germany is based on the latest annual figures (2015)
2. Luxembourg is based on the latest annual figures (2016)



Interesting facts

UK

Banking Sector is the largest submitter of UK SARs, making up 82.85% of the total received.



The UK based NCA has recorded the highest number of SARs for any jurisdiction, with a SAR database containing 2.3 million SARs.

FIU UK state that it's impossible to say how many SARs are investigated or raised to the judicial authorities as a single SAR is often used several times by several different users for different purposes. For example, the information within a SAR may inform HMRC about taxation; it may inform local police about fraud or theft; or it may inform a government department about another issue or weakness in a financial product. Plus, the SARs are retained on the ELMER database for a period of six years or until proven not to be linked to crime.

Ireland

24,398 of Irish SARs were reported to the Gardai and 24,232 were reported to the Revenue commissioner. This was double the number of SARs reported five years ago.

Luxembourg

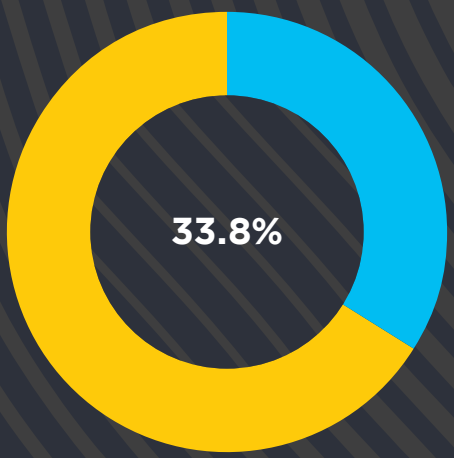
The Luxembourg-FIU saw a 17,860% increase of suspicious activity reports in 2016 compared with the year previous (contributed to electronic money and online payments).

Lithuania

More than €12m was withheld during analysis of SARs.

Belgium

Increase of 33.8% of SARs being raised to judicial authorities from the previous year.



Germany

The Federal Financial Supervisory Authority (BaFin) is the German regulator and the FIU-Germany processes SAR reports.

Customer Due Diligence

The Due Diligence requirement ensures that the individual, or the individual representing the client is identified as well as seeking clarification on the beneficial owner. Firms must take note of the client's address and nationality, or in the case of legal persons, the address of their headquarters.

Standards are in place to ensure there is consistency when verifying an electronic proof of identity and signature.

The German AML Legislation notes that 'appropriate measures,' must be implemented when conducting a business relationship with a client who poses a higher risk of ML/TF.

The AML Legislation ensures that beneficial owners are those who directly/indirectly own 25 percent of either capital or voting rights. Equally, if it can be found that an individual who exerts similar control can be classified as a beneficial owner.

The AML Legislation states that 'indirect control,' constitutes a situation when an individual controls the corresponding units that are held by association. As in other jurisdictions, where an individual cannot be identified, a legal representative or an individual involved with the firm will take their place.

The Transparency Register lists the identification details of Beneficial Owners within Germany, which includes basic information as well as details concerning the nature and extent of the BO's nature and economic interest. The register is online and available to the public.

"The Transparency Register lists the identification details of Beneficial Owners within Germany, which includes basic information as well as details concerning the nature and extent of the BO's nature and economic interest."

The FIU-Germany is an independent body tasked with collecting information related to ML/TF data and forwarding cases to the relevant public authorities for prosecution.

Suspicious Activity Reporting

According to the German AML Legislation, factual circumstances must exist for there to be a suspicion that merits escalation to an external SAR. Firms may contact the FIU-Germany through either telephone, fax or electronic communication. The FIU-Germany has provided a template for what information needs to be outlined in the SAR report. Any oral report must be completed thereafter in writing, following the guidelines of the SAR template.

A transaction cannot be completed unless the Firm has the FIU's consent or before the expiry of the second working day following the transmission date of the SAR.

The German AML Legislation also provides Annexes for indicating high and low risk scenarios. The scenarios are in line with other jurisdictions in this matter. Interestingly, the high-risk annex notes that, 'extraordinary circumstances of a business relationship,' as being high risk. This is ultimately for the Firm to decide as to what would constitute 'extraordinary.'

Record Keeping

Similar to the UK, firms in Germany must maintain records for five years following the termination of the business relationship.

Luxembourg

The CSSF acts as the country's financial regulator, with suspicious activity reports being reported to the FIU-Luxembourg. Luxembourg's process for implementing the 4MLD has been piecemeal. As a result, in November, they were referred to the Court of Justice for failing to fully transpose the 4MLD. There has been no further development on this issue at the time of writing.

"In November, Luxembourg was referred to the Court of Justice for failing to fully transpose the 4MLD. There has been no further development at the time of writing"

The AML Law states that each individual client must be risk assessed against a list of criteria upheld in the legislation. In terms of governance, firms must be able to provide evidence to the supervisory authorities that the measures implemented have been appropriate considering the Firm's risk assessment.In line with 4MLD, the AML Legislation has been enhanced to identify and verify UBOs. The AML states that where no BO can be identified, a senior manager of the firm must then be used for the purposes of identification. The Law also states that ID/V must be performed in all instances.

Customer Due Diligence

CDD must not only apply to all new clients but also to existing clients after taking into consideration the CDD measures that were performed in the first instance. This is to ensure that all the clients of the firm have been subjected to equal information gathering requirements.

Annex II of the Luxembourg AML law provides categories for firms to consider when applying CDD. This includes the level of assets being deposited, the regularity and duration of the business relationship and the subject of an account or a relationship.

Firms will have a statutory obligation to implement controls and procedures to mitigate the ML/TF risk. An independent audit function will be dependent on the size and nature of the firm.

Regarding PEPs, firms must have an appropriate system in place to identify whether a BO or Director is a PEP and it is for the firm to decide what constitutes an appropriate system.

Employees must be trained in a proportionate manner, in tandem with their Data Protection obligations.

Suspicious Activity Reporting

The obligation to report a SAR covers both knowledge or having reasonable grounds to suspect a link to ML/TF. If the circumstances indicate that blocking the transaction were to frustrate the efforts of authorities to combat ML/TF, the transaction may proceed so long as there is a submission of the necessary information immediately afterwards. The FIU provides a template on their website as well as Guidelines for submitting a SAR. Any instruction from the FIU to block the transaction is valid for 3 months. If the instruction has been received orally, it must be followed up in writing no later than three days after the oral communication.

There has been a postponement in Luxembourg's implementation of the UBO Register. The intended implementation date is in March 2019. However, the reporting obligations are detailed in the legislation and is consistent with other reporting obligations throughout Europe.

Record Keeping

Similar to the UK, firms must maintain records for five years following the termination of the business relationship.

Case Study 3:
Notable AML Fines

	Entity	Fine	Date	Failings
Ireland	Bank of Ireland (BOI)	€3.15m	30/05/17	• Inadequate assessments of risks of accounts relating to ML/TF • Failure to report 6 suspicious transactions • Insufficient CDD on overseas PEP to determine source of funds/wealth
The Netherlands	ING Croep NV	€775m	09/18	• *See above case study
Germany	Deutsche Bank	€40m	24/06/16	• Flaws in its systems designed to prevent money laundering
France	BNP Paribas	€10m	30/05/17	• Insufficient staff for spotting and notifying suspicious transactions • Insufficient tools for detecting unusual customer transactions • Delays in SARs
Luxembourg	ICBC	€3.8m	24/03/18	• Insufficient internal governance • Failure to adequately manage compliance risks relating to AML/TF and KYC
Lithuania	UAB Pervesk	€700,000	21/09/18	• Insufficient assessment of customer risk • Incomplete KYC checks • Not all UBOs established • Source of property/funds not completely ascertained

Lithuania

The Bank of Lithuania assumes the role as overseer of the country's AML regime. The Lithuanian AML legislation is the only covered jurisdiction whereby the legislation has been officially translated into English. This means that the English version of an AML regime would be legally binding in the courts, to provide expediency to any firm.

Furthermore, the language of the legislation is very prescriptive, allowing firm ease to evidence their compliance.

Customer Due Diligence

Interestingly, the AML Legislation includes a list of criteria whereby SDD can be applied. It states that all conditions must be included. Simply put, SDD can apply where the value being stored on an e-money card does not exceed €150.

Firms may be interested in one nuance held within the CDD requirements. The AML legislation states that any FX transactions amounting to over €3,000, or equivalent in foreign currency, will require CDD measures to be applied. Something for firms to be aware of, were they to choose Lithuania.

"The AML Legislation states that any FX transactions amounting to over €3, 000 or equivalent in foreign currency, will require CDD measures to be applied."

The AML Law also states that firms need to be vigilant when conducting transactions of no set value. This is to ensure that once the required amount (€10,000) is exceeded, the CDD information gathering begins immediately. Beneficial Owners must provide, amongst other information, their personal code number. A personal code number is defined as being a unique sequence of symbols intended for the identification of a person.

All information gathering requirements have been listed in the AML Law. Enhanced due diligence measures are applied, as always, under a risk-based analysis of the client. However, the AML Law also states that EDD must be applied for the following; International correspondent banking, PEPs, transactions with a high risk third country and where the risk evaluation conducted indicates a high risk.

Suspicious Activity Reporting

Suspicious transactions must be blocked and reported to the FIU-Lithuania and thereafter the FIU have 5 days to make a response. It can be determined that for those 5 days, the transaction cannot be completed.

The record keeping requirement for some documents is stronger in Lithuania than elsewhere. Firms must hold; a register of terminated customers, ID, BO data and any direct video recordings for eight years after the termination of the business relationship.

Documents confirming monetary transactions must also be kept for eight years from the date of the transaction's execution. Investigations into suspicious transactions must be kept for 10 years.

Record Keeping

Records must be kept for a period of eight years following the end of the business relationship, a more stringent timescale than the majority of jurisdictions.

Case Study 4: Danske Bank Money Laundering Scandal

In what is proving to become potentially the biggest money-laundering scandal uncovered in the EU, the situation with Danske Bank and the activities of its Estonian branch are sure to result in wide ranging implications for the enforcement of EU-wide AML governance for many years to come.

Although all the facts are yet to be determined at this point, there are several details that highlight this as an exceptional case.

Firstly, there is the sheer amount of illicit funds involved. By some estimates, as much as €200 billion could have passed through Danske Bank in the decade since they opened their Estonian Branch. The case involves not only numerous financial institutions but also several countries as well. Danske, Denmark's biggest bank, was operating an Estonian based branch to handle non-resident clients, primarily located in the former Soviet Union.

Reports have also emerged that the US subsidiary of Deutsche Bank handled around $150 billion of funds.

Furthermore, details have emerged of the use of UK-Based Scottish Limited partnerships to disguise the individuals responsible for transacting the funds. Questions have been asked of the senior management involved in decision making as concerns had been raised almost as soon as Danske acquired the Estonian Sampo Bank. Despite repeated warnings, the profit consideration proved to be too great to sway management towards enacting tighter controls.

In fact, in 2011, the Estonian Branch was generating 11% of Danske group's total pre-tax profits. At the moment, it is too early to tell what the consequences will be exactly.

However, looking forward, one can imagine that this embarrassing episode will act as an impetus for the EBA and EU-wide regulators to consider the implications of being lax with AML controls.

It is to the credit of the EU that advance plans have been made as to the transposition of both 5MLD and 6MLD into Member States legislation. 5MLD must be transposed by 10th January 2020 and 6MLD by the 3rd December of that year. Both soon-to-be Directives will tighten the net on areas such as cryptocurrency as well as introducing stronger criminal and financial penalties for those who are in breach of the regulation.

At the moment, we can only envisage that such a high profile money laundering case will only strengthen the hand of those who wish to combat money laundering and terrorist financing, and in the future financial institutions will be under a lot more scrutiny when it comes to their commercial decisions and any failure to adhere to the regulation will result in severely adverse consequences.

Conclusion

As noted above, we can see that although all EU jurisdictions were mandated to fully transpose 4MLD on the 26th of June 2017, the results have not been entirely uniform. At a cursory glance, although the main provisions are straightforward, nuances exist that are varying from one jurisdiction to the next.

There are numerous considerations that firms need to take into account when determining their post-Brexit destination.

Chief amongst the differences has been the SAR reporting regime. Firms will be required to follow the necessary timelines and report to the relevant Financial Intelligent Unit and await their instruction.

Furthermore, firms must be aware of a jurisdiction's expectations when it comes to the governance of an AML regime within their country. For example, in Germany, firms are expected to report information relevant to the inclusion of BO details for the Transparency Register.

Generally, record keeping requirements have been transposed into national law equally. Lithuania and Belgium are the notable exceptions, with a general requirement to maintain documentation for eight years and, in Lithuania's case, SAR reports must be held for ten years.

Most jurisdictions have made a commitment to implement an online UBO register by March 2019, in line with what the German authorities have instituted.

Finally, it can be said that the FCA and the broader UK AML regime have tight controls in place to mitigate and combat the threat of ML/TF. The UK authorities have received a positive report in the recently published FATF Mutual Evaluation which underlines the strong and effective AML/CTF regime in place throughout the UK. Therefore, firms are already well versed in the requirements that have been broadly set out by 4MLD and will be able to implement policies and procedures that will satisfy the authorities in each of the given jurisdictions.

"Europe-wide, UBO registers have been viewed as a means of increasing transparency. In contrast, Switzerland has declared it has no intention of implementing a register in the near future."

Glossary of Terms

4MLD	The 4th Money laundering Directive
ACPR	French Prudential Supervision and Resolution Authority
AML	Anti-Money Laundering
BaFin	Federal Financial Supervisory Authority
CBI	Central Bank of Ireland
CDD	Customer Due Diligence
CSSF	Commission de Surveillance du Secteur Financier (Luxembourg)
CTIF-CFI	Financial Intelligence Processing Unit (Belgium)
DNB	De Nederlansche Bank
EBA	European Banking Authority
EDD	Enhanced Due Diligence
FIU	Financial Intelligence Unit
FSMA	Financial Services Market Authority
Garda Síochána	Irish Police Force
ID/V	Identification and Verification
MLRs 2017	The Money Laundering. Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017
ML/TF	Money Laundering and Terrorist Financing
PEP	Politically Exposed Persons
SAR	Suspicious Activity Report
Tracfin	The Treatment of Information and Action Against Illicit
UBO/BO	Ultimate Beneficial Owner/Beneficial Owner

Bibliography

Ireland

- Guidance on the completion of the AML questionnaire; https://www.centralbank.ie/docs/default-source/regulation/how-we-regulate/anti-money-laundering-and-countering-the-financing-of-terrorism/guidance/req-guidance-final-pdf.pdf?sfvrsn=8
- Criminal Justice (Money Laundering and Terrorist Financing) Act 2010
- Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2018

The Netherlands

- Implementatieregeling vierdew anti-witwasrichtijn (Implementation Regulation of the 4th Money laundering Directive 2018)
- Algemene leidraad Wet ter voorkoming van witassen en financieren van terror isme (General guideline law for prevention of money laundering and financing of terrorism 2008) ("Wwft")
- Sanctiewet 1977 (Sanctions Act 1977)
- Regeling Toezicht Sanctiewet 1977 (Regulation on Supervision pursuant to the Sanctions Act 1977) Wetboek van Strafvordering (Code of Criminal Procedure 2012)
- Financial Intelligence Unit – the Nederlands, Annual Report 2017
- (https://www.fiu-nederland.nl/sites/www.fiu-nederland.nl/files/documenten/7238- fiu_jaaroverzicht_2017_eng_web_1.pdf)

Germany

- Geldwäschegesetz, The Anti-Money Laundering Act Strafgesetzbuch, The Criminal Code (Sections 89c and 261) Kreditwesengesetz, The Banking Act (Sections 6a, 24c and 25g to 26)
- Strafgesetzbuch, The Criminal Code (Sections 263 to 265e, fraud-related)

France

- Code monétaire et financier (Monetary and Financial Code) (Consolidated version of the 1st October 2018);
- Ordonnance n° 2016-1635 du 1er décembre 2016 renforçant le dispositif français de lutte contre le blanchiment et le financement du terrorisme (Order no. 2016-1635 of the 1st of December 2016, Strengthening French Measures against Money Laundering and Terrorist Financing);
- Décret n° 2018-284 du 18 avril 2018 renforçant le dispositif français de lutte contre le blanchiment de capitaux et le financement du terrorisme (Decree no. 2018-284 of the 18th of April 2018, Strengthening French Measures against Money-Laundering and Terrorist Financing);
- French Financial Intelligence Unit- Tracfin Annual Activity Report 2017: (https://www.economie.gouv.fr/files/ra-2017-tracfin.pdf)

Belgium

- Loi du 18 Septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (Law of the 18th of September 2017 on the prevention of money laundering and terrorist financing and on the restriction of the use of cash);
- Belgian Financial Intelligence Unit- CTIF-CFI Annual Report 2017: (http://www.ctif-cfi.be/website/images/FR/annual_report/ra2017fr.pdf)

Luxembourg

- The tax reform law of 23 December 23rd, 2016 – leading to the insertion of criminal tax offences as a predicate crime. (fraude fiscal aggravée and escroquerie fiscal)
- Bill No. 7128, February 6th, 2018: implementation of the main provisions on 4MLD
- Bill No 7208, implements the directive 2016/2258 pursuant to which national tax authorities shall be granted access to the mechanisms, procedures, documents and information referred to in Articles 13 and 30 of 4MLD
- Bill No7216: implements Article 31 4MLD pertaining to the register of UBOs Guidance published by the Commission de Surveillance du Secteur Financier
- ("CSSF"): http://www.cssf.lu/en/supervision/financial-crime/aml-ctf/additional-documentation/

Lithuania

- Republic of Lithuania: law on the approval and entry into force of the criminal code 26 September 2000 No VIII-1968.
- Republic of Lithuania: Law on the prevention of money laundering and terrorist financing, 19 June 1997 No VIII-275.
- Money Laundering and Terrorist Financing Investigation, Annual Report. (http://www.fntt.lt/data/public/uploads/2018/05/ml_tfp_activities_financial_crime_investigation_s ervice_2017.pdf).

General

- FATF Mutual Evaluation Report of the United Kingdom – 2018: http://www.fatf-gafi.org/publications/mutualevaluations/documents/mer-united-kingdom-2018.html

About fscom

fscom is a boutique firm of compliance experts who specialise in the fintech sector specifically in payments, e-money, crypto and challenger banks.

Established in 2011, fscom is headquartered in Belfast with offices in London and Dublin. fscom has experience assisting firms adhere to the regulatory requirements in multiple european jurisdictions. The team has in-depth industry knowledge from the frontline, having run businesses, headed up global compliance teams, and worked for the regulators. We are a highly skilled team of deep domain compliance experts who thrive on transferring our knowledge to compliance teams. Ultimately, this adds value to the business. And value is what we are all about. fscom has won numerous awards for its work with clients in providing advisory and project-based work across three core technical areas, financial crime advisory, regulatory compliance and cyber security.

fscom is on hand to help with any query on the regulatory requirements in a specific european jurisdiction.

Please get in touch with the team and we will be happy to assist.

Philip Creed
Director
philip.creed@fscom.co.uk

Eoin Kearns
Compliance Associate
eoin.kearns@fscom.co.uk

Melissa Hughes
Trainee Compliance Associate
melissa.hughes@fscom.co.uk

Disclaimer

Please note that this disclaimer applies to anyone who reads this White Paper. Nothing held within the White Paper gives rise to a FSCom/client relationship. Specialist legal/compliance advice should be taken in relation to specific circumstances. The contents of this White Paper are for general information purposes only. Whilst we endeavour to ensure that the information contained within the White Paper is accurate and up-to-date, no warranty, expressed or implied, is given as to its accuracy and we do not accept any liability for error or omission. We shall not be liable for any damage (including, without limitation, damage for loss of business or loss of profit) arising in contract, tort or otherwise from the use of, or inability to use the information contained within this White Paper. The current legal situation in Europe regarding Brexit, anti-money laundering legislation is subject to continuing change. If you require further information from the time of this White Paper's publication, please contact FSCom Ltd for an up-to-date statement of the relevant anti-money laundering legislation.

fscom
Expertise that adds value.

Let's start a conversation.

Have a compliance question?

+44(0)28 9042 5451

info@fscom.co.uk

fscom.co.uk

@fscom1

@fscom-limited