Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

Why Ireland for Fintech?

Overview of Certain Prudential and Conduct of Business Rules for Payment Institutions and Electronic Money Institutions

This document is an annex to the:

- Why Ireland for Fintech? (Payment Institutions) ("**API Guide**")
- Why Ireland for Fintech? (Electronic Money Institutions) ("**AEMI Guide**")
- Why Ireland for Fintech? (MiFID) ("**MiFID Guide**")
- Why Ireland for Fintech? (Virtual Asset Service Provider) ("**VASP Guide**")

This Overview document and the two 'Why Ireland for Fintech' documents are available at https://fintechireland.com/fintech-authorisations.html.

You have found the right people to assist you obtain a presence in Ireland. Peter Oakes is recognised by Chambers & Partners[1] in its Fintech 2021 and 2020 edition as a Band 1 leading fintech expert. Peter is a past member of the selection panel of the Fintech 50 Panel.

As of 31 October 2021, Ireland has more than 40 e-money and payment services firms authorised by the Central Bank of Ireland.

Why Peter Oakes (www.peteroakes.com)

[1] https://chambers.com/department/peter-oakes-consulting-fintech-49:2743:114:1:23173986

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

Peter is leading expert in fintech, including emoney, payments, crowdfunding, banking and investment management specialising in start-ups, governance, risk and compliance. Peter is a non-executive director of regulated emoney, payment services and investment services firms (investment advice and options market making). He is a former senior executive regulator in Australia (ASC/ASIC), the UK (FSA/FCA), Saudi Arabia (SAMA) and in Ireland (CBI). Between 2010-2013, Peter was appointed as Ireland's inaugural director of enforcement and financial crime at the CBI. He was one of six individuals with an international background recruited into CBI at that time to address the economic and regulatory fallout arising from Ireland's financial crisis.

During his time at the CBI he was involved in the implementation of numerous financial laws and regulations, including the regulations (PSD 1) preceding the European Communities (Payment Services) Regulations 2018 (the "**PSR**") which transposed the Directive 2015/2336 (PSD 2) into Ireland.

Since leaving the CBI in 2013, Peter has established the European services operations of Bank of America Merchant Services (including its authorisation as a PSD 2 firm with the UK FCA), led and supported numerous fintech authorisations with the UK FCA and the CBI. Peter worked on the application for a company which successfully achieved authorisation as a specialised bank with the Bank of Lithuania ("**BoL**"), including engagements with the BoL's senior director. Peter is a leading fintech and regulatory expert and the Founder of both Fintech Ireland[2] and Fintech UK[3]. Peter Oakes brings extensive practical experience and operational know-how to client instructions as well as unrivalled executive director, non-executive director and governance expertise, founded on a vast background of international regulator and central bank experience.

What is the purpose of this Overview of Certain Prudential and Conduct of Business Rules document?

Note: We have tried not to duplicate content between the guides and this document, except where the context of the issue requires it. You need to read the API Guide or AEMI Guide in conjunction with this Overview document.

[2]https://fintechireland.com/index.html
[3] https://fintechuk.com/index.html

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

In our Guides on *Why Ireland for Fintech for Payments Institutions* and *Electronic Money Institutions*, which focus on how to obtain an authorisation from the Central Bank of Ireland ("**CBI**"), we pointed out that other topics for authorised payments institutions ("**API"**) and authorised electronic money institutions ("**AEMI**") include:

- prudential supervision requirement;
- passporting provisions;
- conduct of business rules; and
- data protection.

The purpose of this document is to provide our clients and others with further information about the regulatory environment for APIs and AEMIs, particularly after they obtain authorisation. This document and our API Guide and AEMI Guide are available here https://fintechireland.com/fintech-authorisations.html

Key Prudential Requirements

Part II of the PSR which transposed the Directive 2015/2336 (PSD 2) into Ireland at sets out key prudential requirements for APIs[4]. Note that not all the PSR in this area apply to Account Information Service Providers ('AISPs') for the reason being that AISPs are not authorised but are registered by the CBI.

Capital Requirements

As noted in our API Guide, APIs have both initial and on-going capital requirements under the PSR.

Initial Capital requirement: APIs at the time of authorisation must hold a minimum level of initial capital of between €20,000 to €125,000 which is determines by the type of payment services the API provides. If you are an AEMI, the initial capital requirement is €350,000.

Own Funds requirement: Separate to the Initial Capital Requirement APIs, on an ongoing basis, must maintain sufficient capital also known as "Own Funds" to meet the applicable capital requirement under the PSRs. In broad terms, an API holds a minimum level of capital

[4] Regulations 8 - 61 of the PSR

equal to the higher of its initial capital or the capital requirement calculated in accordance with one of three methods:

- Method A – 10% of the previous year's fixed overheads (or in the first year the projected overheads);
- Method B – Formula based calculation based on the level of payment transactions in the previous year (or projected in the first year); or
- Method C – Formula based on the level of income of the payment institution.

It should be noted that every AEMI in Ireland is authorised to provide at least one, if not two, payments services. In fact as of 31st October 2021 there are two AEMIs authorised to provide 10 payment services. It seems that the CBI does not regard any payment service conducted by an AEMI to be a 'related' payment service. The view of the CBI in Ireland seems to be that at least one *unrelated payment service* must be sort by an AEMI during authorisation. Accordingly, in Ireland, an AEMI will be required to hold Own Funds of at least—

(a) the higher of—

(i) the amount required by virtue of Regulation 13 European Communities (Electronic Money) Regulations 2011 S.I. No. 183/2011 ("**EMR**") as its initial capital, and

(ii) the amount calculated—

(I) in respect of the issuance of electronic money, by Method D, and

(II) if it proposes to engage in payment services which are not related to the issuance of electronic money, by whichever of Methods A, B or C the CBI directs the AEMI, under Regulation 16(2) of the EMR, to use.

(b) if the Bank so permits under paragraph (5), the amount required by virtue of Regulation 13 EMR as the applicant's initial capital.

Method D is set out in Regulation 15 EMR and is the amount being *at least 2% of the average outstanding electronic money*.

Each API and AEMI will be directed by the CBI in its letter of authorisation about which Own Funds method is to be used. For example, an API may be directed to use Method B, while an AEMI will be directed to use Method D to calculate the amount of Own Funds in respect of the

issuance of electronic money and may be directed to use Method A (or B or C) to calculate the amount of Own Funds that the AEMI must hold in respect of its provision of payment services *unrelated to the issuance of electronic money*.

Conduct of Business Rules

In general, the legislation relevant to APIs and AEMIs for the purposes of their conduct of business rules, include:

- Statutory Instrument No. 183 of 2011 - European Communities (Electronic Money) Regulations 2011 (as amended)
- S.I. No.6 of 2018 - European Union (Payments Services) Regulations 2018
- S.I. No.255 of 2019 - European Union (Payment Services) (Amendment) Regulations 2019
- S.I. No.482 of 2016 - European Union (Payment Accounts) Regulations 2016
- S.I. No. 292/2016 - European Union (Interchange Fees for Card-based Payment Transactions) (Amendment) Regulations 2016
- S.I. No. 853/2004 - European Communities (Distance Marketing of Consumer Financial Services) Regulations 2004
- The Consumer Protection Code

APIs and AEMIs have additional responsibilities in, broadly, three key areas

- Transparency of conditions and information requirements.
- Rights and obligations in relation to the provision and use of payment services.
- Data protection, operational and security risks and strong customer authentication.

At a high level, the main points to note under each of the foregoing three key areas are:

(a) Transparency of conditions and information requirements
    - Information to be provided to the payee.
    - Information to be provided to the payer.
    - Charges for information.
    - Additional information and conditions for framework contracts.
    - Conditions imposed relating to a framework contract.

- Derogation from information requirements for certain low-value payment instruments and electronic money.
- Currency conversion.

(b) Rights and obligations in relation to the provision and use of payment services

- Charges.
- Low-value payment instruments.
- Consent and withdrawal consent by payment user.
- Availability of funds.
- Access to payment accounts.
- Customer's use of payment instrument.
- Obligations of issuers of payment instruments.
- Payer's liability for certain unauthorised payment transactions.
- Execution time and value dating.
- Derogation.

(c) Data protection, operational and security risks and strong customer authentication

- Data protection.
- Risk management.
- Strong customer authentication.
- Incident Reporting.

As noted on the CBI's website, the European Banking Authority (**EBA**) has published guidelines relating to this important area for APIs / AEMIs, including:

(i) final guidelines on security measures for operational and security risks of payments (December 2017);
(ii) final guidelines on major incident reporting (July 2017); and
(iii) updated final guidelines on fraud reporting (December 2018).

The Commission Delegated Regulation (EU) 2018/389 containing regulatory technical standards for strong customer authentication ("**SCA**") and common and secured open standards of communication, as supplemented by an opinion and a final report from the EBA were due to come into force on 14 September 2019. However the EBA released an opinion stating that a revised deadline for migration to SCA was set for 31 December 2020,

representing a 15-month extension[5]. It should be noted that in the UK payment services providers operating there have been given several extensions to implement SCA standards for e-commerce transactions. A backstop deadline for compliance of 14 March 2022 now applies[6].

Consumer Protection Code

In addition to the PSR and EMR which transpose the EU Directives on payments and electronic money into Irish law, APIs and AEMIs must be aware of the Consumer Protection Code ("**CPC**"), which is a local code and applying to regulated entities providing payment services and / or issuing electronic money in Ireland. The CPC is an extensive document, however only the following sections of the Code apply to APIs and AEMIs:

- Chapter 2, General Principles 2.1 to 2.4 and 2.7 to 2.12
- Chapter 3, General Requirements: Provisions 3.1, 3.17 to 3.23 and 3.28 to 3.45
- Chapter 4, Provision of Information: Provisions 4.7 to 4.11
- Chapter 8, Arrears Handling
- Chapter 9, Advertising: Provisions 9.1 to 9.18 and 9.30 to 9.31
- A2 [Chapter 10, Errors and Complaints Resolution, except that:
    - in the case of regulated entities providing payment services provision 10.2 (c) of the Code applies without prejudice to the rights and obligations arising pursuant to Part 4 (Rights and Obligations in relation to the provision and use of payment services) of the European Union (Payment Services) Regulations 2018 (S.I. No. 6 of 2018),
    - in the case of regulated entities providing payment services, provisions 10.9(c) and 10.9(d) of the Code do not apply to them, and
    - in the case of regulated entities providing solely account information services, provisions 10.7 to 10.12 of the Code do not apply to them.]
- Chapter 11, Records and Compliance: Provisions 11.5 to 11.10

Safeguarding User Funds

[5] https://www.eba.europa.eu/eba-publishes-report-data-provided-psps-their-readiness-apply-strong-customer-authentication-e
[6] https://www.fca.org.uk/news/statements/deadline-extension-strong-customer-authentication

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

As per Regulation 17 of the PSR and Regulation 29 of the EMR, APIs and AEMIs must have adequate arrangements in place to safeguard the funds of payment service users[7]..

There are two ways in which APIs and AEMIs may demonstrate compliance Regulation 17 PSR and Regulation 29 EMR, respectively:

i. segregation of the users' funds in the manner prescribed in an account with a credit institution or invested in assets designated or approved by the CBI as secure, liquid and low-risk assets; or
ii. users' funds are covered by an insurance policy or other comparable guarantee issued by an insurance company or a credit institution not belonging to the same group as the API, and which are payable in the event that the API cannot meet its financial obligations.

With respect to AEMIs that are engaged in payment services not related to the issuance of electronic money, the above safeguarding arrangements are broadly the same.

Outsourcing

[Note: see also Outsourcing section in API Guide and AEMI Guide at https://fintechireland.com/fintech-authorisations.html]

Regulation 30 of the PSR and Regulation 22 of the EMR set out the outsourcing requirements imposed on both by the CBI.

An intention of an API or AEMI to outsource an operational function relating to the provision of payment services or electronic money must be informed to the CBI not less than 30 days prior to the date on which it proposes to commence such outsourcing. However where the intention is to outsource an ***important*** operational function including information technology systems, such outsourcing shall not be undertaken in a manner that materially impairs the quality of institution's internal control and the ability of CBI to monitor and review the institution's compliance with the PSR or EMR as the case may be.

Furthermore, the API or AEMI as the case may be, may only outsource an *important* operational function where it meets the following requirements:

[7] Regulation 17 PSR does not apply to payment initiation or account information services

(a) the outsourcing will not result in the delegation by senior management of its responsibility;
(b) the relationship and obligations of the API / AEMI towards its payment service users or electronic money holders under the PSR / EMR will not be altered;
(c) the conditions with which the institution is to comply in order to be authorised and remain so will not be breached;
(d) none of the other conditions subject to which the institution's authorisation was granted will be removed or modified.

Recalling the maxim, *you can delegate the function, but not the responsibility* referred to in the API Guide and the AEMI Guide, APIs and AEMIs must ensure that their agents and branches inform users of their payment service / electronic money service of outsourcing in place. Both the PSR and the EMR provide that APIs and AEMIs remain fully liable for any acts of its employees, or agent, branch or entity to which its activities are outsourced.

In February 2021, the CBI issued CP138 - Consultation on Cross-Industry Guidance on Outsourcing. Closing date for submissions was 26 July 2021[8]. In April 2021, the CBI issued CP140 - Cross Industry Guidance on Operational Resilience. Closing date for submissions was 9 July 2021[9]. Both Consultation Papers are highly recommended to applicants seeking authorisation as a payments institution or electronic money institution.

Passporting of APIs and AEMI's services across the EEA

The API Guide and the AEMI Guide set out how APIs and AEMIs can passport their services. Please refer to those documents located at https://fintechireland.com/fintech-authorisations.html.

In brief, once authorised by the CBI, your API or AEMI will be able to passport to other European Economic Area countries. The EEA comprises of the 27 European Union Member States[10] plus Norway, Liechtenstein and Iceland. APIs and AEMIs may 'passport' on either a freedom of establishment or a freedom of services.

[8] https://www.centralbank.ie/publication/consultation-papers/consultation-paper-detail/cp138---consultation-on-cross-industry-guidance-on-outsourcing
[9] https://www.centralbank.ie/publication/consultation-papers/consultation-paper-detail/cp140---cross-industry-guidance-on-operational-resilience
[10] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania,

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

Fitness and Probity

All individuals being proposed by the applicant to hold a pre-approval controlled function ("**PCF**") role must complete a fitness and probity individual questionnaire ("**IQ**").

[Note: See also Fitness & Probity section in API Guide and AEMI Guide at https://fintechireland.com/fintech-authorisations.html]

IQs are submitted electronically via the CBI's Online Reporting System which becomes available after an application has been deemed to contain all the key information needed to progress to the assessment phase of the application process (see below). To fulfil a PCF role, the person must be competent and capable, honest, ethical and of integrity and also financially sound.

It is worth pointing out that:

- the CBI issued *Guidance on Fitness and Probity for a Payment Institution, Electronic Money Institution or Account Information Service Provider Under Payment Services Regulations 2018 and Electronic Money Regulations 2011* (April 2021).
    - Persons seeking approval for Pre-Approval Controlled Function (PCF) roles in a payment institution, electronic money institution, or account information service provider must comply with the requirements of the EBA Guidelines on the Information to be Provided for Authorisation and Registration under PSD2 (EBA Guidelines). The CBI has made a number of amendments to the standard Fitness and Probity IQ to reflect the requirements outlined in the EBA Guidelines.
    - The April 2021 document provides guidance on the requirements under PSR and EMR that apply to persons seeking approval for a PCF role in an API, AEMI, or AISP. Any F&P IQ submitted to the Central Bank via its Online Reporting System (ONR) must be in accordance with these requirements.[11]
- On 22 September 2021, the CBI issued a 'Notice of Intention' informing of its intention to make changes to PCFs. (See Fitness & Probity section in API Guide and AEMI Guide at https://fintechireland.com/fintech-authorisations.html)

Slovakia, Slovenia, Spain and Sweden (note that the United Kingdom left the EU on 31 December 2020 and is not part of the EEA).

[11] https://www.centralbank.ie/docs/default-source/regulation/industry-market-sectors/electronic-money-institutions/authorisation-process/guidance-note-on-completing-an-application-for-emi-pi-aisp.pdf?sfvrsn=4

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

- On 27 July 2021, the Minister of Finance announced the publication of the General Scheme of the Central Bank (Individual Accountability Framework) Bill 2021. See also Fitness & Probity section in API Guide and AEMI Guide at https://fintechireland.com/fintech-authorisations.html). CompliReg has established a specific website to assist firms understand the important obligations proposed by the IAF and SEAR which can be accessed here - https://SEARHub.com (www.sear.ie).

Anti-Money Laundering and Countering of Financing of Terrorism

Anti-Money Laundering and Countering Financing of Terrorism is an important Conduct of business rule for APIs and AEMIs. As noted in the API Guide and the AEMI Guide, on 23 April 2021, Ireland signed into law the Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Act 2021 (the "2021 Act"). The 2021 Act (No. 3 of 2021) makes several changes to the 2010 Act (No. 6 of 2010) transposing the EU 5AMLD (EU 2018/843) into national law. Please note that a refence to the CJA 2010 is a reference to the 2010 Act.

The CBI has a dedicated team focused on Anti-Money Laundering and Countering of Financing of Terrorism which sits under the Enforcement and AML Supervision Directorate.

Irish law reflects, at both European and Irish level, the recommendations made by the Financial Action Task Force, which is a specialist international organisation that concentrates on the international fight against money laundering and terrorist financing. The CBI is the competent authority in Ireland for the monitoring and supervision of financial and credit institutions' (including APIs and AEMIs) compliance with their AML/CFT obligations. The CBI is empowered to take measures that are reasonably necessary to ensure that credit and financial institutions comply with the provisions of Irish law.

Who does the CJA 2010 apply to?

Section 25 lists the types of persons classified as a "designated person" and subject to AML / CFT obligations under the CJA 2010. This includes APIs and AEMIs. Schedule 2 also sets out a list of activities which are subject to AML / CFT obligations under the CJA 2010 irrespective of the regulatory status of the entity.

Role of the CBI under the CJA 2010

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

The CJA 2010 is divided up into 5 separate parts. Part 2 addresses the various Money Laundering offences which can be committed under the CJA 2010 and Part 3 deals with Directions, Orders and Authorisations relating to Investigations under the CJA 2010. The CBI plays no role in the operability of Parts 2 & 3, as this is the remit of law enforcement and other statutory bodies.

Part 4 of the CJA 2010 sets out the role of the CBI as the Irish State competent authority in Ireland responsible for effectively monitoring credit and financial institutions' compliance with their Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations. The CBI is empowered to take measures that are reasonably necessary to ensure that designated persons comply with their obligations under the CJA 2010.

Key features of the CJA 2010

The CJA 2010 sets out legal provisions to ensure effective implementation of and technical compliance with international standards relating to AML and CFT. The CJA 2010:

- defines broadly the offence of money laundering;
- defines "designated persons" and "beneficial owners" that come under the provisions of the CJA 2010;
- sets out the "customer due diligence" (CDD) requirements which designated persons are required to apply, and the instances when they must be applied;
- establishes the requirements for designated persons to embed a risk based approach to AML/CFT, including the requirement for designated persons to complete both a business level risk assessment and customer / transaction level risk assessments;
- obliges designated persons to identify the "beneficial owner" behind a customer who is not a natural person, requiring the designated person to take measures to understand the ownership and control structure of the customer;
- requires the identification of politically exposed persons (PEPs) i.e. persons holding a prominent public position and their families or close associates;
- sets out the reporting, internal policies and procedures, training and record keeping requirements of designated persons;
- provides for the monitoring and supervision of designated persons.

Certain on-going CBI supervisory interactions with electronic money institution and payments institutions

Annual Risk Evaluation Questionnaire (REQ): Institutions selected by the CBI are required to submit a REQ in the specified format, through the CBI's Online Reporting System ('ONR'), within the time period specified on ONR. The REQ, requires institutions to input data in X number of areas: Firms Details; Governance; Risk Profile, Risk Based Approach to Monitoring, Suspicious Activities Investigations/Escalations; Reporting of Management Information; and a Statement of Compliance.

AML/CFT Minimum Supervisory Engagement Model: The minimum frequency that an institution will be required to submit a REQ is predicated on the level of ML/TF risk presented by the firm, either by virtue of its business model and/or the sector into which it falls (for further information on the frequency of submission. The diagram below sets out the Financial Sector Risk Rating for various sectors.

Table: Financial Sector Risk Rating

High	**E-Money Institutions** **Payment Institutions:** *Money Remitters* **Retail Banks**	Medium High	**Bureau de Change** **Fund Administrators/Funds** **Investment Firms:** *Stockbrokers and Trading Platforms* **Non-Retail Banks:** *Engaging in higher risk activities such as Corporate Banking, Corporate Finance, Private Banking, Corporate Trust, Treasury, Aircraft Financing, Maritime Financing and Depositary Services*
Medium Low	**Credit Unions** **Investment Firms:** *Other than Stockbrokers and Trading Platforms* **Life Insurance Firms** **Non-Retail Banks:** *Engaging in Asset Finance, Bonds, Money Market Services, Covered Banks.* **Payment Institutions:** *Other than Money Remitters*	Low	**Money Lenders** **Retail Intermediaries** **Trust or Company Services Providers:** *Subsidiaries of Credit or Financial Institutions only*

With respect E-Money Institutions and Payments Institutions (as well as Banks), the CBI has placed these institutions into High Risk Rating quadrant. Because of this High Risk Rating, Electronic Money and Payments Institutions face:

- an Inspection Cycle of once every three (3) years
- AML/CFT review meetings annually
- AML/CFT Risk Evaluation Questionnaires annually (see above)

You can read more about the CBI's supervisory role with respect to Money Laundering and Terrorist Financing at its website[12].

Filing/Reporting of Suspicious Activities: Furthermore, APIs and AEMIs, being designated persons, are required to file/report suspicious activity reports with Financial Intelligence Unit Ireland[13] and at the same time with Revenue Commissioners[14]. The requirements to report suspicious transactions is contained in section 42 of the Criminal Justice (Money Laundering and Terrorism Financing) Act, 2010 as amended.

Other Relevant Legislation

- The Criminal Justice (Terrorist Offences) Act 2005. The Criminal Justice (Terrorist Offences) Act, 2005 (the "CJA 2005") gave effect to the 1999 United Nations Convention for the Suppression of the Financing of Terrorism. The CJA 2005 created a new offence of financing terrorism and inserted a scheme through which An Garda Síochána can freeze and/or confiscate funds used or allocated for use in connection with an offence of financing terrorism or funds that are the proceeds of such an offence.
- S.I. No. 110 of 2019 - European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019. The European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2019 were introduced on the 26th of March 2019, replacing SI 560/2016. The Regulations place an obligation on companies and other legal entities incorporated in Ireland to retain adequate, accurate and up-to-date information on their beneficial owners within an internally maintained register.

[12] https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism
[13] https://fiu-ireland.ie/Home
[14] https://www.revenue.ie/en/online-services/services/register-for-an-online-service/submit-suspicious-transaction-reports.aspx

- S.I. No. 16 of 2019 - European Union (Anti-Money Laundering: Beneficial Ownership of Trusts) Regulations 2019. Similar to the above item, S.I. No. 16 of 2019 introduced on 1st February 2019 requires trustees to identify beneficiaries under the trust and maintain a beneficial ownership register.
- S.I. No. 608 of 2017 - European Union (Information Accompanying Transfers of Funds) Regulations 2017. The European Union (Information Accompanying Transfer of Funds) Regulations 2017 ("the Regulations") were introduced on the 2 of January 2018 to supplement Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 ("the Funds Transfer Regulation"). The Regulations amend and replace the previous regime (The European Communities (Information on the Payer Accompanying Transfer of Funds) Regulations 2007 (S.I. No. 799 of 2007).

Risk and Guidance

It is important for supervisors and designated persons to be aware of risk factors when conducting its risk assessment and to apply an effective risk-based approach. Risk factors can fall under categories including customer, products/services, geography and channels/distribution.

There is a range of sources where guidance on Money Laundering (ML) and Terrorist Financing (TF) risk and applying a risk based approach to supervision and preventive measures can be accessed, some of which is set out below.

CBI Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector

The CBI published Anti-Money Laundering and Countering the Financing of Terrorism Guidelines for the Financial Sector ("the Guidelines")[15] on 6 September 2019, which were revised on 23 June 2021.

The Guidelines set out the expectations of the CBI in respect of credit and financial institutions compliance with their AML/CFT obligations as set out in the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010 (the CJA 2010), following the transposition of the EU's Fourth Anti-Money Laundering Directive (4AMLD) and the EU's Fifth Anti-Money Laundering Directive(5AMLD) into Irish Law. The Guidelines also

[15] https://www.centralbank.ie/docs/default-source/regulation/amld-/guidance/anti-money-laundering-and-countering-the-financing-of-terrorism-guidelines-for-the-financial-sector.pdf?sfvrsn=9

incorporate expectations set out in previous CBI AML/CFT sectoral reports, AML/CFT bulletins, and relevant European Supervisory Authority Guidelines.

Use of electronic means to verify the identity of customers

AEMIs and APIs may rarely meet, if ever meet, their customers. A question often raised is 'What is the regulatory position about the use of electronic means to verify the identity of a customer?"

This question is addressed in part by the AML/CFT Guidelines. Paragraph 5.2.1 of the guidelines – 'Documentation and Information' – notes that evidence of identity can take a number of forms. Regulated entities (i.e. designated bodies) will be required to set out in their policies and procedures the documents and information which they are willing to accept and the circumstances under which they are willing to accept them in order to identify and verify the identity of a customer/beneficial owner. The amendment to the CJA 2010 under the Act of 2021 broadens the sources of information, which can be used by institutions to identify and verify a customer's identity to explicitly include information from relevant trust services as specified in the eIDAS Regulation. Firms must retain records evidencing identity in either paper or electronic format. Further information on the eIDAS Regulation on Electronic identification and Trust Services is located at The European Commission's website[16].

National Money Laundering and Terrorist Financing Risk Assessment

The Department of Finance and the Department of Justice and Equality have published Ireland's first ML/TF National Risk Assessment (NRA).

The NRA is an assessment of the ML/TF threats in Ireland and the vulnerabilities of certain sectors to being used for ML/TF as a result of the products and/or services they offer, their customer base, the countries in which they operate and the delivery/distributions channels they utilize. As such, the NRA is an important source for financial institutions to support and inform their own ML/TF risk assessment. The NRA can be accessed at gov.ie - National Risk Assessment - Money laundering and Terrorist Financing[17].

European Guidance on Money Laundering and Terrorist Financing Risk

ML/TF Risk Factor Guidelines

[16] https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
[17] https://www.gov.ie/en/publication/e21f7b-national-risk-assessment-money-laundering-and-terrorist-financing/

On the 1 March 2021, the European Banking Authority (the EBA) published final revised Guidelines on ML/TF risk factors[18] (the ML/TF Risk Factor Guidelines).
The revisions take into account changes to the EU Anti-Money Laundering and Counter Terrorism Financing (AML/CFT) legal framework and address new ML/TF risks, including those identified by the EBA's implementation reviews. In addition to strengthening financial institutions risk-based approaches to AML/CFT, the revision supports the development of more effective and consistent supervisory approaches where evidence suggested that divergent approaches continue to exist. The Guidelines are central to the EBA's work to lead, coordinate and monitor the fight against ML/TF. The purpose of the Guidelines is to assist firms when carrying out risk assessments and the risk factors to be taken into consideration when applying simplified and enhanced customer due diligence.

European Commission Supranational Risk Assessment Report (SNRA)

On 24 July 2019, the European Commission published its latest supranational risk assessment of the risk of ML/TF across the EU – view the report for more information[19].
View further details regarding the European Commission's work in this area[20].

High Risk Third Countries

The European Union has identified high-risk third countries with strategic AML/CFT deficiencies that are set out in Annex[21] to the Commission Delegated Regulation supplementing the 4AMLD.

The Delegated Act[22] is legally binding on member states and must be complied with by designated persons.

FATF Guidance

The Financial Action Task Force ("**FATF**") is the international standard setting body for combating money laundering, the financing of terrorism and proliferation of weapons of mass destruction. It publishes guidance that assists in the identification of ML/TF threats and

[18] https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf
[19] https://ec.europa.eu/info/files/supranational-risk-assessment-money-laundering-and-terrorist-financing-risks-affecting-union_en
[20] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-countering-financing-terrorism_en
[21] https://ec.europa.eu/transparency/documents-register/detail?ref=C(2016)4180&lang=en
[22] https://ec.europa.eu/transparency/documents-register/detail?ref=C(2016)4180&lang=en

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

vulnerabilities that assist supervisors, financial institutions and designated non-financial businesses and professions (DNFBPs) to adopt a risk based approach to supervision and applying preventative measures.

The FATF identifies jurisdictions with weak measures to combat ML/TF in two FATF public documents that are issued three times a year. The latest list of high-risk and un-cooperative jurisdictions can be found at:

FATF High Risk Jurisdictions

Improving Global AML/CFT Compliance - Ongoing Process[23]
The FATF also publishes guidance on adopting a risk-based approach.

Risk-Based Approach for the Life Assurance Sector (2018)[24]
Risk-Based Approach for the Securities Sector (2018)[25]
Guidance for a Risk-Based Approach for Money or Value Transfer Services (2016)[26]
This guidance will assist countries and their competent authorities, as well as the practitioners in the MTVS sector and in the banking sector that have or are considering MTVS providers as customers, to apply the risk-based approach to the development of measures to combat ML/TF for the MTVS sector.

Guidance for a risk-based approach: effective supervision and enforcement by AML/CFT supervisors of the financial sector and law enforcement (2015)[27]
This guidance is intended to assist countries in developing an effective supervisory and enforcement model.

Risk-Based Approach for the Banking Sector (2014)[28]
This guidance assists in the design and implementation of this approach for the banking sector, taking into account national risk assessments and the national legal and regulatory framework.

Basel Committee

[23] http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/documents/fatf-compliance-june-2017.html
[24] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Life-Insurance.pdf
[25] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/RBA-Securities-Sector.pdf
[26] http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf
[27] http://www.fatf-gafi.org/media/fatf/documents/reports/RBA-Effective-supervision-and-enforcement.pdf
[28] http://www.fatf-gafi.org/media/fatf/documents/reports/Risk-Based-Approach-Banking-Sector.pdf

Risk management guidelines related to anti-money laundering and terrorist financing issued by the Basel Committee[29]

This guidance describes how banks should include risks related to money laundering and financing of terrorism within their overall risk management framework.

Financial Sanctions and Terrorist Financing – additional obligations

To ensure compliance with Ireland's AML and CFT requirements and to prevent the financing of terrorism, credit and financial institutions including payment institutions and emoney institutions must monitor their customers and transactions against both the EU and UN Sanctions Committees lists relating to terrorism. The lists are regularly updated and must be frequently checked to ensure that they are the latest ones available.

Financial Sanctions lists that relate to terrorism should be monitored to assist in preventing terrorist financing from occurring, including, but not limited to, the following:

- EU Financial Sanctions list; and
- United Nations Sanctions Committees lists.

You can read more about the CBI's requirements on Financial Sanctions and Terrorist Financing at its website[30].

The MLRO *and* Member of Senior Management with primary responsibility for implementing, managing and overseeing compliance with AML/CFT

The term "MLRO" is not defined in Irish legislation.

The CBI will require the applicant to appoint either or both a Head of Compliance (PCF 12) and / or PCF 15 (Head of Compliance with responsibility for AML/CFT Legislation). This person must be fit and proper and be pre-approved by the CBI before he/she may commence his/her role. In terms of custom and practice, this person will often be called the "MLRO".

Like all PCF roles, the person must be competent and capable, honest, ethical and of integrity and also financially sound.

[29] https://www.bis.org/bcbs/publ/d353.pdf
[30] https://www.centralbank.ie/regulation/anti-money-laundering-and-countering-the-financing-of-terrorism/countering-the-financing-of-terrorism

Ph +353 87 273 1434
www.complireg.com / www.peteroakes.com
Email: peter@peteroakes.com

In addition, Section 54(8) of the CJA2010 (explained at para 6.3 of the AML/CFT Guidelines) provides that designated persons, such as emoney and payments institutions, shall appoint a member of Senior Management with primary responsibility for the implementation and management of anti-money laundering measures in accordance with Part 4 CJA 2010 if directed in writing to do so by the CBI for that designated person. The CBI expects institutions to appoint a Member of Senior Management with primary responsibility for implementing, managing and overseeing compliance with AML/CFT measures, where such an appointment is proportionate to the nature, scale and complexity of an institution's activities.

Where an institution has decided that it is not necessary to appoint a Member of Senior Management, having regard to the nature, scale and complexities of the institution activities, *it should record in detail its rationale for such decision*. In such circumstances, the institution must ensure that it remains in compliance with all obligations under the CJA2010. This includes ensuring that all matters requiring approval by senior management are approved at the appropriate level.

Next Steps?

Like what you have read? Contact Peter Oakes at peter@peteroakes.com (or office@complireg.com) to discuss how establishing an Authorised Payment Institution in Ireland is the wise choice and why Peter Oakes is the wise choice to assist.

This Overview document and the two 'Why Ireland for Fintech' documents are available at https://fintechireland.com/fintech-authorisations.html

See also the ***Why Ireland for Fintech?*** Guides on payment institutions and electronic money institutions at https://fintechireland.com/fintech-authorisations.html.