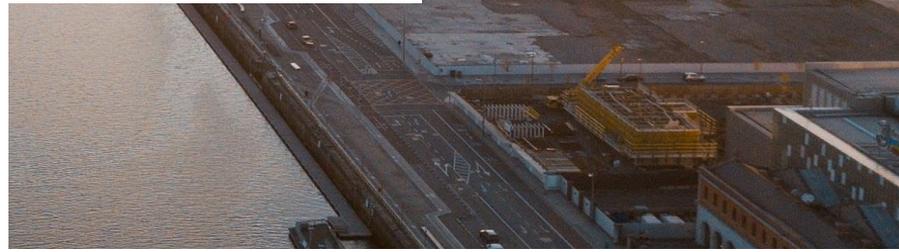
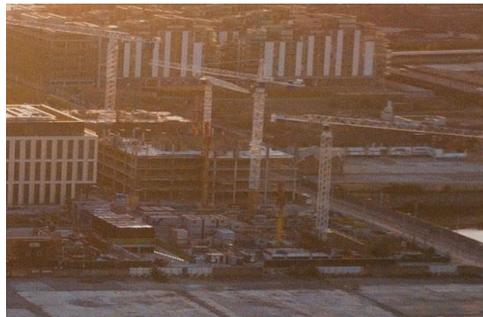


Q3 2022 Financial Crime Quarterly Update

PwC Ireland

June - August 2022



Introduction

Welcome to our Quarterly Financial Crime newsletter, which outlines all of the latest news and regulatory updates across the world of Financial Crime.

From an Irish perspective, in July, the Central Bank published a bulletin in relation to Virtual Asset Service Providers (VASPs), seeking to assist applicant firms to strengthen both their applications for registration and their Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Frameworks

While in Europe, in June 2022, the European Banking Authority (EBA) published Guidelines detailing the roles and responsibilities of the anti-money laundering and countering the financing of terrorism (AML/CFT) compliance officer and of the management body of credit or financial institutions.

In May 2022, the European Supervisory Authorities published a joint Report, which provides a comprehensive analysis on the completeness, adequacy and uniformity of the applicable laws and practices on the withdrawal of license for serious breaches of the rules on AML/CFT.

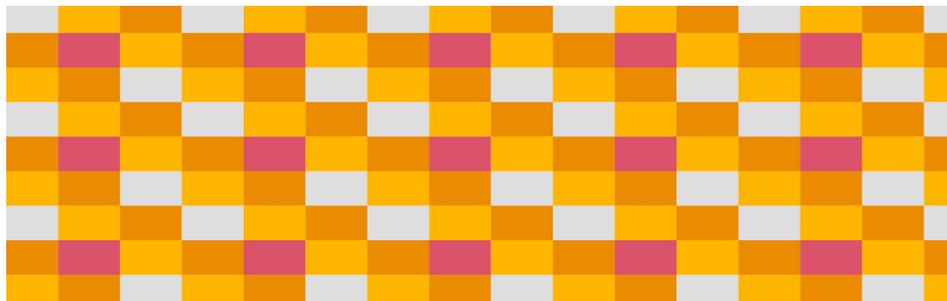
We hope you enjoy reading this newsletter, which contains further details on the issues outlined above, and more!

Sinead Ovenden

Partner, FS Risk and Regulation

Contents

- Irish Financial Crime Updates 3
 - Central Bank contacts business groups regarding Financial Sanctions obligations
 - Central Bank highlights weaknesses in Virtual Asset Service Providers' AML/CFT Frameworks
- European Financial Crime Updates 6
 - EDPB letter to the European Parliament on the protection of personal data in the AML-CFT legislative proposals
 - ESAs publish the joint Report on the withdrawal of authorisation for serious breaches of AML/CFT rules
 - EBA publishes Guidelines on role and responsibilities of the AML/CFT compliance officer
 - Crypto assets: deal on new rules to stop illicit flows in the EU
 - EBA calls for more proactive engagement between supervisors in AML/CFT colleges
- FATF Insights 12
 - AML/CFT Digital Strategy for Law Enforcement Authorities
 - FATF Releases Mutual Evaluation Reports for Germany and the Netherlands
- How PwC can help you 15



IRISH FINANCIAL CRIME UPDATES

1

Central Bank contacts business groups regarding Financial Sanctions obligations

In June 2022, against the backdrop of Russia's invasion of Ukraine, the Central Bank wrote to business and professional representative bodies to provide information to assist their members as they meet their obligations under EU Financial Sanctions

Director of Enforcement and Anti-Money Laundering, Seána Cunningham wrote "It is vitally important that Ireland plays its part in the effective implementation of sanctions to ensure that the sanctions achieve their desired goal."

The letter aims to ensure that all individuals and entities fully understand their obligations under sanctions regulations and their role in effective implementation. Where a business or individual is in possession or control of funds or economic resources of a person/entity that is subject to a Financial Sanction, that business or individual are legally obliged to:

- Freeze the funds or economic resources
- Refuse to deal with or release the funds or economic resources to the sanctioned person, unless there is an available exemption and you have obtained the required authorisation from the Central Bank of Ireland
- Report the freezing of the funds or economic resources to the Central Bank using the Sanctions Return Form.

Where an individual or entity suspects that a breach of the sanctions has or will occur it must report this to An Garda Síochána. This information can also be brought anonymously to the attention of the European Commission via the EU Sanctions Whistleblower Tool.





Central Bank highlights weaknesses in Virtual Asset Service Providers' AML/CFT Frameworks

In July 2022, the Central Bank of Ireland published a bulletin in relation to Virtual Asset Service Providers (VASPs), seeking to assist applicant firms to strengthen both their applications for registration and their Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Frameworks.

VASPs have been required to comply with relevant AML/CFT obligations under the Criminal Justice Act 2010, as amended, since April 23rd 2021. This CBI bulletin outlines key issues identified through the Central Bank assessment process, and sets out the Central Bank's expectations in relation to key AML/CFT requirements. Specifically, the Central Bank identified that in the vast majority of VASP registration applications there was a lack of understanding and compliance with key AML/CFT obligations, in addition to significant control weaknesses.

Some of the Key Central Bank observations on the VASP registrations received and assessed to date included:

- Incomplete Applications, noting that the majority of firms who did not progress to the assessment phase had not availed of the pre application meeting or had not given consideration to the CBI guidance documents;
- Not assessing or documenting the ML/TF risks as they pertain to their firm's customers and business activities;
- Not including the firm's procedures that document how the firm meets their legislative obligations;
- Not documenting the frequency of Financial Sanctions screening, how the firm screens or the actions that the firm would take in the case of a Financial Sanctions hit;
- Not including their policies around outsourcing or not submit their service level agreements.

The Central Bank advised firms that registered VASPs, as with all supervised entities, will be subject to a supervisory levy. All firms regulated and supervised by the Central Bank for AML/CFT purposes must be able to demonstrate a robust AML/CFT control framework that complies with the relevant obligations.

All current and potential VASP applicants should review the content of the bulletin and take actions to rectify weaknesses, as relevant. Firms undertaking VASP activities are also reminded that a failure to register may result in significant criminal and/or administrative sanctions.

EUROPEAN FINANCIAL CRIME UPDATES

2

EDPB letter to the European Parliament on the protection of personal data in the AML-CFT legislative proposals

In May 2022, the European Data Protection Board (“EDPB”) issued letters to the European institutions on the protection of personal data in the AML-CFT legislative proposals.

The letters draw the attention of the European institutions to a number of points, including:

- The important data protection issues raised by the implementation of the AML/CFT obligations, as provided by the AML Legislative proposals;
- Ensuring AML legislative proposals are in line with the General Data Protection Regulation (‘GDPR’).
- Ensuring a better consistency between the AML legislative proposals and the GDPR principles, such as the accuracy principle or the data minimisation principle, improving the efficiency of the implementation of the AML/CFT legal framework; and,
- The importance of involving the EDPB in the discussions on the AML legislative proposals.

Without further amendments, the EDPB is of the view that the AML legislative proposals would have a disproportionate negative impact to the rights and freedoms of individuals and would lead to significant legal uncertainty. Therefore, the EDPB further highlights the following safeguards to be included in the AML legislative proposals:

- Consultation of the EDPB in the context of the drafting and adoption of regulatory technical standards, guidelines and recommendations;
- The need to better specify the conditions and limits of the processing of special categories of data and of personal data relating to criminal convictions; and,
- The need to provide additional provisions in relation to the sources of information



ESAs publish the joint Report on the withdrawal of authorisation for serious breaches of AML/CFT rules

In May 2022, the European Supervisory Authorities (EBA, EIOPA and ESMA – ESAs) published a joint Report, which provides a comprehensive analysis on the completeness, adequacy and uniformity of the applicable laws and practices on the withdrawal of license for serious breaches of the rules on anti-money laundering and countering the financing of terrorism (AML/CFT).



The joint Report:

- Advocates for the introduction in all relevant EU sectoral laws of a specific legal ground to revoke licences for serious breaches of AML/CFT rules;
- Calls for the inclusion of assessments by competent authorities of the adequacy of the arrangements and processes to ensure AML/CFT compliance as one condition for granting authorisation or registration (for this purpose, cooperation and information exchange between prudential supervisors and AML/CFT supervisors should be ensured);
- Highlights the importance of the appropriate integration of AML/CFT issues into prudential regulation and supervision, including in the proposal for the Markets in Crypto-Assets Regulation (MiCA), currently under negotiation;
- Clarifies the nature of the decision to revoke licenses as a last resort measure, subject to a discretionary and proportionality assessment;
- Lays down uniform criteria for the notion of serious breach of AML/CFT rules, highlighting that the identification of a serious breach is subject to a case-by-case assessment by the AML/CFT supervisor; and,
- Provides a preliminary analysis of the interaction between serious breaches of AML/CFT rules and the crisis management and resolution frameworks as well as a first mapping of operational and legislative criticalities.

The report further refers to the next steps for the ESAs to stand ready to provide additional specific advice to the EU institutions, as appropriate. The full report can be found here:

https://www.esma.europa.eu/sites/default/files/library/joint_report_on_withdrawal_of_authorisation_aml_breaches.pdf

EBA publishes Guidelines on role and responsibilities of the AML/CFT compliance officer

In June 2022, the European Banking Authority (EBA) published its Guidelines specifying the role and responsibilities of the anti-money laundering and countering the financing of terrorism (AML/CFT) compliance officer and of the management body of credit or financial institutions. These Guidelines aim to ensure a common interpretation and adequate implementation of AML/CFT internal governance arrangements across the EU in line with the requirements of the EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (ML/FT).

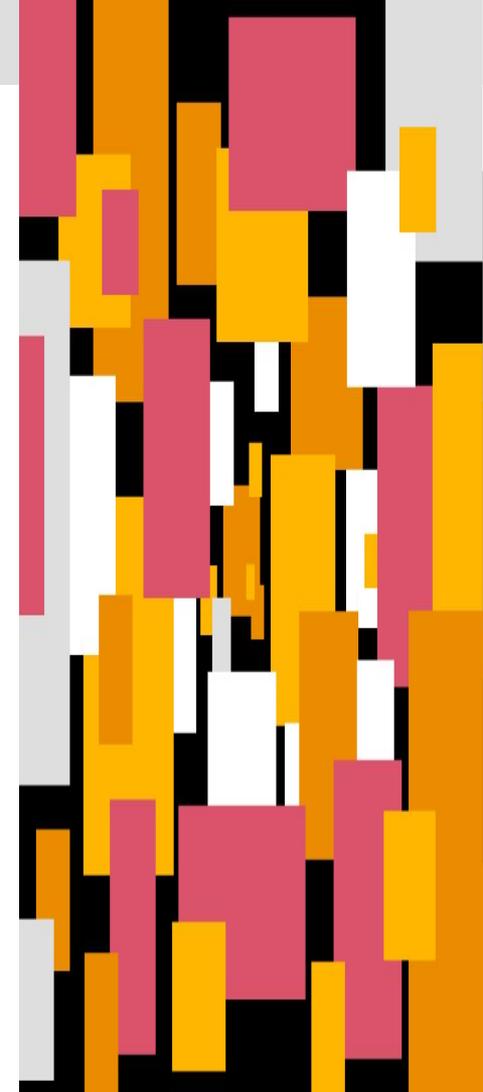
The Guidelines, which set clear expectations on the role, tasks and responsibilities of the AML/CFT compliance officer and the management body:

- Specify that credit or financial institutions should appoint one member of their management body who will ultimately be responsible for the implementation of the AML/CFT obligations and clarify the tasks and functions of that person.
- Describe the roles and responsibilities of the AML/CFT compliance officer, when this person is appointed by the management body pursuant to the proportionality criteria;
- Prescribe that, where a credit or financial institution is part of a group, a group AML/CFT compliance officer should be appointed and this person's tasks and responsibilities should be clarified;
- Aim to create a common understanding, by competent authorities and credit or financial institutions, of credit or financial institutions' AML/CFT governance arrangements.

The guidelines complement but do not replace relevant guidelines issued by the EBA on wider governance arrangements and suitability checks.

The guidelines will be translated into the official EU languages and published on the EBA website. The deadline for competent authorities to report whether they comply with the guidelines will be two months after the publication of the translations. The guidelines will apply from 1 December 2022. These Guidelines can be found here:

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-05%20GLs%20on%20AML%20compliance%20officers/1035126/Guidelines%20on%20AML%20CFT%20compliance%20officers.pdf



Crypto assets: deal on new rules to stop illicit flows in the EU

In June 2022, the European Parliament and Council negotiators reached a provisional deal on a new bill aiming to ensure that crypto transfers can always be traced and suspicious transactions blocked. The rules are part of a wider anti-money laundering (AML) package that will align with the Markets in Crypto-assets rules (MiCA).

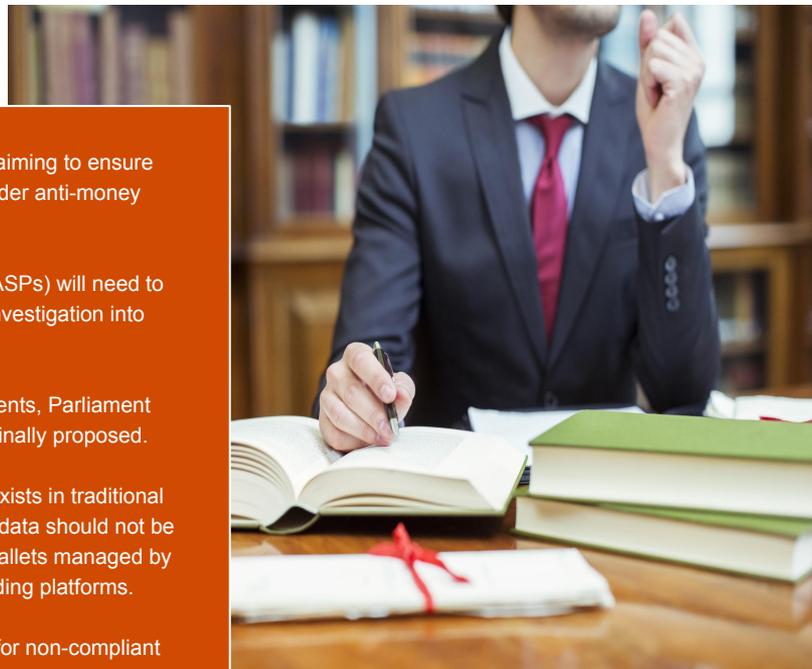
Following the agreement between Parliament and Council negotiators, crypto-asset service providers (CASPs) will need to provide information on the source of the asset and its beneficiary to competent authorities in case of an investigation into money laundering and terrorist financing.

As crypto-asset transactions easily circumvent existing thresholds that would trigger traceability requirements, Parliament negotiators assured that there are no minimum thresholds nor exemptions for low-value transfers, as originally proposed.

Regarding protecting personal data, including a name and an address required by the travel rule, which exists in traditional finance, negotiators agreed that if there is no guarantee that privacy is upheld by the receiving end, such data should not be sent. The agreement will also cover transactions from unhosted wallets, when they interact with hosted wallets managed by CASPs but does not apply to person-to-person transfers conducted without providers, such as bitcoin trading platforms.

To curb money laundering and terrorism financing, negotiators agreed that the set-up of a public register for non-compliant and non-supervised CASPs, with which EU CASPs would not be allowed to trade, will be covered in the Markets in Crypto-assets rules (MiCA), currently being negotiated.

Ernest Urtasun, co-rapporteur for ECON noted that: "this new regulation strengthens the European framework to fight money-laundering, reduces the risks of fraud and makes crypto-asset transactions more secure."



EBA calls for more proactive engagement between supervisors in AML/CFT colleges

In September 2022, the European Banking Authority (EBA) published its second report on the functioning of AML/CFT supervisory colleges in the EU. The Report finds that, although competent authorities are committed to implementing the AML/CFT colleges framework, they need to do more to ensure ongoing collaboration and proactive information exchange within colleges.

This Report sets out findings and observations from EBA staff participation in AML/CFT college meetings and from its monitoring activities. In the report, the EBA sets out its observations of good practices with an aim to help competent authorities to enhance their effectiveness in future. Recommended good practices include:

- well-structured and organized college meetings by lead supervisors;
- pro-active participation and sharing of comprehensive information by some members; and
- an effective involvement of prudential supervisors in some colleges.

The report also highlights areas for improvement. In particular, it points out that, due to their immaturity, AML/CFT colleges are not yet fully embedded in supervisory processes. The Report reminds the supervisors of the importance of exchanging information in colleges on an ongoing basis and without delay, particularly where material weaknesses in the institution's AML/CFT framework have been identified. It also emphasizes the need for colleges to be organized in a more risk-sensitive manner with more frequent meetings being held for those cross-border institutions that are exposed to higher risks of ML/TF.

The EBA encourages all supervisors to make use of the practices and observations set out in this report and adjust their approach where necessary. In 2022, the EBA will continue to monitor and provide technical support to competent authorities in this process to ensure that AML/CFT colleges function effectively and achieve their objectives.

The summary of the report can be found here:

https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1038179/Report%20on%20functionion%20of%20AML%20CFT%20Colleges.pdf

FATF INSIGHTS

3



AML/CFT Digital Strategy for Law Enforcement Authorities

In May 2022, the Financial Action Task Force (FATF) prepared a confidential report that examined how law enforcement agencies can use technology to successfully investigate money laundering and terrorist financing, mitigate the risks of these crimes and share information in a secure manner.

The summary of the report was released by FATF in June 2022, where the opportunities and requirements as well as the key prerequisites for removing the barriers to successful digital transformation were highlighted. The document also highlighted key strategic questions to be considered prior to launching digital initiatives.

A number of considerations have been posed to law enforcement agencies with respect to the use of technology for data analysis and digital investigative capabilities in the fight against financial crime such as:

- Which specific types of ML/TF crimes would benefit most from the use of technology?
- How to align with existing and foreseeable data protection, privacy, and security frameworks and legislation?
- What are the ethical considerations with the use of emerging or advanced technology?
- How can data be “sanitised” to remove potential bias and inaccuracy?
- How will key components of data be shared, and why such sharing is in line with the national AML/CFT priorities and risk profile of the country?
- Is the data to be shared available in compatible data format or structure, that will not require substantive cleaning and harmonization efforts?
- Is there a plan to verify data accuracy, or to obtain updated data to increase the relevance and value of the shared data?

The full confidential report is available to public authorities, in particular law enforcement agencies. Operational agencies may get in touch with their domestic AML/CFT coordinating agency for access to the report.

The summary of the report can be found here:

<https://www.fatf-gafi.org/media/fatf/documents/Digital-Transformation-law-enforcement.pdf>

FATF Releases Mutual Evaluation Reports for Germany and the Netherlands

In August 2022, the Financial Action Task Force (“FATF”) released mutual evaluation reports for Germany and the Netherlands. Some of the key findings from these reports are outlined below.

The Netherlands

- The Netherlands’ measures to combat ML/TF are delivering good results, but the country needs to do more to prevent legal persons from being used for criminal purposes, strengthen risk-based supervision, and ensure sanctions for ML/TF offences are proportionate and dissuasive.
- The Netherlands’ main money laundering risks are related to fraud and drug related offences, which represent 90% of all Dutch proceeds of crime.
- The country faces terrorist financing risks from religious extremism such as ISIL and other UN designated groups, but also from extreme right-wing terrorism.
- The Netherlands has a good understanding of the risks it faces and has developed robust risk-based policies and strategies to address them, but it needs to address some outstanding technical deficiencies such as the regulation of virtual asset service providers.
- There is strong cooperation between the Dutch financial intelligence unit (FIU-NL) and law enforcement agencies, who regularly use high quality financial intelligence from FIU-NL, datahubs and cooperation platforms in the course of their investigations.

Germany

- Germany has implemented significant reforms in the last five years to strengthen its system and more effectively combat money laundering and terrorist financing. Some of these new measures are already delivering results but Germany needs to continue to implement reforms and take steps to make sure that there is resourcing and prioritization at the operational level to combat illicit financial flow
- Domestic coordination across Germany’s 16 states is a challenge and coordination and consistency between the different supervisory and law enforcement authorities should be enhanced. Priority should also be given to mitigating the risks associated with the high use of cash in the country and the use of informal MVTS services.
- Germany’s transition in 2017 to an administrative FIU model has been a positive step towards improving the collection and use of financial intelligence. Priority needs to be given to the implementation of these reforms at the operational level and continue to enhance the collection, analysis, dissemination and use of financial intelligence.
- Germany faces significant terrorist financing risks and has a good track record of investigating, prosecuting and disrupting financing activity as part of a holistic approach to combating terrorism.

How PwC can help you

4



PwC Financial Services Regulatory Team

Our Financial Services Regulation Team at PwC Ireland have the experience and expertise to provide solutions that have the overarching aim of addressing new and existing financial crime threats. Get in touch to find out more on how we can help you.

Central Bank RMPs focused on AML

PwC can assist firms in navigating the many demands and challenges of completing an RMP with a selection of our services provided below:

- Design and implementation of a RMP response framework, including tracking, monitoring and reporting
- Constructing a Governance framework, that includes management and Board reporting
- Developing risk mitigation planning, implementation, and progress monitoring
- Leveraging the latest technology to assist in assessing risk and data analytics

Customer Due Diligence & ESG

Our team are experienced in designing policies and procedures for conducting ESG risk assessments, as well as identifying ESG risk:

- Leveraging our established due diligence and risk assessment process to support firms in identifying ESG risk in their customer portfolios and creating a suitable ESG framework.
- Providing access to our network of ESG practitioners consisting of Subject Matter Experts, trainers, experienced project managers and due diligence analysts.

AML Remediation Programmes

PwC is an expert in conducting large scale AML remediation programmes, achieved by:

- Designing a tailored and specific remediation plan, which includes a formalised governance framework and comprehensive resource planning.
- Providing a team of highly experienced and industry focused individuals.
- Assisting clients with the delivery of the programme, including client outreach and independent quality assurance.

AML Risk Mitigation

PwC can support your Firm in identifying and assessing your AML risk through the following:

- Business Wide Risk Assessment - identification of gaps and opportunities for improvement in AML and CFT policies, methodology and processes.
- Customer Risk Assessment process - identifying and assessing a comprehensive list of risks making up your customer's risk profile.

Target Operating Model

PwC can assist firms in transforming their Financial Crime Target Operating Model through:

- Reviewing your current FC model to identify / address regulatory gaps
- Assessing and advising on the most appropriate technology available to manage your FC risks
- Advising on your 3LOD structure to ensure that all FC activities are operating effectively, efficiently and meeting regulatory expectations

Contacts

FS Risk and Regulation - Financial Crime



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



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



Ri Drozan
Manager - FS Risk & Regulation
E: irina.drozan@pwc.com



Karolina Zugaj
Manager - FS Risk & Regulation
E: karolina.zugaj@pwc.com

© 2022 PwC. The information contained in this newsletter is for general guidance on matters of interest only. The application and impact of laws can vary widely based on the specific facts involved. Given the changing nature of laws, rules and regulations, and the inherent hazards of electronic communication, there may be delays, omissions or inaccuracies in information contained in this newsletter. Accordingly, the information on this newsletter is provided with the understanding that the authors and publishers are not herein engaged in rendering legal, accounting, tax, or other professional advice and services. As such, it should not be used as a substitute for consultation with professional accounting, tax, legal or other competent advisers. Before making any decision or taking any action, you should consult a PwC professional. While we have made every attempt to ensure that the information contained in this newsletter has been obtained from reliable sources, PwC is not responsible for any errors or omissions, or for the results obtained from the use of this information. All information in this newsletter is provided "as is", with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this information, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, merchantability and fitness for a particular purpose. In no event will PwC, its related partnerships or corporations, or the partners, agents or employees thereof be liable to you or anyone else for any decision made or action taken in reliance on the information in this newsletter or for any consequential, special or similar damages, even if advised of the possibility of such damages.

Certain links in this newsletter connect to other websites maintained by third parties over whom PwC has no control. PwC makes no representations as to the accuracy or any other aspect of information contained in other websites.

