March 2018

PRIVATE BANK BRIEFING

Issues Impacting the Private Bank Sector

Welcome to our quarterly round-up of legal and compliance issues impacting private banks and their clients.

In This Edition

Advice: FCA Policy Statement on Personal Recommendations on Retail Investments

On 23 February 2018, the FCA published a Policy Statement with new perimeter guidance on what amounts to a personal recommendation in relation to advising on retail investments. The guidance came into effect on the same day.

This new guidance follows the narrowing of the scope of what amounts to "regulated advice" from 3 January 2018. The narrower definition means that most regulated firms are exempt from the need to hold a permission to advise on investments, unless the firm is providing a "personal recommendation". If a firm is authorised to advise on investments, it will not need to comply with the detailed regulatory rules around giving advice, unless providing a personal recommendation.

Firms had voiced concerns that they were deterred from providing services that help customers make their own investment decisions by offering guidance, information and support, because of uncertainty about whether such services might amount to regulated advice. The guidance is therefore intended to make it easier for regulated firms to provide more advanced guidance services to customers without needing permission to advise on investments, or without triggering the usual regulatory obligations associated with providing advice (such as suitability).

The guidance may be particularly helpful for private banks wishing to set up non-traditional offerings, such as web-based services and "robo advice".

Private banks should:

- Update policies and procedures to reflect the new boundaries
- Update any practical guides provided to employees who give advice
- Train advisors on the new boundaries
- Consider whether additional services, which were previously considered to constitute regulated advice, can now be offered to customers

Private banks should also note that in 2019 the FCA will be reviewing the advice market as part of its review of the implementation of the Financial Advice Market Review, and the next phase of the post-implementation review of the Retail Distribution Review.

> "The aim of our new Guidance is to give firms greater confidence that they can, among other things, inform a customer that they have not increased their pension contributions over a long period of time, warn a customer about any adverse consequences of a transaction they propose to make, or offer products designed to meet a particular investment objective without necessarily making a personal recommendation".
>
> FCA

Product Governance: Preparing for the Spotlight

There is a working assumption that the FCA will launch a thematic review into firms' implementation of the MiFID II product governance regime before the year is out. For many private banks, implementation presented a challenge in terms of how to anticipate the regulator's expectations and how to interpret proportionality. There is also ongoing learning in relation to how different manufacturers define their target market for similar products, and the frequency and detail of the distributor feedback expected.

Monitoring the FCA's messaging in this area remains important and the latest publication, aimed at retail banks, contains the following messages:

> "The most effective product governance frameworks focused on delivering good customer outcomes during all stages of the product lifecycle, from design to review. In these cases, firms set the measures of customer outcomes at the design stage and used them to assess continuing performance".
>
> FCA

Good practice

- Actively seeking client feedback, both for existing and new products and services
- Reviewing a range of client and commercially-focused Management Information to help identify potential conduct risks
- Senior management providing a positive "tone from the top", encouraging a focus on clients and conduct
- Contacting clients to let them know when product events occur

Bad practice

- Weak product review processes that fail to identify (and record) lessons or risks
- Unclear terms and conditions and other product information about early redemption rights
- Failing to test customer understanding (see PCBS recommendations about testing customer understanding and FCA Thematic Review on Customer Understanding)

Data Protection: GDPR Implementation Date Fast Approaching

The General Data Protection Regulation (GDPR) comes into force on 25 May 2018, and private banks need to ensure they are ready to comply. GDPR makes a whole host of enhancements to the data protection regime, including for example giving individuals more control over their personal data, requiring data controllers to be more transparent about how they use data, and substantially increasing the level of fines that may be imposed for non-compliance.

Key aspects that private banks should consider to ensure they are prepared include:

- **Record of processing**: GDPR requires a record of processing, including certain information about a controller's processing activities, to be prepared and maintained. This record needs to be prepared in time for 25 May.
- **Legal basis for processing**: many businesses currently rely on consent as the legal basis for processing personal data. However, under GDPR it will become much more difficult to rely on this basis, and so data controllers need to consider which legal bases they may soundly rely upon going forwards.
- **Data subject rights**: various new data subject rights apply to individuals under GDPR (such as the "right to be forgotten"). These differ based on the legal basis for processing, and so businesses need to be clear as to which specific data subject rights apply. They also need to ensure that they can act upon these rights (for example, that data can be erased to give effect to the right to be forgotten).
- **Updating notices**: businesses need to update their privacy notices (information that tells individuals how their personal data will be used by the controller) accordingly to reflect the more prescriptive requirements under the GDPR.
- **Incident response policy**: businesses will need to have processes in place to make sure they can comply with new requirements, such as notifying breaches to the authorities within 72 hours whenever feasible.

Although a recent joint statement issued by the FCA and the Information Commissioner's Office acknowledges that some uncertainties remain about the regime and its implementation by financial services firms, the statement stresses that the FCA believes the GDPR is compatible with the rules in the FCA Handbook. The messaging indicates that the FCA expects firms to be ready by 25 May, and firms must be able to produce evidence to demonstrate the steps that they have taken to comply. The FCA views GDPR compliance as a board-level responsibility, so private banks need to make sure that it is receiving sufficient attention at the right level.

PRIIPs: Tackling Ongoing Uncertainties

Performance scenarios

The FCA published a statement on its website in relation to concerns raised about the performance scenarios in PRIIPs KIDs on 24 January 2018. In the statement, the FCA explains that the KID is required to be accurate, fair, clear and not misleading. The statement also highlights that directly applicable EU legislation, in the form of the PRIIPs Regulatory Technical Standards, sets out how information in the KID should be calculated.

The FCA is aware of the wider industry concern that the "performance scenario" information required in the KID may appear too optimistic and so has the potential to mislead consumers. This places firms in a conflicted position as regards their obligations in relation to clear, fair and not misleading communications, and also their obligation to act honestly, fairly and professionally, in accordance with the best interests of their clients. Therefore, the FCA states that where a PRIIP manufacturer is concerned that performance scenarios in their KID are too optimistic, such that they may mislead investors, the FCA is comfortable with the firm providing explanatory materials to put the calculation in context and to set out their concerns for investors to consider. Firms and industry bodies are now collectively considering how to clarify performance scenario data in the KID.

Bonds

The applicability of the PRIIPs KID Regulation to bonds continues to be the source of an extensive lobbying effort as firms seek further guidance on what can and cannot be traded with a retail client, without a KID. The stance of European regulators seems relatively clear — that a corporate bond that meets the definition of a PRIIP requires a KID. However, the grey area arises in relation to bonds, with otherwise fixed rates of return, that contain (often investor protection driven) clauses such as make wholes or change of controls, which cause a calculation of return by reference to an underlying asset in the case of an early redemption event.

Pending any clarificatory guidance from from the European Securities and Markets Authority (ESMA), many issuers are restricting sales of these instruments to retail rather than take on the regulatory burden of producing the KID. This has forced many private banks to consider the legal and regulatory risks associated with producing KIDs for third party issued debt in order to continue to be able to service their clients.

Suitability Assessments: Sustainability Preferences

One to note for the next documentation review cycle: the European Commission will amend the relevant MiFID II delegated acts in Q2 2018 to ensure that sustainability preferences are taken into account in the suitability assessment. Based on these delegated acts, the Commission will invite the European Securities and Markets Authority (ESMA) to include provisions on sustainability preferences in its guidelines on the suitability assessment, to be updated by Q4 2018.

This was flagged in the EU's action plan on sustainable finance, released on 8 March 2018, which laid out action points to re-orient European capital markets to long-term sustainable investment.

"*By providing advice, investment firms and insurance distributors can play a central role in reorienting the financial system towards sustainability ... those firms should ask about their clients' preferences (such as environmental, social and governance factors) and take them into account when assessing the range of financial instruments to be recommended, i.e. in the product selection process and suitability assessment*".

Firms should note that this will also need to be reflected in the **product governance** process.

AIFMD: European Commission Proposals on Cross-Border Distribution of Funds

The European Commission has published legislative proposals regarding the cross-border distribution of funds within the EU, which (if implemented), will amend both the UCITS and AIFMD frameworks. This comes as part of the wider Capital Markets Union initiative.

Of particular note, the proposals suggest adding a definition of "pre-marketing", in order to clarify when an EU-authorised AIFM can conduct early stage marketing of an AIF in another Member State without being required to make a formal passporting notification.

> *"As the AIFMD does not contain a definition of pre-marketing at present, Member States have imposed their own definitions. This has led to divergent approaches across the EU, and has made marketing on a cross-border basis a rather confusing and inefficient endeavour".*

While the proposed definition would apply only to EU AIFMs (the purpose of this initiative being to remove cross-border marketing inefficiencies within the EU, not between the EU and third countries), it is clearly indicative of what the European Commission considers should constitute legitimate pre-marketing. Therefore, it may serve more broadly as guidance in this respect for non-EU AIFMs too.

The proposed definition of pre-marketing is: "*a direct or indirect provision of information on investment strategies or investment ideas by an AIFM or on its behalf to professional investors domiciled or registered in the EU in order to test their interest in an AIF which is not yet established*".

The Commission has noted that such information should not amount to "*a prospectus, constitutional documents of a not-yet-established AIF, offering documents, subscription forms or similar documents whether in a draft or final form allowing investors to make an investment decision*".

Although greater clarity in this area is to be welcomed, the proposed definition would greatly reduce the sorts of early stage marketing activities that can be undertaken in many jurisdictions.

At present, the European Commission expects the proposals to be adopted before the European Parliament elections in 2019. Consequently, the application of this new definition to non-EU AIFMs will be something UK AIFMs will be watching closely in the context of Brexit.

Client Money: FCA Policy Statement on Client Money and Unbreakable Deposits

From 22 January 2018, firms have been permitted to place client money into unbreakable term deposits of not more than 95 days, increased from (the original) 30 days.

This was confirmed in the FCA's Policy Statement published on 22 January 2018, and is implemented via amendments to CASS 7.13.

There are a number of obligations with which firms must comply when using term deposits of 31 to 95 days, including:

- Producing a written policy governing the use of these accounts, which must be included in the CASS resolution pack
- Providing clients with written explanations of the risks that arise as a result of the longer notice period for withdrawals
- Additional record keeping obligations

Cybercrime: Building Cyber Resilience

Cyber resilience is a relatively new area of focus for the FCA, and a recent speech outlined some clear FCA expectations in terms of firms protecting themselves against cyber-attacks.

> *"The speech highlights that, while the FCA appreciates that attacks will happen, it wants to see resilience from firms".*

This means firms being able to protect themselves from most attacks, successfully identify threats, and recognise where their vulnerabilities lie (including understanding what their key assets are, so they know what to prioritise if targeted). In the event of an attack, firms will be expected quickly to contain any disruption, restore lost service, and protect vital data.

An important point emphasised in the speech is that "good cyber hygiene" is both about having the right technology and having good governance. Discussions around cyber resilience should not be left to IT specialists, but need to take place at board level. The importance of cyber resilience also needs to be understood across the business as a significant risk to the operation of the firm, its customers and wider markets.

Private banks need to make sure they are thinking ahead, and have the right processes and controls in place. Crucially, they need to ensure they understand what to protect, how they can swiftly detect an attack, and how they can respond and recover.

FCA Expectations of Chairs

In a recent high-profile enforcement case, the FCA took the opportunity in the Final Notice to set out explicitly its expectations of Chairs.

The FCA emphasises that: "*The Chair of a bank holds a special position of trust and influence. Their honesty, integrity and reputation, as well as their competence and capability, can have a significant impact on their bank and upon confidence in the wider financial services industry. The standards expected of Chairs are therefore necessarily of a high order*".

The FCA also stresses what the role of a Chair must entail: "*In particular, the Chair plays a central role in facilitating the important support and challenge by the Board of management, and has a responsibility to demonstrate high standards of integrity, probity and ethical leadership*".

> This is significant because it is the first time that the FCA has made such statements, and so firms (and Chairs) should take note of the high standards expected.

TechTrends: The Global ICO Trend — What Do Private Banks Need to Know?

Given the fast pace of change of the global regulatory landscape in relation to crypto as an asset class, most firms are still in “wait and see” mode when it comes to deciding how to service their clients’ potential needs in this area. However, the continued pressure on the private bank community to deliver solutions to a client population focused on FinTech and ease of access (some of whom may themselves be Bitcoin millionaires), means firms should start to get to grips with the regulatory environment impacting the crypto world. Ultimately, private banks will need to decide whether they will be prepared to advise on, manage, or arrange the custody of crypto, or even whether they will allow third parties to rely on their KYC when clients are seeking to open a crypto wallet.

What Is Crypto?

There are two primary forms of crypto participation: (i) an Initial Coin Offering (ICO) by an individual issuer; and (ii) the subsequent trading of those coins on third party hosted platforms (akin to a secondary market).

Crypto breaks down into two broad categories: currency and securities. Many global regulators have confirmed their view that crypto securities can fall within scope of the regulations applicable to other types of financial instrument.

CRYPTO CURRENCIES

AML
Cash transactions in goods / services over £10,000 are in scope of MLD4

Crypto exchanges and custody wallet providers in scope of MLD5.

Available KYC solutions — selfie based OR reliance (with consent) on a third party financial institution

PSD
Transferring the cash leg of crypto payments to a third party who is a money transmitter amounts to a payment service

CRYPTO SECURITIES

Regulatory permissions
To arrange deals; advise on; manage or execute transactions in securities

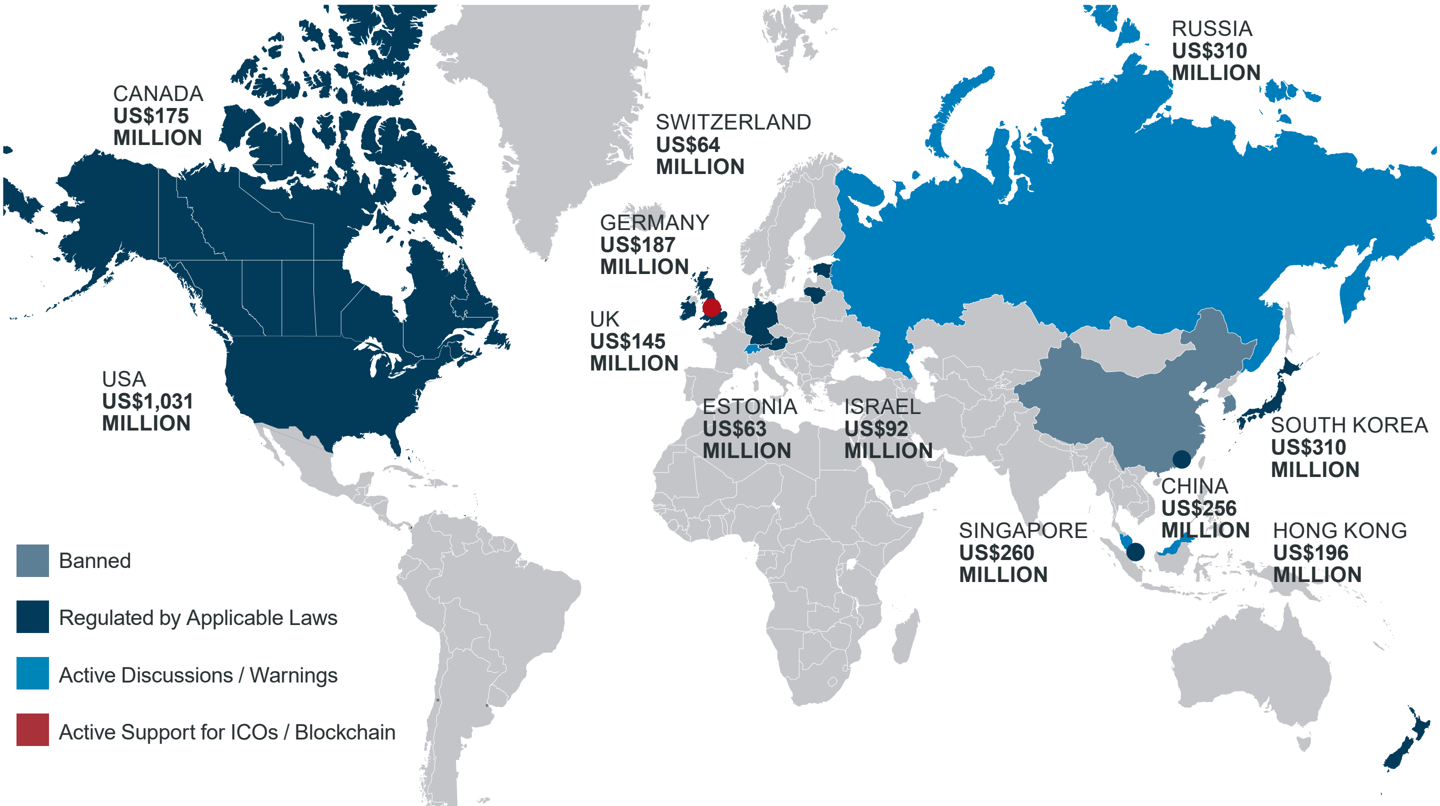
Client agreements
To capture services specifically related to crypto securities

Regulatory responsibilities
Product governance — due diligence issuers

PRIIPs KID — investigate the nature of the securities

Custody arrangements — are wallet providers appropriately licensed?

Access to platforms — are platform providers appropriately licensed?



**Data Source: EY research - initial coin offerings (ICOs) December 2017*

Global Developments

Regulators in the UK, Germany, Switzerland, Hong Kong, Singapore, and the US have all indicated that ICOs involving crypto securities are likely to need to comply with existing securities laws. However, most leave responsibility for characterising the token and identifying the applicable regulatory obligations solely to ICO participants. In the UK, the FCA is still deliberating how to address ICOs, although HM Treasury has said it will collaborate with the Bank of England and the FCA to form a crypto assets task force. The German regulator has issued some guidance for participants, but the Swiss regulator has gone much further by actually offering ICO participants assistance with understanding the regulatory position (for a fee).

For the time being, most jurisdictions seem to be trying to apply existing laws and regulations to ICOs. In contrast, jurisdictions such as Gibraltar and Belarus have announced plans to create specific regulatory regimes tailored to ICOs. Other jurisdictions such as China and South Korea take a more restrictive approach and have banned ICOs entirely.

In the US, regulators are becoming increasingly wary of the sharp increase in ICO activity. The SEC in particular continues to send strong messages to the market by issuing statements and taking enforcement action when it believes that securities laws have not been properly complied with. Most recently, the SEC has focused on the position of crypto trading platforms.

Outlook

In a recent speech, Mark Carney considered the advent of crypto, explaining that regulators need to decide whether to isolate, regulate, or integrate crypto currencies and assets. A key dilemma for regulators is that lack of regulation may leave consumers and markets exposed, while regulation may lend crypto-related activities some perhaps unwarranted credibility or legitimacy. One thing that many regulators acknowledge is that given the global nature of crypto activities, discussions should be held at a global level in order to try to achieve a coordinated approach. Consequently, talks on crypto are planned for this year's G20 meetings.

Lessons from Enforcement: US Secondary Sanctions and Their Applicability to Non-US Banks

EU banks and financial institutions need to be particularly vigilant in ensuring compliance with all applicable sanctions laws. These include not only EU sanctions and US primary sanctions — which are applicable particularly where transactions involve US persons or are denominated in US dollars — but also US secondary sanctions.

The US secondary sanctions relating to Russia, principally contained in the Countering America's Adversaries Through Sanctions Act (CAATSA), are often overlooked. This legislation added to US primary sanctions by targeting foreign (*i.e.*, non-US) persons that engage in certain categories of activities or transactions that are not otherwise covered by US primary sanctions.

Activities targeted by CAATSA include investments "that directly and significantly contribute to the enhancement of the ability of the Russian Federation to construct energy export pipelines", engaging in a "significant transaction" with a person that is part of or operates for or on behalf of the Russian Government defence or intelligence sectors, and the "facilitation" of "a significant transaction or transactions, including deceptive or structured transactions, for or on behalf of any person subject to sanctions imposed by the United States".

Non-US persons that engage in a specified activity under CAATSA may be subject to various sanctions, included denial of access to over US$10 million credit from any US financial institution.

European and other non-US banks accordingly need to take care to comply with these sanctions in any dealings related to Russia.

Global Insights — Switzerland

The current expectation is that the proposed new Swiss legislation on financial services and on the supervision of financial institutions, which is currently making its way through the legislative process, is unlikely to come into force before 1 January 2020. The proposed Financial Services Act and Financial Institutions Act would bring aspects of Swiss regulation into line with MiFID II and the PRIIPs Regulation.

What to Look Out for in Q2 2018

- FCA expected to publish an update on its strategic review of retail banking business models
- FCA expected to publish a Policy Statement to CP17/37, its Consultation Paper on Industry Codes of Conduct and Discussion Paper on FCA Principle 5
- Expected adoption of MLD5 (an 18-month transposition period is anticipated)
- FCA Business Plan and Risk Outlook to be published on 9 April, setting out supervisory priorities for the next year
- First enforcement case under the SMCR anticipated

Latham & Watkins
99 Bishopsgate
London EC2M 3XF

CONTACTS

Nicola Higgs
+ 44.20.7710.1154
nicola.higgs@lw.com

Becky Critchley
+44.20.7710.4519
becky.critchley@lw.com

Charlotte Collins
+44.20.7710.1804
charlotte.collins@lw.com

LW.com

Beijing
Boston
Brussels
Century City
Chicago
Dubai
Düsseldorf
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Moscow
Munich
New York
Orange County
Paris
Riyadh*
Rome
San Diego
San Francisco
Seoul
Shanghai
Silicon Valley
Singapore
Tokyo
Washington, D.C.

*In cooperation with the Law Office of Salman M. Al-Sudairi

LATHAM & WATKINS