REGULATORY ESSENTIALS 2020: FINANCIAL CRIME AND FINANCIAL SERVICES

Michelle de Kluyver, Partner

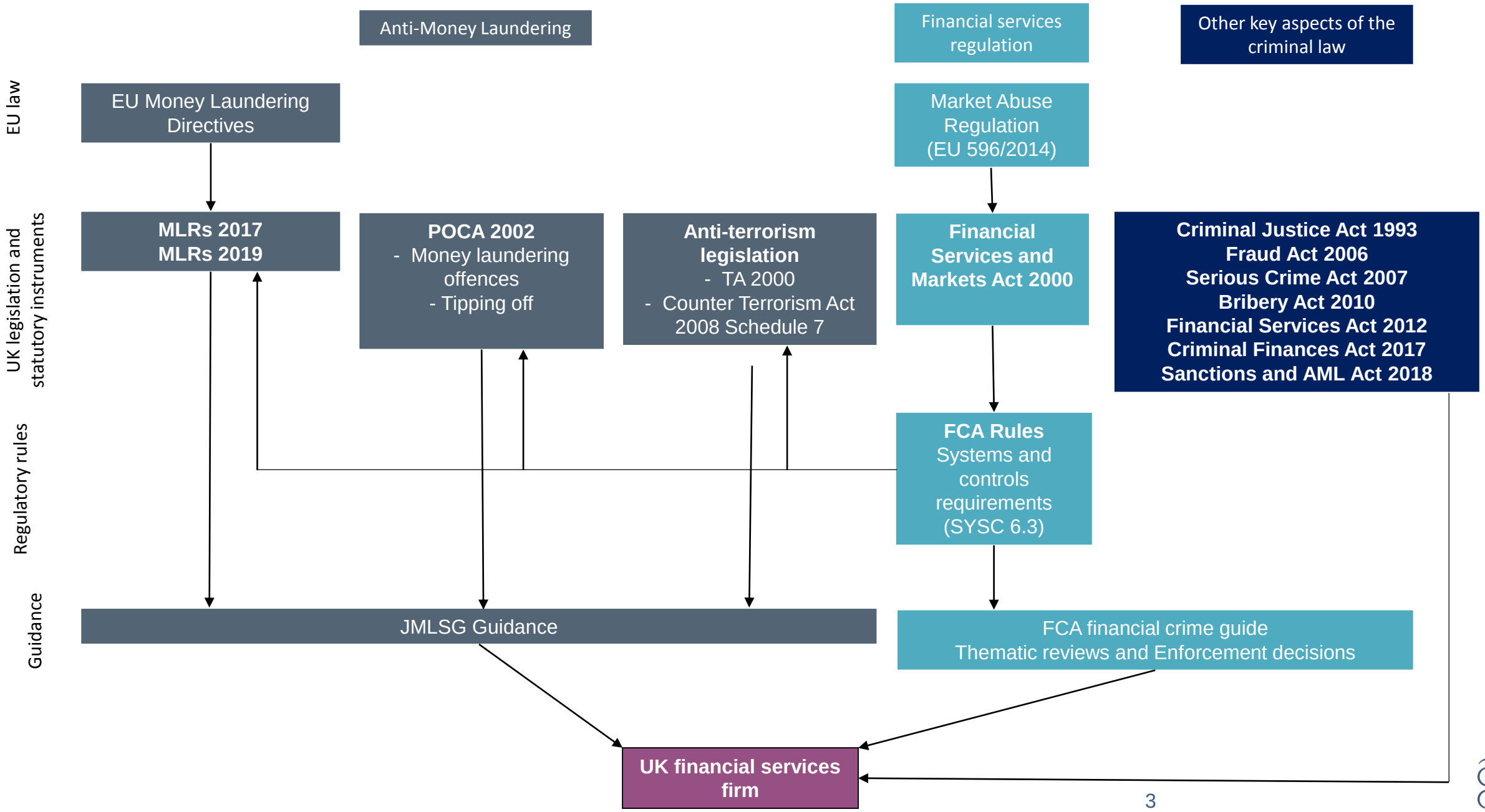
David Pygott, Partner

22 June 2020

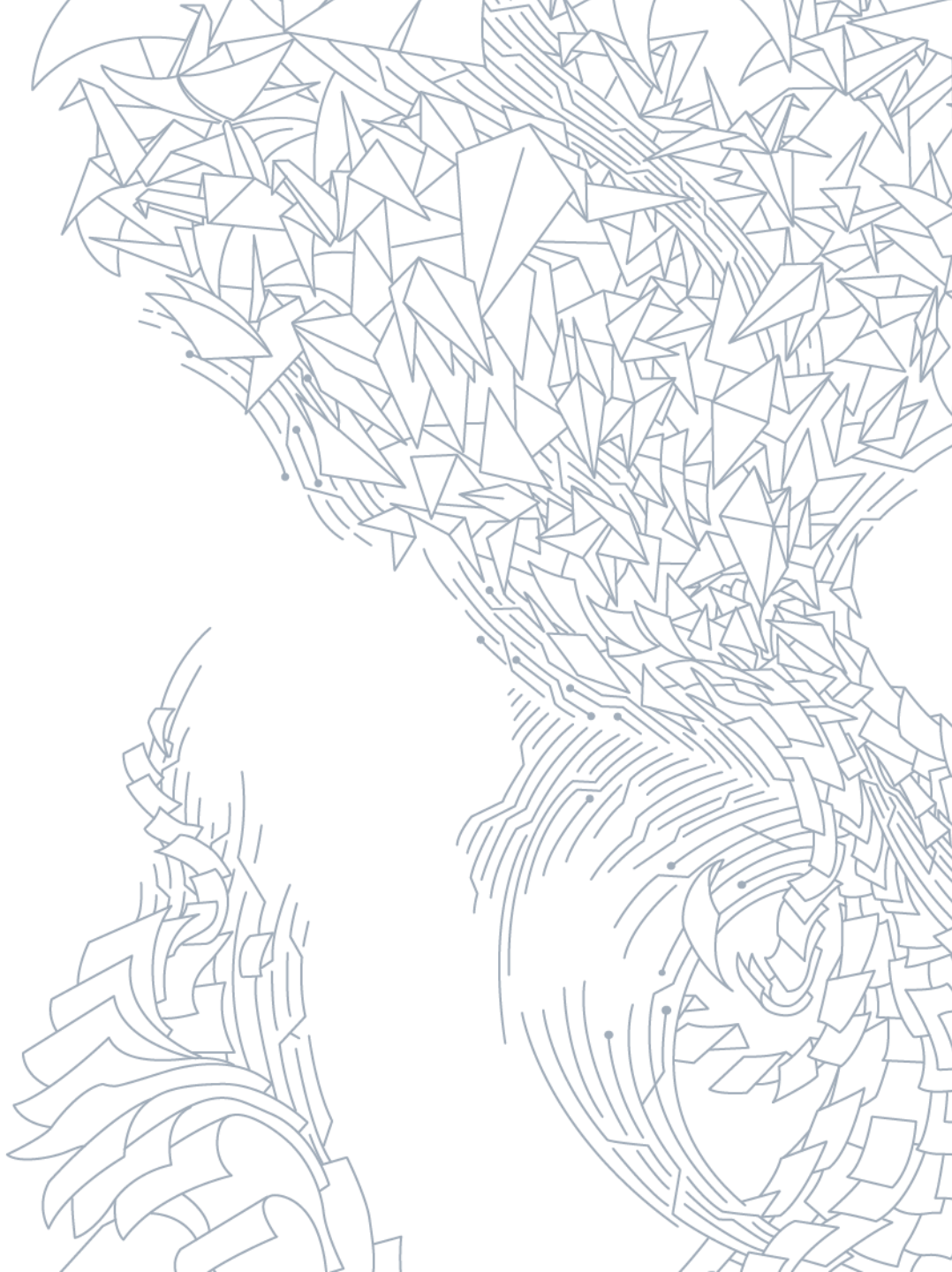
ADDLESHAW GODDARD

AGENDA

- **An overview – how the criminal law, regulatory rules and guidance fit together**
- **Anti-money laundering and counter terrorist financing**
  - Proceeds of Crime Act 2002 ("**POCA 2002**")
  - Terrorism Act 2000 ("**TA 2000**")
  - Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("**MLRs 2017**")
  - Money Laundering and Terrorist Financing (Amendment) Regulations 2019 ("**MLRs 2019**")
- **Other key aspects of the criminal law**
  - Some other key offences for financial services lawyers to be aware of
  - Bribery Act 2010 ("**BA 2010**")
  - Financial sanctions regime
- **The role of financial services regulation: controls against financial crime**
  - FCA rules
  - The FCA Financial Crime Guide


Anti-Money Laundering
Financial services regulation
Other key aspects of the criminal law
EU law
UK legislation and statutory instruments
Regulatory rules
Guidance
EU Money Laundering Directives
Market Abuse Regulation (EU 596/2014)
MLRs 2017
MLRs 2019
POCA 2002
- Money laundering offences
- Tipping off
Anti-terrorism legislation
- TA 2000
- Counter Terrorism Act 2008 Schedule 7
Financial Services and Markets Act 2000
Criminal Justice Act 1993
Fraud Act 2006
Serious Crime Act 2007
Bribery Act 2010
Financial Services Act 2012
Criminal Finances Act 2017
Sanctions and AML Act 2018
FCA Rules
Systems and controls requirements (SYSC 6.3)
JMLSG Guidance
FCA financial crime guide
Thematic reviews and Enforcement decisions
UK financial services firm

ANTI-MONEY LAUNDERING



ADDLESHAW GODDARD

WHAT IS ‘MONEY LAUNDERING’ UNDER POCA 2002? (1)

Structure of the Act – POCA 2002 Part 7

- Three main money laundering offences:
  - Concealing, disguising, converting, transferring or removing criminal property (s.327)
  - Involvement in arrangements relating to criminal property (s.328)
  - Acquisition, use or possession of criminal property (s.329)
- Subject to certain defences
  - Consent / DAML regime (ss.335, 336)
  - ‘Overseas conduct’ defence (ss.327 to 329)
  - ‘Adequate consideration’ defence (for s.329 offence only - acquisition, use, possession)
- Failure to report offences (ss.330, 331)
- Tipping off offence (s.333A)
- Offence of prejudicing an AML investigation (s.342)

WHAT IS ‘MONEY LAUNDERING’ UNDER POCA 2002? (2)

- ‘Money laundering’ defined in s.340(11)
  - one of the main offences in ss.327 to 329
  - an attempt, conspiracy or incitement to commit one of those offences
  - aiding, abetting, counselling or procuring the commission of one of those offences
  - an act which would constitute one of those offences if done in the United Kingdom
- “Criminal property” defined in s.340
  - any benefit arising from “criminal conduct” (in whole or in part, and whether directly or indirectly)
  - which is known or suspected to constitute or represent such a benefit
- “Criminal conduct” – all conduct which constitutes an offence in any part of the United Kingdom, or overseas conduct which could have amounted to an offence if it took place in the UK
- No de *minimis* limit
  - But threshold amounts for deposit-taking institutions

WHAT IS ‘MONEY LAUNDERING’ UNDER POCA 2002? (3)

What is ‘suspicion’?

- **R v Da Silva [2006] EWCA Crim 1654:**
  - Defendant thought that there was a possibility, which was more than fanciful, that the other person was or had been engaged in, or had benefitted from, criminal conduct
  - A vague feeling of unease would not suffice, but it was not necessary for the suspicion to be clear or firmly grounded and targeted on specific facts or based upon reasonable grounds
- **Shah & Anr v HSBC Private Bank (UK) Limited [2010] EWCA Civ 31 (CA) and [2012] EWHC 1283 (QB)**
  - Adopted the *Da Silva* test. However, the court accepted that the bank could be required to provide evidence of its suspicion
  - A bank’s duty of care to its customers may not be completely excluded by POCA. A claim by Mr Shah might have been made out if, for example, there was unreasonable delay in making a disclosure, or carrying out a transaction after consent was granted

PRINCIPAL DEFENCES TO MONEY LAUNDERING (1)

‘Overseas conduct’ defence

- Applies where:
  - Underlying “criminal conduct” reasonably believed to have taken place overseas
  - Conduct was not unlawful in that country
  - Conduct is not of a description prescribed by the Secretary of State
- Effect is that where conduct is of a non-serious nature (i.e. would be punishable by less than 12 months in prison in the UK) and was lawful where it occurred, dealing with the proceeds of that conduct is not “money laundering”

PRINCIPAL DEFENCES TO MONEY LAUNDERING (2)

The “consent regime”: obtaining a defence against money laundering (‘DAML’)

- A person does not commit an offence if he
  - Makes a disclosure to a constable or customs officer before he does the act and has the appropriate consent
  - Makes a disclosure after the act if there is a good reason for his failure to disclose beforehand and the disclosure is made on his own initiative and as soon as practicable
  - Makes a disclosure whilst doing the act, if he began to do it when he had no suspicions, and he makes a disclosure on his own initiative and as soon as practicable after forming a suspicion
  - Intended to make a disclosure but had a reasonable excuse for not doing so

PRINCIPAL DEFENCES TO MONEY LAUNDERING (3)

The “consent regime” (cont.)

- What constitutes consent?
  - Express consent (when given)
  - Deemed consent: no response by NCA to the disclosure within seven working days (“notice period”)
- Deemed consent: permission to transact is refused within 7 working days, **but** the moratorium expires (31 day moratorium, can be extended for 31 days at a time, up to 186 days)
- Avoid tipping off (regulated sector) or prejudicing an investigation
- NCA fact sheet ‘Requesting a defence from the NCA under POCA and TACT” is available from https://nationalcrimeagency.gov.uk/ and describes the DAML process in more detail

FAILURE TO REPORT OFFENCES (S.330 POCA 2002)

Failure to report money laundering – employees

- Only applies to ‘Regulated Sector’ (i.e. credit and financial institutions (as defined) and other specified professions/businesses e.g. auditors, tax advisers, lawyers)
- The firm itself is not involved in money laundering (and therefore does not need consent) – but suspects that someone else is
- Employee obligation to report to MLRO; MLRO obligation to report to NCA
- Knowledge, suspicion or “reasonable grounds for knowing or suspecting” that another has committed a money laundering offence
- Obligation to report only if it is possible to identify the money launderer, or the whereabouts of any criminal property, or reasonable to believe that the information will assist in identifying that person or property. Disclosure must include these matters, if known

“REASONABLE GROUNDS”

- Failing to assess adequately the facts and information that are either presented or available and that would put an honest person on enquiry
- Determined by:
  - Information available to the individual at the time
  - Their experience and awareness
  - Their actions and inquiries
  - Comparison to peer group
  - Their training
- May have reasonable grounds if there is enough cumulative information on the file through previous transactions to determine which transactions are outside the normal course of business for that client
- Important that you take all reasonable steps to identify the customer and understand the rationale for the transaction/instruction

MLRO FAILURE TO REPORT OFFENCE (S.331 POCA 2002)

Failure to report money laundering – MLRO

- MLRO commits an offence if he receives an internal report which he does not pass on, if he knows or suspects or has reasonable grounds for knowing or suspecting that another is engaged in money laundering (s.331)
- Report must identify money launderer or whereabouts of criminal property, or information that would assist in identifying them
- Internal reports must be treated as such even if not made in accordance with employer's procedures

TERRORISM ACT 2000

- Key offences relate to “terrorist property” – defined in s.14 TA 2000:
  - money or other property which is likely to be used for the purposes of terrorism (including any resources of a proscribed organisation)
  - proceeds of the commission of acts of terrorism
  - proceeds of acts carried out for the purposes of terrorism

- Key offences in TA 2000:
  - Fund raising (s.15)
  - Use and possession of terrorist property (s.16)
  - Becoming concerned in ‘funding arrangements’ (s.17)
  - Arrangements which facilitate the retention of control of terrorist property (s.18)
  - Failure to disclose (ss.19 and 21A)

MLRS 2017

- Implement the EU's Fourth Money Laundering Directive (2015/849) in the UK
- Key obligations under the Regulations
  - AML and counter terrorist financing policies and procedures
  - Risk assessment
  - Customer due diligence (KYC / CDD)
  - Ongoing monitoring
  - Record-keeping
  - Training
- A risk based approach

MLRS 2019

- Implement the EU's Fifth Money Laundering Directive (2018/843) in the UK
- Amend the MLRs 2017, mostly as from 10 January 2020 (but some provisions not yet in force)
- Key changes made:
  - Widened scope of AML regulation, e.g. certain crypto-currency firms brought into scope
  - Stronger customer due diligence requirements, particularly:
    - Clearer definition of enhanced due diligence
    - Stronger measures in relation to 'high risk third countries'
  - Provision made for authorities to obtain information about holders of bank accounts using a central automated mechanism

PENALTIES

- **POCA 2002 (s.334)**
  - Money laundering offences (ss. 327-329) – up to 14 years' imprisonment or a fine or both
  - Failure to disclose offences (ss. 330-332) – up to 5 years' imprisonment or a fine or both
  - Tipping-off offences (ss.333A and 342) – up to 2 years' imprisonment or a fine or both
- **TA 2000 (ss.21D and 22)**
  - Ss.15 to 19 and 21A – up to 14 years' imprisonment or a fine or both
  - Tipping-off – up to 2 years' imprisonment or a fine or both
- **MLRs 2017 (as amended)**
  - Breaches can result in civil fines or (in serious cases) criminal prosecution
  - Criminal fines: up to 2 years' imprisonment or a fine or both (MLRs 2017 reg.86)

JOINT MONEY LAUNDERING STEERING GROUP

- **JMLSG** - http://www.jmlsg.org.uk/
  - Publishes money laundering guidance for the financial sector
    - Assist firms to implement and design systems and controls to mitigate the risk of being used in connection with money laundering and terrorist financing
    - Indicates good industry practice in compliance with POCA 2002, TA 2000, MLRs 2017
    - Updated June 2020
  - Structure of the JMLSG guidance
    - Part I - General guidance: governance, internal controls, risk based approach, KYC/CDD, suspicious activity reporting, staff awareness and training, record keeping
    - Part II – Sectoral guidance, e.g. retail banking, wealth management, financial advisers, general insurers, private equity, corporate finance, wholesale markets
    - Part III – Specialist guidance – includes guidance on compliance with the UK financial sanctions regime

OTHER KEY ASPECTS OF THE CRIMINAL LAW

ADDLESHAW GODDARD

SOME OTHER KEY CRIMINAL OFFENCES IN FINANCIAL SERVICES

- Theft Act 1968 – false accounting, false statements by company directors
- Criminal Law Act 1977 – conspiracy
- Forgery and Counterfeiting Act 1981 – forgery of documents / making ‘false instruments’
- Criminal Justice Act 1993 – criminal offence of insider dealing (see EU Market Abuse Regulation for civil ‘offences’)
- Fraud Act 2006 – fraud offences (note also common law offence of conspiracy to defraud)
- Serious Crime Act 2007 – encouraging or assisting an offence
- **Bribery Act 2010 – bribery and corruption**
- Financial Services Act 2012 – misleading statements, misleading impressions, benchmark offences
- Criminal Finances Act 2017 – offences of failure to prevent tax evasion
- **Sanctions and AML Act 2018 and other sanctions regulations – sanctions offences**
- Tax offences – under various pieces of tax legislation

BRIBERY ACT 2010 – THE KEY OFFENCES

- BA 2010 includes four criminal offences
  - An offence of active bribery (i.e. giving, promising or offering a bribe), which applies in the public or private sector – s.1 BA 2010
  - An offence of passive bribery (i.e. requesting, agreeing to receive or accepting a bribe), which applies in the public or private sector – s.2 BA 2010
  - A specific offence of bribing a foreign public official – s.6 BA 2010
  - A ‘corporate’ offence which applies where a corporate or partnership fails to prevent those performing services on its behalf from paying bribes – s.7 BA 2010
- No exemption in BA 2010 in respect of facilitation payments

BRIBERY ACT 2010 – JURISDICTION (ACTIVE AND PASSIVE BRIBERY)

- UK proceedings possible where any act or omission which forms part of the offence takes place in the UK (s.12 BA 2010)
- BUT even if no act or omission takes place in the UK (e.g. all acts take place overseas) proceedings may still be possible against a person with a “close connection with the UK”
- “Close connection”?
  - British citizens, British overseas territories citizens
  - a person ordinarily resident in the UK
  - a body incorporated under UK law

S.7 BRIBERY ACT 2010 – FAILURE TO PREVENT BRIBERY

The corporate offence of failure to prevent bribery

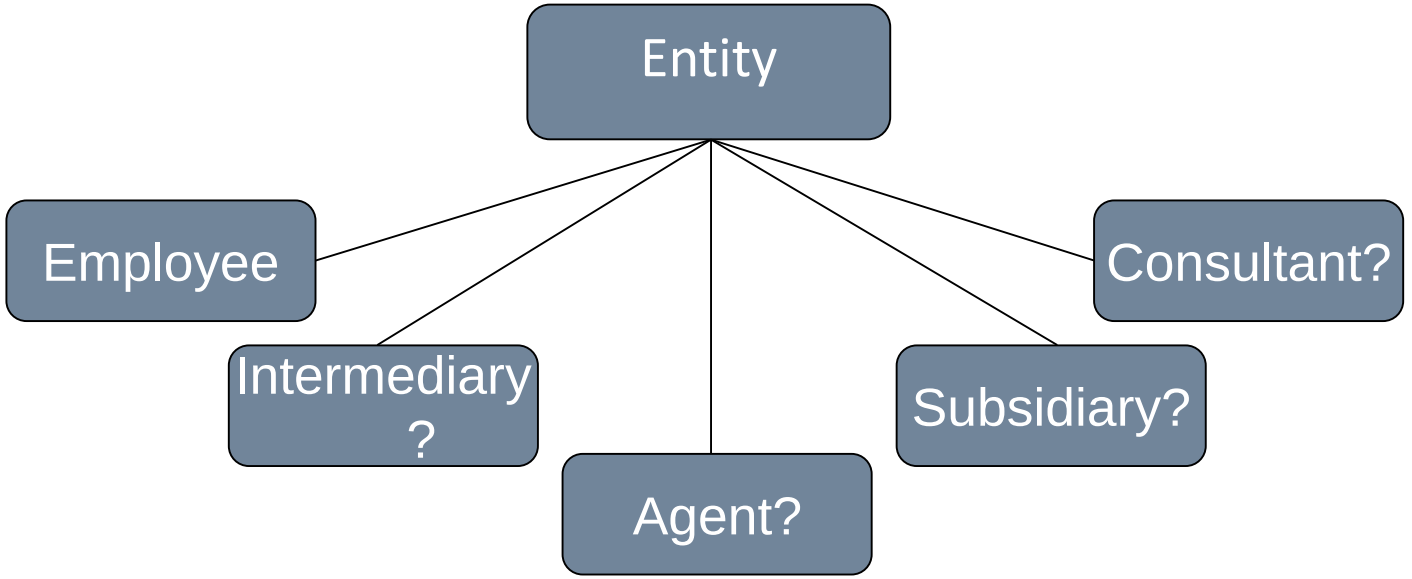
- A relevant commercial organisation ("C") is guilty of an offence if:
- Someone ("A") associated with C bribes another person
- Intending to obtain or retain business or a business advantage for C

The 'adequate procedures' defence

- It is a defence for the commercial organisation to show that it had 'adequate procedures' in place designed to prevent persons associated with it from undertaking such conduct
- importance of adequate procedures e.g. policies, procedures, due diligence, payment controls, audit/monitoring
- statutory guidance on what is 'adequate' – s.9

WHO IS AN ‘ASSOCIATED PERSON’

- A is associated with C, if disregarding any bribe under consideration – A “performs services for the benefit of C”
- Capacity in which A performs services does not matter – instead determined by reference to all the relevant circumstances



WHAT DO ‘ADEQUATE PROCEDURES’ LOOK LIKE

- To comply with BA 2010, organisations must develop and implement “adequate procedures” to prevent corruption by those providing services on their behalf
- The MoJ has published guidance on ‘adequate procedures’ as required by s.9 BA 2010
  - https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf
- Broad principles and illustrative examples (but no formal ‘safe harbours’)
- The 6 broad principles are:
  - Proportionate procedures (but note being a small firm does not exempt entirely - Skansen Interiors, 2018)
  - Top level commitment
  - Risk assessment
  - Due diligence
  - Communication (including training)
  - Monitoring and review

S.7 BA 2010 – JURISDICTION

- A relevant commercial organisation is:
  - a body/partnership incorporated/formed in the UK
  - incorporated or formed elsewhere which carries on a business or part of a business in any part of the UK
- S12(5) it does not matter whether the act or omissions which form part of the s7 offence take part in the UK or elsewhere

BA 2010: PENALTIES

- Penalties for commission of offences in BA 2010 (s.11)
  - For individuals: up to 10 years' imprisonment, an unlimited fine or both
  - For companies: an unlimited fine
  - Confiscation of the gross revenue of any contracts/benefits obtained from bribery

WHAT ARE FINANCIAL SANCTIONS AND TRADE CONTROLS?

- Financial sanctions: require funds and assets of an individual or entity to be frozen
- Trade controls: restrict/prohibit supply of certain items/listed goods/technology/information to certain countries/people
- Prevent dealing with certain individuals/entities or countries
- Prevent investment in certain industries where there is a connection to a specific state

WHY ARE THEY IMPLEMENTED?

- To achieve a number of different foreign policy aims:
  - To restrict trade with individuals, entities, political regimes, or countries with a view to encouraging behavioural change
  - To prevent the financing of terrorism
  - As a reaction to human rights abuses or other behaviours which are considered by the international community as being inappropriate
  - To restrict the supply of military or defence items, or to prevent the development or proliferation of weapons

WHO IMPOSES THEM

- Sanctions regime is complex and can change quickly
- Sanctions can be imposed in a number of different ways:
  - by the United Nations
  - the EU
  - unilaterally by an individual state
- UK powers: Sanctions and Anti-Money Laundering Act 2018
- From a regulatory perspective, FCA expects financial services firms to have:
  - Proper governance in place to ensure adherence with the sanctions regime
  - Effective, up to date screening systems appropriate to the nature, size and risk of its business
  - See FCA Handbook - Financial Crime Guide chapter – covering sanctions

WHO IMPOSES SANCTIONS IN THE UK?

- **Sanctions imposed by the European Union** are directly applicable to individuals and entities of all Member States. However, it is for Member States to enforce the measures through national law
- **Financial Sanctions** are implemented and enforced by the office of Financial Sanctions Implementation (**“OFSI”**)
- **Trade sanctions** are implemented and enforced by the UK Department of Business, Innovation and Skills (**“BIS”**)

COUNTRIES CURRENTLY SUBJECT TO UK FINANCIAL SANCTIONS

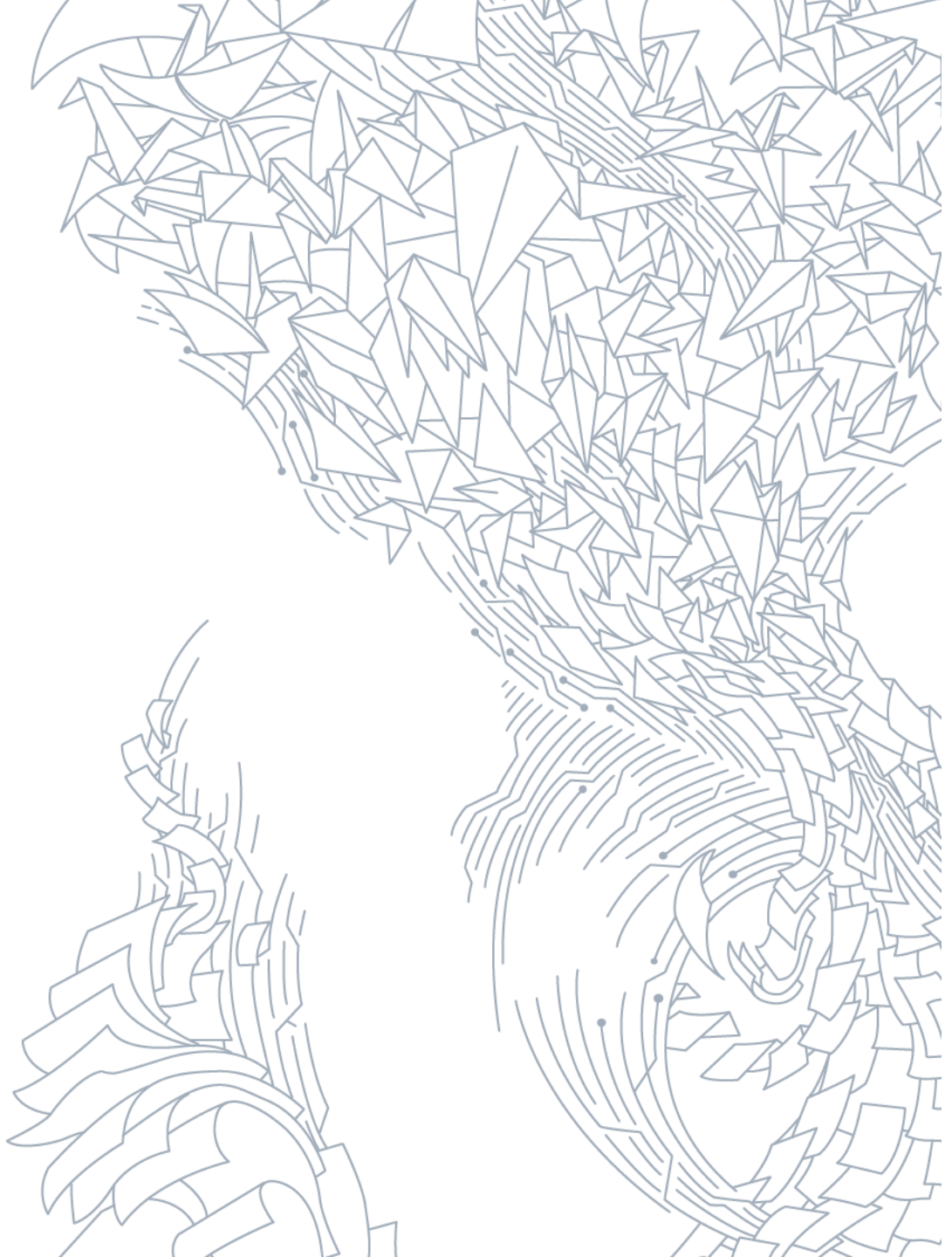
- Afghanistan
- Belarus
- Burma / Myanmar
- Burundi
- Central African Republic
- Democratic Republic of Congo
- Egypt
- Iran
- Iraq
- Libya
- Mali
- Nicaragua
- North Korea
- Republic of Guinea
- Republic of Guinea-Bissau
- Ukraine/Russia
- Somalia
- Sudan
- South Sudan
- Syria
- Tunisia
- Turkey
- Venezuela
- Yemen
- Zimbabwe

- Current consolidated list: https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets

BREACHES OF FINANCIAL SANCTIONS REGIME: PENALTIES

- Criminal prosecution – usually up to 7 years' imprisonment, an unlimited fine, or both
- Civil regime – OFSI is now able to issue financial penalties (in some cases) up to a maximum of £1 million or 50% of the value of the breach
- OFSI has issued:
  - A general guide to the UK financial sanctions regime
  - Guidance regarding its approach to issuing financial penalties
  - See https://www.gov.uk/government/publications/financial-sanctions-faqs

FINANCIAL SERVICES REGULATION



ADDLESHAW GODDARD

KEY FCA RULES AND GUIDANCE (1)

- FCA's market integrity objective (FSMA s1D) includes
  - protecting and enhancing the integrity of the UK financial system
  - seeing that it is not used "for a purpose connected with financial crime"
- Key focus of the regulatory regime is on firms' systems and controls against financial crime, especially money laundering
- Close interrelationship between underlying law (especially MLRs 2017/2019) and FCA rules systems and controls rules
- Key sections of the FCA handbook relevant to financial crime issues
  - SYSC 6.3 – high level systems and controls requirements
  - Financial crime guide (**"FCG"**) – practical guidance on what FCA expects in key risk areas

KEY FCA RULES AND GUIDANCE (2)

- SYSC 6.3.1R: a regulated firm must ensure its policies and procedures include systems and controls that
  - enable it to identify, assess, monitor and manage money laundering risk
  - are comprehensive and proportionate to the nature, scale and complexity of its activities
- SYSC 6.3.4G: cross reference to firms' obligations under POCA 2002, TA 2000, and MLRs 2017
- SYSC 6.4.5G: FCA will have regard when assessing whether there has been a breach of its rules on systems and controls against money laundering as to whether JMLSG guidance has been followed

KEY FCA RULES AND GUIDANCE (3)

- Guidance in FCG includes examples of what FCA considers good / poor practice in control of key areas of risk (AML, fraud, bribery and corruption, sanctions and asset freezes, insider dealing):
  - Governance
    - active engagement of senior management
    - quality of management information
    - clear organisational structure
    - risk assessments
    - documented policies and procedures
  - Risk-sensitive due diligence and ongoing monitoring
  - Policies and procedures for dealing with higher risk situations
  - Good record keeping

ROLE OF THE FCA

- A **supervisor** reviewing firms' compliance and challenging them to improve
  - Particularly through thematic reviews (past reviews covered in FCTR section of FCA Handbook)

- An **enforcement** authority
  - A regulatory enforcement authority with powers under FSMA and MLRs 2017 (as amended by MLRs 2019) to impose fines and other sanctions on firms and individuals for regulatory failings in relation to financial crime controls
  - A criminal prosecutor: ability to prosecute serious breaches of the MLRs 2017 (as amended by MLRs 2019), offences under POCA 2002, certain other financial services offences before the Crown Court

FCA ENFORCEMENT EXAMPLES

- Examples of civil / regulatory enforcement action for financial crime-related issues:
  - June 2020 – bank fined £37.8m for poor AML controls in higher risk areas of its business
  - April 2019 – bank fined £102.1m for poor AML controls in higher risk areas of its business
  - June 2018 – bank fined £896k and prevented from accepting deposits from new customers for approx. 5 months for poor AML controls
  - January 2017 – bank fined £163m for AML controls failings in corporate banking / securities division
  - October 2016 – bank fined £3.2m and prevented from accepting deposits from new customers for approx. 5 months for poor AML controls; former MLRO also fined and prohibited
  - March 2012 – bank fined £8.75m for poor AML controls, poor due diligence of high risk customers
  - August 2010 – bank fined £5.6m for failing to put in place adequate controls to prevent sanctions breaches
  - January 2009 – insurance broker fined £5.25m for poor bribery and corruption controls (payments to overseas third parties in high risk jurisdictions), making of suspicious payments

QUESTIONS?

Michelle de Kluyver
Partner
+44 (0)20 7788 5101
michelle.dekluyver@addleshawgoddard.com

David Pygott
Partner
+44 (0)20 7788 5123
david.pygott@addleshawgoddard.com

www.addleshawgoddard.com

Aberdeen, Doha, Dubai, Edinburgh, Glasgow, Hamburg, Hong Kong,
Leeds, London, Manchester, Muscat, Singapore and Tokyo*

* a formal alliance with Hashidate Law Office