
FINAL NOTICE

To: BASTION CAPITAL LONDON LTD
Firm Reference Number: 232423
Address: C/O Opus Restructuring Llp
Evergreen House North, Grafton Place
London, NW1 2DX
Date 12 July 2023

1. ACTION

- 1.1 For the reasons given in this Final Notice, pursuant to section 206 of the Financial Services and Markets Act 2000 (“the Act”), the Financial Conduct Authority (“the Authority”) hereby imposes on Bastion Capital London Limited (“Bastion” or “the Firm”) a financial penalty of £2,452,700.
- 1.2 Bastion agreed to resolve this matter and qualified for a 30% (Stage 1) discount under the Authority’s executive settlement procedures. Were it not for this discount, the Authority would have imposed a financial penalty of £2,837,600 on Bastion.

2. SUMMARY OF REASONS

- 2.1 Fighting financial crime is an issue of international importance, and forms part of the Authority’s operational objective of protecting and enhancing the integrity of the UK financial system. Reducing and preventing financial crime is one of the key priorities of the Authority as set out in its published business plan. Authorised firms

are at risk of being abused by those seeking to conduct financial crime, such as fraudulent trading and money laundering. Therefore, it is imperative that firms have in place effective systems and controls to identify and mitigate the risk of their businesses being used for such purposes, and that firms will act with due skill, care and diligence to adhere to the systems and controls they have put in place, and to properly assess, monitor and manage the risk of financial crime.

2.2 Between 29 January 2014 and 29 September 2015 (the "Relevant Period"), Bastion:

a) had inadequate systems and controls to identify and mitigate the risk of being used to facilitate fraudulent trading and money laundering in relation to business related to four authorised entities known as the Solo Group, thereby breaching Principle 3; and

b) breached Principle 2 as it did not exercise due skill, care and diligence in applying its AML policies and procedures, and in failing to properly assess, monitor and mitigate the risk of financial crime in relation to business related to the Solo Group, as set out in this Notice.

2.3 The Solo Clients were off-shore companies including British Virgin Islands ("BVI") and Cayman Islands incorporated entities and a number of individual US 401(k) pension plans previously unknown to Bastion. They were introduced by the Solo Group, which purported to provide clearing and settlement services as custodians to clients within a closed network, via a custom over the counter ("OTC") post-trade order matching platform in 2014 and a trading and settlement platform in 2015, known as Brokermesh. They were controlled by a small number of individuals, some of whom had worked for the Solo Group, without apparent access to funds to settle the transactions.

2.4 On behalf of the Solo Clients, Bastion executed purported OTC equity trades to the value of approximately £49.03 billion in Danish equities and £22.48 billion in Belgian equities and received gross commission of approximately £1.55 million.

2.5 The Solo Trading was characterised by a purported circular pattern of extremely high value OTC equity trading, back-to-back securities lending arrangements and forward transactions, involving EU equities on or around the last day of cum-dividend. Following the purported Cum-Dividend Trading that took place on designated days, the same trades were subsequently purportedly reversed over

several days or weeks to neutralise the apparent shareholding positions (the "Unwind Trading").

- 2.6 The purported OTC trades executed by Bastion on behalf of Solo Clients, were initially conducted via email and a post-trade order matching platform in 2014, and then in 2015 executed on Brokermesh, which did not have access to liquidity from public exchanges. Yet the purported trades almost invariably were filled within a matter of minutes, and represented up to 30% of the shares outstanding in the companies listed on the Danish stock exchange, and up to 10% of the equivalent Belgian stocks. The volumes also equated to an average of 41 times the total number of all shares traded in the Danish stocks on European exchanges, and 23 times the Belgian stocks traded on European exchanges on the relevant last cum-dividend trading date.
- 2.7 The Authority's investigation and conclusions in respect of the purported trading are based on a range of information including, in part, analysis of transaction reporting data, material received from Bastion, the Solo Group, and five other Broker Firms that participated in the Solo Trading. The combined volume of the Cum-Dividend Trading across the six Broker Firms was between 15 and 61% of the shares outstanding in the Danish stocks traded, and between 7 and 30% of the shares outstanding in the Belgian stocks traded. These volumes are considered implausible, especially in circumstances where there is an obligation to publicise holders of over 5% of Danish and Belgian listed stocks.
- 2.8 As a broker for the equity trades, Bastion executed the purported Cum-Dividend Trading and the purported Unwind Trading. However, the Authority believes it is unlikely that Bastion would have executed both the purported cum-dividend trades and purported unwind trades for the same client in the same stock in the same size trades and therefore it is likely Bastion only saw one side of the purported trading. Additionally, the Authority considers that purported stock loans and forwards linked to the Solo Trading are likely to have been used to obfuscate and/or give apparent legitimacy to the overall scheme. However, Bastion did not execute the purported stock loans and forwards.
- 2.9 The purpose of the purported trading was so the Solo Group could arrange for Dividend Credit Advice Slips ("DCAS") to be created, which purported to show that the Solo Clients held the relevant shares on the record date for dividend. The DCAS were in some cases then used to make withholding tax ("WHT") reclaims from the tax agencies in Denmark and Belgium, pursuant to Double Taxation Treaties. In

2014 and 2015, the value of Danish and Belgian WHT reclaims made, which are attributable to the Solo Group, were approximately £899.27 million and £188.00 million respectively. In 2014 and 2015, of the reclaims made, the Danish and Belgian tax authorities paid approximately £845.90 million and £42.33 million respectively.

- 2.10 The Authority refers to the trading as 'purported' as it has found no evidence of ownership of the shares by the Solo Clients, or custody of the shares and settlement of the trades by the Solo Group. This, coupled with the high volumes of shares purported to have been traded, is highly suggestive of sophisticated financial crime.
- 2.11 Bastion had in place inadequate systems and controls to identify and mitigate the risk of being used to facilitate fraudulent trading and money laundering in relation to business related to four authorised entities known as the Solo Group. In addition, Bastion staff did not exercise due skill, care and diligence in applying AML policies and procedures and in failing to properly assess, monitor and mitigate the risk of financial crime in relation to business related to the Solo Group.
- 2.12 Bastion did not have adequate policies and procedures in place to properly assess the risks of the Solo Group business, and lacked an appreciation of the risks involved in the purported equity trading that the Solo Clients were engaged in, which resulted in inadequate CDD being conducted and a failure to adequately monitor transactions and to identify unusual transactions. This heightened the risk that the Firm could be used for the purposes of facilitating financial crime in relation to the purported equity trading (the "Solo Trading") executed by Bastion between 26 February 2014 and 29 September 2015.
- 2.13 The way these purported trades were conducted in combination with their scale and volume are highly suggestive of financial crime. The Authority's findings are made in the context of this finding and in consideration that these matters have given rise to additional investigation by other tax agencies and/or law enforcement agencies, as has been publicly reported.
- 2.14 In addition to the Solo Trading, Bastion executed a series of trades on behalf of 11 Solo Clients on 18, 19 and 30 June 2014 and 20 May 2015, in German and Belgian listed stocks. Each of these trades resulted in a single Solo Client (Ganymede Cayman Ltd, an entity wholly owned by the Solo Group's controller) making a loss, and cumulatively resulted in a combined loss of EUR €22,729,508.15 million to the benefit of the remaining 10 Solo Clients.

- 2.15 These trades were materially different from the Solo Trading for various reasons as set out in this Notice. In the days before the transactions took place, some of these Solo Clients were urgently onboarded at the request of the Solo Group. The trades were executed using intraday prices, instead of end of day prices and not executed based on cum-dividend dates.
- 2.16 Bastion acted as the only executing broker for all of these trades on behalf of the 11 Solo Clients. On each occasion, the trades were reversed by the same clients within hours, at different prices, meaning a substantial net loss for one client and profits for the other parties, therefore making the economic rationale for the transactions unclear and highly suggestive of financial crime.
- 2.17 Bastion ignored or failed to notice a series of red flags in relation to these sets of trades it executed on behalf of these 11 Solo Clients, which had no apparent economic purpose except to transfer funds from the Solo Group's controller to his business associates. The circumstances of the onboarding and trading relating to these Solo Clients ought to have prompted Bastion to adequately consider associated financial crime risks posed to the Firm.
- 2.18 The Authority considers that Bastion failed to take reasonable care to organise and control its affairs responsibly and effectively with adequate risk management systems, as required by Principle 3, in relation to business related to the Solo Group. Its policies and procedures were inadequate for identifying, assessing and mitigating the risk of financial crime posed by the Solo Group business as they:
- a) Failed to establish the requirement for risk assessments to be documented, as well as to document the rationale for any due diligence measures the firm waived when compared to its standard approach, in view of its risk assessment of a particular customer;
 - b) Failed to set out adequate processes and procedures for EDD;
 - c) Failed to set out adequate processes and procedures for client categorisation; and
 - d) Failed to set out adequate processes and procedures for transaction monitoring, including how transactions are monitored, and with what frequency, and set out adequate processes and procedures for how to identify suspicious transactions.

2.19 The Authority considers that Bastion failed to act with due skill, care and diligence as required by Principle 2 in that it failed to properly assess, monitor and manage the risk of financial crime associated with the business related to the Solo Group, in that the Firm:

- a) Failed to properly conduct customer due diligence prior to onboarding, and consequently failed to identify that the Solo Clients presented a higher risk of financial crime before they started trading;
- b) Failed to gather information to enable it to understand the purpose and intended nature of the business that the Solo Clients were going to undertake, the likely size or frequency of the purported trading intended by the Solo Clients or their source of funds;
- c) Failed to undertake and document a risk assessment for each of the Solo Clients prior to onboarding and trading for the Solo Clients;
- d) Failed to complete EDD for any of the Solo Clients despite the fact that none of the Solo Clients were physically present for identification purposes and a number of other risk factors were present;
- e) Failed to assess each of the Solo Clients against the categorisation criteria set out in COBS 3.5.2R and failed to record the results of such assessments, including sufficient information to support the categorisation, contrary to COBS 3.8.2(2)(a);
- f) Failed to conduct transaction monitoring of the Solo Clients' purported trades;
- g) Failed to recognise numerous red flags with the purported trading, including failing to consider whether it was plausible and/or realistic that sufficient liquidity was sourced within a closed network of entities for the size and volumes of trading conducted by the Solo Clients. Likewise, failing to consider or recognise that the profiles of the Solo Clients meant that they were highly unlikely to meet the scale and volume of the trading purportedly being carried out, and failed to at least obtain sufficient evidence of the clients' source of funds to satisfy itself to the contrary; and

h) Failed to recognise numerous red flags arising from the purported Ganymede trades and adequately consider financial crime and money laundering risks they posed to the Firm.

2.20 Bastion's failings merit the imposition of a significant financial penalty. The Authority considers the failings to be particularly serious because they left the Firm exposed to the risk that it could be used to further financial crime;

- 1) Bastion onboarded 327 clients, some of which emanated from jurisdictions which did not have AML requirements equivalent to those in the UK;
- 2) Bastion's AML policies and procedures were not proportionate to the risks in the Solo business that it was undertaking;
- 3) Bastion failed to review and analyse the KYC materials that were provided by the Solo Group properly or ask appropriate follow up questions to red flags in the KYC materials;
- 4) Even after a number of red flags appeared, Bastion failed to conduct any ongoing monitoring, allowing these same clients to purportedly trade equities totalling more than £71.5 billion;
- 5) Because Bastion failed to both have and apply appropriate AML systems and controls in relation to the Solo business, there was an unacceptable risk that Bastion could be used by clients to launder the proceeds of crime;
- 6) Bastion executed a series of uneconomic trades, while ignoring numerous red flags that were highly suggestive of financial crime.
- 7) Finally, these failings were not identified Bastion.

2.21 Accordingly, to further the Authority's operational objective of protecting and enhancing the integrity of the UK financial system, the Authority hereby imposes on Bastion a financial penalty of £2,452,700.

3. DEFINITIONS

3.1 The following definitions are used in this Notice:

"401(k) pension plan" means an employer-sponsored retirement plan in the United States. Eligible employees may make pre-tax contributions to the plan but are taxed on withdrawals from the account. A Roth 401(k) plan is similar in nature; however, contributions are made post-tax although, withdrawals are tax-free. For

the 2014 tax year, the annual contribution limit was \$17,500 for an employee, plus an additional \$5,500 catch-up contribution for those aged 50 and over. For the tax year 2015, the contribution limits were \$18,000 for an employee and the catch-up contribution was \$6,000. For a more detailed analysis, please see Annex C;

"2007 Regulations" or **"Regulation"** means the Money Laundering Regulations 2007;

"the Act" means the Financial Services and Markets Act 2000;

"AML" means Anti-Money Laundering;

"AML certificate" means an AML introduction form which is supplied by one authorised firm to another. The form confirms that a regulated firm has carried out CDD obligations in relation to a client and authorises another regulated firm to place reliance on it in accordance with Regulation 17;

"AML policy" means Bastion's 'Anti Money Laundering and Combating Terrorist Financing Policy' dated September 2013;

"Authority" means the Financial Conduct Authority, known prior to 1 April 2013 as the Financial Services Authority;

"Bastion" means Bastion Capital London Ltd;

"Broker Firms" means the other broker firms who agreed with the Solo Group to carry out the Solo Trading;

"Brokermesh" means the bespoke electronic platform set up by the Solo Group for the Solo Clients to submit orders to buy or sell cash equities, and for the Broker Firms to provide or seek liquidity and execute the purported trading;

"CDD" means customer due diligence measures, the measures a firm must take to identify each customer and verify their identity and to obtain information on the purpose and intended nature of the business relationship, as required by Regulation 5;

"Clearing broker" means an intermediary with responsibility to reconcile trade orders between transacting parties. Typically, the clearing broker validates the availability of the appropriate funds, ensures the delivery of the securities in exchange for cash as agreed at the point the trade was executed, and records the transfer;

"COBS" means the Authority's Conduct of Business Sourcebook Rules;

"Compliance Manual" means Bastion's Compliance Manuals dated 1 May 2013 and 6 October 2014, which were applicable during the Relevant Period;

"Cum-dividend" means when a buyer of a security is entitled to receive the next dividend scheduled for distribution, which has been declared but not paid. A stock trades cum-dividend up until the ex-dividend date, after which the stock trades without its dividend rights;

"Cum-Dividend Trading" means the purported trading that the Solo Clients conducted where the shares are cum-dividend in order to demonstrate apparent shareholding positions that would be entitled to receive dividends, for the purposes of submitting WHT reclaims;

"Custodian" means ^a financial institution that holds customers' securities for safekeeping. They also offer other services such as account administration, transaction settlements, the collection of dividends and interest payments, tax support and foreign exchange;

"DCAS" means Dividend Credit Advice Slips. These are completed and submitted to overseas tax authorities in order to reclaim the tax paid on dividends received;

"DEPP" means the Authority's Decision Procedure and Penalties Manual;

"Dividend Arbitrage" means the practice of placing shares in an alternative tax jurisdiction around dividend dates with the aim of minimising withholding taxes (WHT), or generating WHT reclaims. Dividend Arbitrage may include several different activities including trading and lending equities and trading derivatives, including futures and total return swaps, designed to hedge movements in the price of the securities over the dividend dates;

"Double Taxation Treaty" means a treaty entered into between the country where the income is paid and the country of residence of the recipient. Double Taxation Treaties may allow for a reduction or rebate of the applicable WHT;

"EDD" means enhanced due diligence, the measures a firm must take in certain situations, as outlined in Regulation 14;

"European exchanges" means registered execution venues, including regulated markets, multilateral trading facilities, organised trading facilities and alternative trading systems encapsulated in Bloomberg's European Composite;

"Executing broker" means a broker that merely buys and sells shares on behalf of clients. The broker does not give advice to clients on when to buy or sell shares;

"Financial Crime Guide" means the Authority's consolidated guidance on financial crime, which is published under the name "Financial crime: a guide for firms". In this Notice, the applicable versions for the Relevant Period were published in April 2013, April 2014, January 2015 (incorporating updates which came into effect on 1 June 2014) and April 2015. The Financial Crime Guide contains "general guidance" as defined in section 139B FSMA. The guidance is not binding and the Authority will not presume that a firm's departure from the guidance indicates that it has breached the Authority's rules. But as stated in FCG 1.1.8 the Authority expect firms to be aware of the Financial Crime Guide where it applies to them, and to consider applicable guidance when establishing, implementing and maintaining their anti-financial crime systems and controls;

"Ganymede" means Ganymede Cayman Ltd, a private entity incorporated in the Cayman Islands and wholly owned by Sanjay Shah, who was also the owner and controller of the Solo Group.

"Ganymede trades" means a series of trades in German and Belgian stocks executed by Bastion on 18, 19 and 30 June 2014 and 20 May 2015 on behalf of eleven clients with connections to the Solo Group.

"Handbook" means the collection of regulatory rules, manuals and guidance issued by the Authority;

"JMLSG" means the Joint Money Laundering Steering Group, which is comprised of leading UK trade associations in the financial services sector;

"JMLSG Guidance" means the 'Prevention of money laundering/combating terrorist finance guidance for the UK financial sector' issued by the JMLSG, which has been approved by a Treasury Minister in compliance with the legal requirements in the 2007 Regulations. The JMLSG Guidance sets out good practice for the UK financial services sector on the prevention of money laundering and combating terrorist financing. In this Notice, applicable provisions from the version dated 20 November 2013 and 19 November 2014 have been referred to.

The Authority has regard to whether firms have followed the relevant provisions of the JMLSG Guidance when deciding whether a breach of its rules on systems and controls against money laundering has occurred, and in considering whether to take action for a financial penalty or censure in respect of a breach of those rules (SYSC 3.2.6E and DEPP 6.2.3G);

"KYC" means Know Your Customer, which refers to CDD and EDD obligations;

"KYC pack" means the bundle of client identity information received, which usually included incorporation documents, certified copies of identity documents, utility bills and CVs;

"Matched principal trading" means a transaction where the facilitator interposes itself between the buyer and the seller to the transaction in such a way that it is never exposed to market risk throughout the execution of the transaction, with both sides executed simultaneously, and where the transaction is concluded at a price where the facilitator makes no profit or loss, other than a previously disclosed commission, fee or charge for the transaction;

"MLRO" means Money Laundering Reporting Officer;

"OTC" means over the counter trading which does not take place on a regulated exchange;

"Principles" means the Authority's Principles for Businesses as set out in the Handbook;

"Relevant Period" means the period from 29 January 2014 to 29 September 2015;

"SCP" means Solo Capital Partners LLP;

"Solo Clients" means the entities introduced by the Solo Group to Bastion and the other brokers on whose behalf Bastion executed purported equity trades for some of the clients during the Relevant Period;

"Solo Group" or **"Solo"** means the four authorised firms owned by Sanjay Shah, a British national residing in Dubai, details of which are set out in paragraph 4.6;

"Solo Trading" means purported Cum-Dividend Trading and the purported Unwind Trading executed for Solo Clients during the Relevant Period;

"Tribunal" means the Upper Tribunal (Tax and Chancery Chamber);

"UBO" means ultimate beneficial owner with "beneficial owner" being defined in Regulation 6;

"Unwind Trading" means purported trading that took place over several days or weeks to reverse the Cum-Dividend Trading to neutralise the apparent shareholding positions;

"Withholding Tax" or "WHT" means a levy deducted at source from income and passed to the government by the entity paying it. Many securities pay periodic income in the form of dividends or interest, and local tax regulations often impose a WHT on such income; and

"Withholding Tax Reclaims" means in certain cases where WHT is levied on payments to a foreign entity, the WHT may be reclaimed if there is a Double Taxation Treaty between the country in which the income is paid and the country of residence of the recipient. Double Taxation Treaties may allow for a reduction or rebate of the applicable WHT.

4. FACTS AND MATTERS

Background

Bastion

- 4.1 During the Relevant Period, Bastion was a UK-based brokerage firm, incorporated in 2004 and authorised by the Authority to deal as a matched principal or agent in a variety of investment types. It did not have permission to hold positions or client money and conducted all of its trading on a give-up basis, with clearing and settlement undertaken by separate FCA authorised entities. Bastion was not authorised to trade for retail clients and the majority of its top 20 clients during the Relevant Period were large financial institutions.
- 4.2 On 7 June 2019, a special resolution that the Firm be wound up voluntarily was passed and joint liquidators were appointed.

- 4.3 Bastion's compliance function was managed internally, although it also received support from an external compliance adviser who conducted the firm's Compliance Monitoring Programme and produced periodic reports on the Firm's compliance with rules in the Authority's handbook. Despite Bastion stating that it also relied upon the external compliance adviser to flag issues regarding the Firm's financial crime risk, in its annual firm-specific risk assessment conducted by the same external compliance adviser, such risk did not feature.
- 4.4 However, Bastion's external compliance adviser has confirmed that its advice was usually provided on a general basis and was not specific to the Solo business. In fact, the adviser stated that it was not even aware of Bastion's ongoing relationship with Solo until it was referenced in September 2014, eight months after the commencement of the Solo Trading. The adviser has also stated that it did not see the transactions that took place, and were dependant on Bastion providing records to them for review.

Bastion's Negligence

- 4.5 Bastion staff had in place inadequate systems and controls to identify and mitigate the risk of being used to facilitate fraudulent trading and money laundering in relation to business introduced by four authorised entities known as the Solo Group. In addition, Bastion staff did not exercise due skill, care and diligence in applying AML policies and procedures, and in failing to properly assess, monitor and mitigate the risk of financial crime in relation to the Solo Clients and the purported trading.

The Solo Group

- 4.6 The four authorised firms referred to by the Authority as the Solo Group were owned by Sanjay Shah, a British national currently based in Dubai:
- Solo Capital Partners LLP ("SCP") was first authorised in March 2012 and was a broker.
 - West Point Derivatives Ltd was first authorised in July 2005 and was a broker in the derivatives market.
 - Old Park Lane Capital Ltd was first authorised in April 2008 and was an agency stockbroker and corporate broker.
 - Telesto Markets LLP was first authorised on 27 August 2014 and was a wholesale custody bank and fund administrator.

- 4.7 During the Relevant Period, SCP, and others in the Solo Group at various stages, held regulatory permissions to provide custody and clearing services. The Solo Group has not been permitted to carry out any activities regulated by the Authority since December 2015 and Solo Capital Partners formally entered Special Administration insolvency proceedings in September 2016. The three other entities are in administration proceedings.

Statutory and Regulatory Provisions

- 4.8 The statutory and regulatory provisions relevant to this Notice are set out in Annex B.
- 4.9 Principle 3 requires firms to take reasonable care to organise and control their affairs responsibly and effectively, with adequate risk management systems. The 2007 Regulations and rules in the Authority's Handbook further require firms to create and implement policies and procedures to prevent and detect money laundering, and to counter the risk of being used to facilitate financial crime. These include systems and controls to identify, assess and monitor money laundering risk, as well as conducting CDD and ongoing monitoring of business relationships and transactions.
- 4.10 Principle 2 requires firms to conduct their businesses with due skill, care and diligence. A firm merely having systems and controls as required by Principle 3 is not sufficient to avoid the ever-present financial crime risk. A firm must also carefully apply those systems and controls with due skill, care and diligence as required by Principle 2 to protect itself, and to properly assess, monitor and manage the risk of financial crime.
- 4.11 Money laundering is not a victimless crime. It is used to fund terrorists, drug dealers and people traffickers as well as numerous other crimes. If firms fail to apply money laundering systems and controls, they risk facilitating these crimes.
- 4.12 As a result, money laundering risk should be taken into account by firms as part of their day-to-day operations, including those in relation to the development of new products, the taking on of new clients and changes in its business profile. In doing so, firms should take account of their customer, product and activity profiles and the complexity and volume of their transactions.
- 4.13 The JMLSG has published detailed guidance with the aim of promoting good practice and giving practical assistance in interpreting the 2007 Regulations and

evolving practice within the financial services industry. When considering whether a breach of its rules on systems and controls against money laundering has occurred, the Authority will have regard to whether a firm has followed the relevant provisions in the JMLSG guidance.

- 4.14 Substantial guidance for firms has also been published by the Authority regarding the importance of AML controls, in the form of its Financial Crime Guide, which cites examples of good and bad practice, publications of AML thematic reviews and regulatory notices.

Background of Dividend Arbitrage and the Purported Solo Trading

Dividend Arbitrage Trading

- 4.15 The aim of dividend arbitrage is to place shares in certain tax jurisdictions around dividend dates, with the aim of minimising withholding taxes or to generate WHT reclaims. WHT is a levy deducted at source from dividend payments made to shareholders.
- 4.16 If the beneficial owner is based outside of the country of issue of the shares, he may be entitled to reclaim that tax if the country of issue has a relevant treaty (a "Double Taxation Treaty") with the country of residence of the beneficial owner. Accordingly, dividend arbitrage aims at transferring the beneficial ownership of shares temporarily overseas, in sync with the dates upon which dividends become payable, in order that the criteria for making a withholding tax reclaim are fulfilled.
- 4.17 As the strategy is one of temporary transfer only, it is often executed using 'stock lending' transactions. While such transactions are structured economically as loans, the entitlement to a tax rebate depends on actual transfer of title. The legal structure of the 'loan' is therefore a sale of the shares, on condition that the borrower is obliged to supply equivalent shares to the lender at a specified future date.
- 4.18 Dividend arbitrage may give rise to significant market risk for either party as the shares may rise or fall in value during the life cycle of the loan. In order to mitigate this, the strategy will often include a series of derivative transactions, which hedge this market exposure.

- 4.19 A key role of the share custodian in connection with dividend arbitrage strategies is to issue a voucher to the beneficial owner which certifies such ownership on the date on which the entitlement to a dividend arose. The voucher will also specify the amount of the dividend and the sum withheld at source. This is sometimes known as a Dividend Credit Advice Slip' or 'Credit Advice Note'. The purpose of the voucher is for the beneficial owner to produce it (assuming the existence of a relevant Double Taxation Treaty), to the relevant tax authority to reclaim the withholding tax. The voucher generally certifies that 1) the shareholder was the beneficial owner of the share at the relevant time, 2) the shareholder had received the dividend, 3) the amount of the dividend, and 4) the amount of tax withheld from the dividend.
- 4.20 Given the nature of dividend arbitrage trading, the costs of executing the strategy will usually be commercially justifiable only if large quantities of shares are traded.

The Purported Solo Trading

- 4.21 The Authority's investigation and understanding of the purported trading in this case is based, in part, on analysis of transaction reporting data and material received from Bastion, the Solo Group, and five other Broker Firms that participated in the Solo Trading. The Solo Trading was characterised by a circular pattern of purported extremely large-scale OTC equity trading, back-to-back securities lending arrangements and forward transactions.
- 4.22 The Solo Trading can be broken into two phases:
- 1) purported trading conducted when shares were cum-dividend in order to demonstrate apparent shareholding positions that would be entitled to receive dividends, for the purposes of submitting WHT reclaims ("Cum-Dividend Trading"); and
 - 2) the purported trading conducted when shares were ex dividend, in relation to the scheduled dividend distribution event which followed the Cum-Dividend Trading, in order to reverse the apparent shareholding positions taken by the Solo Group clients during Cum-Dividend Trading ("Unwind Trading").
- 4.23 The combined volume of the purported Cum-Dividend Trading across the six Broker Firms was between 15 and 61% of the shares outstanding in the Danish stocks traded, and between 7 and 30% of the shares outstanding in the Belgian stocks traded.

- 4.24 As a broker for the equity trades, Bastion executed the purported Cum-Dividend Trading and the purported Unwind Trading. However, the Authority believes it is unlikely that Bastion would have executed both the purported cum-dividend trades and purported unwind trades for the same client in the same stock in the same size trades and therefore it is likely Bastion only saw one side of the purported trading. Additionally, the Authority considers that purported stock loans and forwards linked to the Solo Trading are likely to have been used to obfuscate and/or give apparent legitimacy to the overall scheme. However, Bastion did not execute the purported stock loans and forwards.
- 4.25 The purpose of the purported trading was to enable the Solo Group to arrange for Dividend Credit Advice Slips (“DCAS”) to be created, which purported to show that the Solo Clients held the relevant shares on the record date for dividend. The DCAS were in some cases then used to make WHT reclaims from the tax agencies in Denmark and Belgium, pursuant to Double Taxation Treaties. In 2014 and 2015, the value of Danish and Belgian WHT reclaims made, which are attributable to the Solo Group, was approximately £899.27 million and £188.00 million respectively. In 2014 and 2015, of the reclaims made, the Danish and Belgian tax authorities paid approximately £845.90 million and £42.33 million respectively.
- 4.26 The Authority refers to the trading as ‘purported’ as it has found no evidence of ownership of the shares by the Solo Clients, or custody of the shares and settlement of the trades by the Solo Group.

Bastion’s introduction to the Solo Group business

- 4.27 Prior to the Relevant Period, Bastion had a pre-existing relationship, trading futures for SCP between 15 June 2012 and 2 October 2013, although the Firm’s management was not involved in managing the day to day relationship. In that instance, Bastion had performed the function of an introducing broker and had facilitated an arrangement between SCP and one of Bastion’s clearers. SCP had been a trading client of Bastion and not a custodian with underlying clients.
- 4.28 At the start of the Relevant Period, Bastion understood SCP to be a successful hedge fund, which had the potential to become a large institution. Based on its previous work with, and knowledge of, SCP, and with a view to obtaining additional revenue, Bastion was keen to be involved when it was approached by SCP about a new line of business it was looking to conduct.

- 4.29 Bastion met with SCP early 2014 to discuss a proposal from SCP whereby Bastion would execute equity trades on behalf of clients introduced by SCP, and SCP would clear and settle the trades using its own platform. Bastion did not make and/or retain any notes of the initial meetings or discussions, but has confirmed that only onboarding and settlement processes were discussed, and not the detail of the clearing and settlement, or strategy of the proposed trading.
- 4.30 Bastion has stated that before the trading commenced it did not have any understanding about the expected size or frequency of the anticipated trading, or the level of commission it would generate for the Firm. Additionally, it stated that it did not know whether the trades would be linked to particular stocks, dates or markets.
- 4.31 Bastion signed and returned a custody agreement with SCP on 19 February 2014. A custody agreement with OPL was executed on 31 July 2014 and further service agreements with each of the Solo Group entities were signed by Bastion on 27 and 28 January 2015.

Onboarding of the Solo Clients

Introduction to Onboarding requirements

- 4.32 The 2007 Money Laundering Regulations required authorised firms to use their onboarding process to obtain and review information about a potential customer to satisfy their KYC obligations.
- 4.33 As set out in Regulation 7 of the 2007 Regulations, a firm must conduct Customer Due Diligence ("CDD") when it establishes a business relationship or carries out an occasional transaction.
- 4.34 As part of the CDD process, first, a firm must identify the customer and verify their identity. Second, a firm must identify the beneficial owner, if relevant, and verify their identity. Finally, a firm must obtain information on the purpose and intended nature of the business relationship.
- 4.35 To confirm the appropriate level of CDD that a firm must apply, a firm must perform a risk assessment, taking into account the type of customer, business relationship, product or transaction. The firm must also document its risk assessments and keep its risk assessments up to date.

- 4.36 If the firm determines through their risk assessment that the customer poses a higher risk of money laundering or terrorist financing then it must apply Enhanced Due Diligence (“EDD”). This may mean that the firm should obtain additional information regarding the customer, the beneficial owner to the extent there is one, and the purpose and intended nature of the business relationship. Additional information gained during EDD should then be used to further inform its risk assessment process in order to manage its money laundering/terrorist financing risks effectively. The information firms are required to obtain about the circumstances and business of their customers is necessary to provide a basis for monitoring customer activity and transactions, so firms can effectively detect the use of its products for money laundering and/or terrorist financing.

Chronology of the onboarding

- 4.37 On 29 January 2014, the onboarding process commenced for the Solo Clients. This involved Bastion receiving onboarding requests from the Solo Clients, which authorised Solo to supply Bastion with the clients’ KYC documents.
- 4.38 Once Bastion had received the onboarding requests, Solo supplied Bastion with the corresponding AML certificates or KYC documents which usually contained company or trust formation documents, photocopies of identity documents and occasionally CVs of the UBO or authorised representative. Solo also arranged for tri-partite give-up agreements to be signed between itself, Bastion and the Solo Clients.
- 4.39 Throughout the process, Bastion maintained a checklist of the Solo Clients which showed the stage each client was at within the onboarding process. The initial list on 13 February 2014 contained 19 clients that had requested to be onboarded, and by 19 February 2014 there were 80. In an email to Solo on 16 February 2014, Bastion acknowledged that 60 new clients would need to be set up the next week, however it had not onboarded that number of clients at once before. Bastion was also not used to having “*small hedge funds [like Solo] as a primary point of on-boarding into the regulatory environment*”.
- 4.40 Given that Bastion did not hold any prior information about the Solo Clients, it was at the point of onboarding that the Firm first became aware of the names and jurisdictions of the clients and ought to have noticed that the entities were a significant departure from its usual institutional and regulated client base.

- 4.41 By 8 June 2014, Bastion had received onboarding requests from 92 Solo Clients who were custodied with SCP. Onboarding continued throughout the Relevant Period, with the number of Solo Clients increasing significantly after OPL became involved in the Solo Trading from July 2014, and Westpoint and Telesto from February 2015.
- 4.42 By the end of the Relevant Period, Bastion had onboarded 327 Solo Clients. The Solo Clients consisted of 260 US 401(k) pension plans, 61 companies incorporated in the British Virgin Islands (BVI), the Cayman Islands, Labuan in Malaysia and Seychelles, plus 6 others incorporated in the UK, Luxembourg, Germany and UAE. More than half of these entities had been incorporated in 2014.
- 4.43 Despite such a large number of clients, the majority of the onboarding requests were sent from a limited number of representatives, which Bastion identified through the use of colour coding on the client checklists. For instance, a spreadsheet sent from SCP to Bastion on 4 March 2015 contained the names and account representatives for 165 clients, broken down across the four custodian firms. Out of the 165 clients on the list, there were just 17 representatives, each of which had a minimum of 3 clients, with one individual responsible for 38 US 401(k) pension plans, and another for 25 US 401(k) pension plans.
- 4.44 Bastion was also aware from the KYC material that some of the client representatives were former Solo employees. In fact, a CV within the KYC materials provided to Bastion showed that an ex-Solo employee was the ultimate beneficial owner of four of the Malaysian companies. Bastion also received KYC documents which showed that Sanjay Shah was the UBO and/or former director of at least one entity that Bastion onboarded.

CDD

- 4.45 CDD is an essential part of the onboarding process, which must be conducted when onboarding a new client. Firms must obtain and hold sufficient information about their clients to inform the risk assessment process and manage the risk of money laundering.
- 4.46 As part of the CDD process first, under Regulation 5 of the 2007 Money Laundering Regulations, a firm must identify the customer and verify their

identity. Second, a firm must identify the beneficial owner, if relevant, and verify their identity. Finally, a firm must obtain information on the purpose and intended nature of the business relationship.

A. Customer Identification and Verification

- 4.47 Regulation 20 of the 2007 Money Laundering Regulations requires that firms establish and maintain appropriate and risk-sensitive policies and procedures related to customer due diligence, and SYSC 6.3.1 requires that the policies must be comprehensive and proportionate to the nature, scale and complexity of its activities.
- 4.48 During the Relevant Period, Bastion's policies and procedures relating to client onboarding, financial crime and AML comprised of several documents including:
- Anti-Money Laundering (AML) and Combating Terrorist Financing (CTF) Policy dated September 2013;
 - Compliance Manual dated 1 May 2013;
 - Compliance Manual dated 6 October 2014;
- 4.49 Bastion's Compliance Manual required the Firm to obtain satisfactory evidence of the identity of each customer with whom it had a business relationship. The policy stipulated that as a minimum this ought to involve identifying the customer and beneficial owner and verifying their identities, as well as obtaining information on the purpose and intended nature of the business relationship.
- 4.50 For private and unregulated corporate entities, such as the Solo Clients, the documented procedure was that Bastion should verify the identity of directors or individuals owning more than 25% of the shares or voting rights, or individuals with principal control over the firm's assets.
- 4.51 An alternative approach was set out in an appendix to the Compliance Manual, which stated that Bastion could rely upon CDD conducted by another financial institution, in accordance with Regulation 17.
- 4.52 Regulation 17 permitted firms to place reliance on CDD conducted by other authorised firms, provided that firm consented to being relied upon, however the firm placing reliance remained responsible for any failure to apply adequate CDD. The JMLSG Guidance contained a pro-forma document, also known as an

AML certificate, the provision of which implied that consent had been provided by the firm relied upon.

- 4.53 Bastion did engage with its external compliance consultants specifically about the form of AML certificates who advised that it would need to be as per the JMLSG Guidance. Bastion agreed with its external compliance consultants that if the Firm received an "appropriate AML form or appropriate KYC documents from another FCA entity about a client then we can accept those for AML on-boarding purposes".
- 4.54 In relation to the Solo Clients, Bastion received KYC documents for some, but only AML certificates for others, although it was unclear to the firm why they were divided in this way.
- 4.55 Bastion therefore undertook two separate processes for conducting CDD on the Solo Clients:
- i) Review of KYC documents*
- 4.56 Bastion's review of KYC documents was to make sure that each new client was incorporated and controlled by "acceptable" individuals and raised queries with the custodian about the accuracy and completeness of the information.
- ii) Reliance on AML certificates from the Solo Group*
- 4.57 Bastion accepted AML certificates in lieu of KYC packs for approximately a third of the Solo Clients. The AML certificates contained the name and address of the Solo Clients and their beneficial owners, details of the directors, and stated that the Solo Group entity had conducted the appropriate CDD checks. It also stated that the certificate would not affect Bastion's responsibility to comply with applicable AML regulations.
- 4.58 AML certificates continued to be received by Bastion throughout the Relevant Period, the final batch being received in respect of 74 new clients on 6 August 2015. Bastion did request the Solo Group for these clients' KYC packs following receipt of AML Certificates. However, the Authority has seen no evidence that Bastion received any of the requested KYC packs. Nevertheless, some clients from this batch were onboarded on the same day.

B. Purpose and Intended Nature of a Business Relationship

- 4.59 As part of CDD, Regulation 5(c) of the 2007 Regulations requires firms to obtain information on the purpose and intended nature of a business relationship. The firm should use this information to assess whether a customer's financial behaviour over time is in line with expectations, whether or not the client is likely to be engaged in criminal activity, and to provide them with a meaningful basis for ongoing monitoring of the relationship.
- 4.60 Regulation 20 of the 2007 Money Laundering Regulations requires that firms establish and maintain appropriate and risk-sensitive policies and procedures related to customer due diligence, and SYSC 6.3.1R requires that the policies must be comprehensive and proportionate to the nature, scale and complexity of its activities.
- 4.61 Bastion's Compliance Manual required the Firm, in relation to corporate clients, to obtain "*sufficient additional information on the nature of company's business, and the reasons for seeking the product or service*".
- 4.62 Although not referred to in its compliance policies, Bastion had two 'Know your client forms' (one for individuals and one for corporate clients) for staff at the Firm to complete. The first question on both of the forms was 'what is the purpose and reason for the client wishing to open the account?'. Others included 'what are the client's objectives in entering into this account?' and 'what is the projected volume of business?'. Although these forms existed and were sent to other clients, Bastion did not send them to the Solo Clients and so did not obtain details about the purpose and intended nature of the Solo business from the Solo Clients.
- 4.63 Despite the questions on the form, Bastion has denied that it would normally discuss with clients the expectations of the sort of trading they would look to be doing or any limits they had, on the basis that "size is good" and "you don't go, 'Oh, this guy's doing too much size, you know. This is a problem, this is suspicious'..."
- 4.64 As the Solo Clients were a significant departure from Bastion's usual client base (see paragraph 4.40), it was particularly important for the Firm to understand the nature and purpose of the intended trading. As a result of not enquiring with the Solo Clients about the nature and expected volumes or sizes of trading, Bastion had insufficient information on which to adequately evaluate whether the trading was in line with expectations and to identify unusually large

transactions. This left Bastion exposed to the risk of facilitating financial crime, notwithstanding that the Firm did not hold client money.

- 4.65 The JMLSG Guidance also states, *“if a firm cannot satisfy itself as to the identity of a customer; verify that identity; or obtain sufficient information on the nature and intended purpose of the business relationship, it must not enter into a new relationship and must terminate an existing one”*. Despite the obvious issues with the lack of information available to Bastion about the nature and intended purpose of the business relationship, it onboarded 327 Solo Clients.

Risk assessment

- 4.66 As part of the onboarding and due diligence process, firms need to undertake and document risk assessments for every client. Such assessments should be based on information contained in the clients’ KYC documents.
- 4.67 Conducting a thorough risk assessment for each client assists firms in determining the correct level of CDD to be applied, including whether EDD is warranted. If a customer is not properly assessed, firms are unlikely to be fully apprised of the risks posed by each client, which increases the risk of financial crime.
- 4.68 Under Regulation 20 of the 2007 Regulations, firms are required to maintain appropriate and risk-sensitive policies and procedures related to risk assessments and management.
- 4.69 Bastion’s AML policy set out its risk based approach to managing money laundering risks, which was focussed on the risks presented by the firm’s customer base; products; delivery channels and geographical areas of operation.
- 4.70 Bastion’s policies and procedures failed to establish the requirement for risk assessments to be documented. Documentation of risk assessments is necessary to demonstrate the basis upon which they are being made, to keep these assessments up to date and to provide appropriate risk assessment information to authorities. Bastion’s policies also failed to set out that Bastion should document the rationale for any due diligence measures it waived when compared to its standard approach, in view of its risk assessment of a particular customer.

- 4.71 In any event, Bastion did not conduct or record risk assessments for any of the Solo Clients pursuant to its AML policy and/or its Compliance Manual.
- 4.72 The only type of risk assessment Bastion conducted across its client-base, was within the documents for its 'Risk Based MiFID Compliance Monitoring Programme'. Here, Bastion classed all its clients as 'low risk' on the basis that either: "*most clients are authorised by the FCA or equivalent*", which was something Bastion knew not to be true in relation to the Solo Clients; or because "all clients are traded on give up agreements with a clearer...[and] must have cleared the AML requirements of the clearing broker" which was not a criteria set out in the risk classification diagram or within the Firm's AML policy. This classification was inconsistent with the wording of Bastion's AML policy, which stated that "*generally our AML/CTF risk would be medium and high.*"
- 4.73 Bastion did not conduct sufficient analysis to determine whether the Solo Clients posed a higher risk of financial crime. Even a brief analysis shows the following risk factors:
- Bastion had no former relationship with the Solo Clients and failed to obtain information regarding the nature of the business each client was going to undertake. Therefore, Bastion did not have a profile against which to base an assessment of their purported trading for the purposes of ongoing monitoring.
 - The Solo Clients' KYC material showed that almost all of the clients had just a single director, shareholder and/or beneficiary.
 - In addition to none of the Solo Clients being regulated, the vast majority of them were based in countries outside the EU with no assumed regulatory equivalence.
 - The Solo Clients were introduced by the Solo Group, where there was a possibility of a conflict of interest as some UBOs were former employees of SCP. Bastion relied on AML certificates provided by Solo for their ex-employees. Because of Solo Group's relationship with their former employees, Solo Group was not in a position to provide an unbiased view.
 - Over half of the Solo Clients were US 401(k) pension plans, linked to trusts, which were classed in Bastion's AML policy as higher-risk vehicles for money laundering, especially if set up in a non-EEA country. The JMSLG has noted

that “some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering.”

- Additionally, Bastion had no awareness of how US 401(k) pension plans operated, the rules for establishment, or the limits for investment.
- None of the Solo Clients were physically present for identification purposes as the onboarding process was conducted via email. This is identified in the 2007 Regulations as being indicative of higher risk and therefore firms are required to take measures to compensate for the higher risk associated with these clients.
- The Solo Clients purportedly sought to do OTC equity trading which under the JMSLG guidance needs a more considered risk based approach and assessment.
- The transactions subsequently undertaken by Bastion on behalf of the Solo Clients were larger than the equity transactions it executed for institutional clients.

4.74 The Authority has not seen any evidence that Bastion assessed the risks posed by each Solo Client on an individual basis or that it documented the risk factors pertinent to each client or how they could be mitigated.

EDD

4.75 Firms must conduct EDD on customers which present a higher risk of money laundering, so they are able to judge whether or not the higher risk is likely to materialise.

4.76 Regulation 14(1)(b) states that firms “must apply on a risk-sensitive basis enhanced customer due diligence and enhanced ongoing monitoring in any . . . situation which by its nature can present a higher risk of money laundering or terrorist financing.” The 2007 Regulations further require firms to implement EDD measures for any client that was not physically present for identification purposes.

4.77 Regulation 20 of the 2007 Regulations requires firms to maintain appropriate and risk-sensitive policies and procedures related to customer due diligence measures, which includes enhanced due diligence. SYSC 6.3.1R further requires

that the policies must be comprehensive and proportionate to the nature, scale and complexity of its activities.

- 4.78 Bastion's AML policy required the Firm to conduct "*enhanced levels of customer, product, geographical location and transaction due diligence*" for all higher risk customers, and review the use of the accounts and transactions undertaken. Higher risk entities were described in the policy as being companies not incorporated in the UK/EU, or ones that had an opaque structure, or if the entity was cash driven such as a casino or bureau de change. The Compliance Manual also mandated that EDD was required in three specific types of relationship, including where the customer was not physically present for identification purposes; in respect of a correspondent banking relationship; and in respect of a business relationship or occasional transaction with Politically Exposed Persons.
- 4.79 A training presentation delivered to staff at Bastion by its external compliance advisers in January 2015 also stated that EDD was mandated for higher risk customers, including "*clients you do not physically meet*", which would have included the Solo Clients.
- 4.80 Bastion's policies were deficient in that they did not provide a consistent definition of higher risk customers, or a documented process which explained step-by-step how to handle higher risk clients and how to undertake EDD in order to be satisfied that Bastion had countered the risk of money laundering in each occasion. The only procedure referred to in the AML policy that was drafted to apply to all higher risk entities was a requirement to verify the identity of all directors and shareholders with an interest over 25%, albeit it was the Firm's standard policy to obtain this information for at least two directors and all shareholders with an interest over 25% for every client.
- 4.81 Aside from the above reference to verification, the EDD procedures within Bastion's compliance documents only related to specific circumstances. For example, the Compliance Manual only stipulated additional documents or verification methods which could be used in relation to non face-to-face client relationships and trust accounts. The AML policy also required the Firm to gain "an understanding of the source of funds" only in relation to 'unregulated funds', which itself was an undefined term. This piecemeal approach created a risk that adequate EDD would not be applied consistently in relation to customers that presented other high risk factors.

- 4.82 Furthermore, no guidance was given as to what would constitute “customer, product, geographical location and transaction due diligence”.
- 4.83 Given that Bastion did not meet a single Solo Client, the Firm was required to implement EDD. However, even if the clients had been present during the CDD process, for the reasons set out in paragraph 4.73, a number of risk factors indicated that the Solo Clients may have presented a higher risk of money laundering, and therefore Bastion ought to have applied EDD by obtaining additional information about the clients and the proposed trading.
- 4.84 In view of the connections between some of the Solo Clients and the Solo Group, Bastion should have recognised the risks that this posed and should have taken steps to mitigate the risk, for example, by undertaking independent enquiries on the sources of funds for the Solo Clients to ensure that they were not still financially connected to the Solo Group as employees, and had sufficient funds to conduct the anticipated trading.
- 4.85 Bastion also failed to apply a reasonable level of scrutiny as to the plausibility of the Solo Clients being able to conduct professional trading, particularly in relation to the level of funds that they would need to hold. An example of a client that was onboarded by Bastion was a 401(k) pension plan where an identity document showed that the sole beneficiary was a 18-year-old college student. The individual was also the sole beneficiary for four other pension plans onboarded by Bastion. Instead of making enquiries as how the beneficiary had sufficient funds and experience to conduct trading as a per se professional client, the purpose of such trading, or his reason for having five 401(k) Pension Plans, Bastion simply relied upon the fact that the client had been “*qualified by an FCA firm*”.
- 4.86 The Firm also considered that it was possible that the trades were leveraged in some way, or that the funding may have been provided by the Solo Group. Other than these assumptions, the Firm had no actual knowledge of the source of funds apparently available to any of the Solo Clients and did not take any steps to obtain this information, even after trading had commenced and the volumes involved had become apparent.

Client Categorisation

- 4.87 Part of the onboarding process also includes categorising clients according to the COBS rules, which is a requirement additional and separate to carrying out risk assessments. Pursuant to COBS 3.3.1R, firms must notify customers of their categorisation as a retail client, professional client or eligible counterparty. Authorised firms must assess and categorise clients based on their level of trading experience, risk knowledge and access to funds, in order to ensure suitable products are offered. Proper application of the rules also ensures that firms only act for clients within the scope of their permissions. Firms are required to notify clients as to the categorisation made by the Firm. Pursuant to COBS 3.8.2R, firms must also keep records in relation to each client, including sufficient information to support that categorisation.
- 4.88 During the Relevant Period, Bastion was authorised to deal as an agent for professional clients and eligible counterparties, which are types of clients that are considered to have experience, knowledge, and expertise to make their own investment decisions. Bastion was aware that it could not accept clients unless they were in one of these categories. There are two types of professional clients: per se professionals and elective professionals. Each of these categories has prescriptive criteria, as listed in the COBS rules.
- 4.89 Bastion's Compliance Manual contained its policy regarding client categorisation, however, it did not set out or explain a clear procedure that should be used, or the types of information and evidence Bastion was required to obtain to verify the status of its clients. Further, there was no procedure requiring Bastion to document the categorisation given to clients in accordance with COBS 3.8.2R, including the basis upon which the decision was made, with reference to the appropriate information gathered and reviewed.
- 4.90 Instead of categorising the Solo Clients according to its policy and the COBS rules, Bastion sought advice from its external compliance consultant about whether it could rely upon the categorisation of the clients given by the Solo Group, so that it would not "*need to go through the classification procedure by looking at trading experience and assets etc*".
- 4.91 Bastion received inaccurate advice that this was permissible and subsequently made a request to Solo for its client categorisation letters. When Solo questioned why the letters were needed, Bastion reiterated the advice it had received and asked for an email confirming the client name and categorisation as an

alternative option. When it did not receive a reply, Bastion emailed Solo stating that it would “*assume that Solo is classifying all clients as per se professional unless...advised otherwise when the aml kyc is sent over*”. Bastion did not independently verify this categorisation with the clients.

- 4.92 Bastion was not able to recall any instances, other than in relation to the Solo Clients, when it had sought to rely upon another firm’s categorisation in this way. Nevertheless, after sending the above email to Solo, Bastion commenced issuing client categorisation letters to the Solo Clients confirming their status as per se professionals. Although the letters asked the Solo Clients to confirm they had read and accepted the terms of the categorisation, the cover emails stated that Bastion would assume the letters were acceptable, unless it heard otherwise. There was no attempt by Bastion to determine if the Solo Clients actually met the rules set out in COBS, or to comply with the assessment process in its policy.
- 4.93 It is not clear from Bastion’s records on what basis it believed the Solo Clients could be categorised as per se professionals, other than the fact that Solo was not permitted to trade on behalf of retail clients.
- 4.94 For the type of business conducted by Bastion, per se professional clients would include authorised firms, government bodies, institutional investors or large undertakings meeting two of: a balance sheet total of EUR 20,000,000; and/or a net turnover of EUR 40,000,000; and/or own funds of EUR 2,000,000.
- 4.95 From the limited KYC material provided to Bastion, it would have been evident that a large proportion of the Solo Clients were personal pension plans with single beneficiaries and therefore not institutions. Bastion was also aware that the Solo Clients were not regulated entities. Notwithstanding this, even if Bastion had considered that the first limb of the test was met, it is noted that they did not seek any information to enable them to assess whether the second limb was met, such as evidence from the Solo Clients about their level of wealth, sufficient to judge whether they met the financial thresholds.

Ongoing monitoring

- 4.96 Regulation 8(1) requires firms to conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes scrutiny of transactions undertaken throughout the course of the

relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile.

- 4.97 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assists them to assess risk and provides greater assurance that the firm is not being used for the purpose of financial crime.

Transaction monitoring

- 4.98 As part of a firm's ongoing monitoring of a client relationship, Regulation 8 requires that firms must scrutinise transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile.
- 4.99 Furthermore, Regulation 14(1) states that enhanced ongoing monitoring must be applied in situations, which can present a higher risk of money laundering or terrorist financing.
- 4.100 Regulation 20 requires firms to have appropriate and risk-sensitive policies and procedures related to ongoing monitoring. These policies must include procedures to identify and scrutinise: 1) complex or unusually large transactions; 2) unusual patterns of activities which have no apparent economic or visible lawful purpose; and 3) any other activity which the relevant person regards as likely by its nature to be related to money laundering or terrorist financing.
- 4.101 Bastion's AML Policy stated that monitoring customer activity would include "reviewing transactions undertaken throughout the course of the customer relationship to ensure that transactions are consistent with the customer's business and risk profile". The policy also stated that the process would only be carried out in relation to higher risk customers and so should have applied to the Solo Clients for the reasons stated in paragraph 4.73.
- 4.102 The policy was deficient as it did not set out any procedures regarding how, or the frequency with which, client activity should have been monitored, even for

higher risk clients, which created a risk that transaction monitoring would not be conducted consistently or at all.

4.103 Bastion did not have an electronic surveillance system and so its trade monitoring process was reliant on the management team being involved in the trading process, who could monitor transactions "in real time". Bastion has informed the Authority that it monitored transactions for market abuse and for incorrect pricing provided to clients, however the Authority has not seen any records suggesting that the Firm checked whether the transactions were consistent with the profile of the Solo Clients, for the purpose of identifying money laundering risk.

4.104 Furthermore, Bastion did not compare the amount it had traded in the Danish and Belgian stocks to the volumes conducted on exchange, as it considered that market surveillance was not its responsibility and that other market participants would do it within the 'market transaction reporting arena'.

4.105 Bastion did not consult its external compliance advisers on whether its monitoring system (which did not include any monitoring for AML purposes) was appropriate for the volume of trades that the Firm was conducting. Furthermore, no records were kept of information provided to the external compliance advisers during their monthly visits to the Firm as part of the Compliance Monitoring Programme. The external compliance advisers have also confirmed that very little advice was given during the course of its relationship with Bastion relating specifically to the Solo business and that it never saw any of the transactions that took place. It was also not consulted about whether any of the transactions could be suspicious.

4.106 It is therefore unlikely that the compliance advisers were fully apprised of the scale of the trading executed for the Solo Clients and the associated money laundering risks. In any event, Bastion remained responsible for ensuring compliance with the relevant rules in the event of compliance outsourcing.

The Purported Solo Trading

4.107 During the Relevant Period, Bastion purportedly executed high volume Cum-Dividend trades for the Solo Clients worth approximately £49 billion in Danish equities and £22 billion in Belgian equities, and received commission of £1.55 million, which made up 26% of Bastion's total revenue for the Relevant Period.

- 4.108 Bastion started executing the purported trades on behalf of the Solo Clients on 26 February 2014. The trades were initially purportedly cleared by SCP, although it was extended to other entities of the Solo Group from July 2014 onwards.
- 4.109 From 26 February 2014, orders were placed via email and the purported trades were executed using a post-trade order matching platform that relied on the brokers uploading trade details into spreadsheets before they were approved by the custodians.

Brokermesh

- 4.110 From 25 February 2015, the order and trading process was automated using a system called Brokermesh. This was an electronic platform, developed by an entity associated with the Solo Group, which generated trade orders from clients and sourced and matched liquidity amongst the Solo Clients and brokers including Bastion. The purported trading on the platform was conducted via an automated process whereby once an order appeared on the system, a broker would seek liquidity from the Solo Clients available on the system. Then, once the liquidity was established, the order would be matched subject to trade authorisation from the relevant custodian.
- 4.111 Liquidity on the Brokermesh platform was sourced from a closed network consisting only of Solo Clients, of which Bastion onboarded 327 during the Relevant Period. Nevertheless, Bastion has recollected that liquidity was virtually always found, and whilst the time varied, liquidity was generally found within one day.
- 4.112 Bastion considered that Brokermesh was similar to other trade settlement platforms on the market. However, the functionality differed from other legitimate trading platforms as trading records were wiped from Bastion's view the day after the trades took place, and so it was necessary for the Firm to retain its own records.
- 4.113 In one instance, on 30 March 2015 Bastion was purportedly able to source liquidity to buy shares in a Danish listed stock within six minutes for a trade that represented over 4 times the volume of shares traded in that stock on European exchanges on that date. In total that day, for the same stock, Bastion purportedly executed trades approximately 97 times the number of shares traded on all European exchanges.

A. Trade sizes

4.114 During the Relevant Period, Bastion purportedly executed Cum-Dividend Trading to the value of approximately £49.03 billion in Danish equities and £22.48 billion in Belgian equities on behalf of Solo Clients.

4.115 Analysis of the Cum-Dividend Trading reveals the following:

- Between February 2014 and August 2015, Bastion purportedly executed orders on behalf of Solo Clients in 16 listed Danish stocks over 22 cum-dividend dates. An average of 14.98% of the outstanding shares in each stock was traded, which were cumulatively worth a total of £49 billion. The volumes also equated to an average of 40 times the total number of all shares traded in those stocks on European exchanges.
- Between February 2014 and August 2015, Bastion purportedly executed orders on behalf of Solo Clients in 15 listed Belgian stocks over 14 cum-dividend dates. An average of 5.81% of the outstanding shares in each stock was traded, which were cumulatively worth a total of £22 billion. The volumes also equated to an average of 22 times the total number of all shares traded in those stocks on European exchanges.

4.116 The Authority considers that it is significant for market surveillance and visibility that individual trades were below the applicable disclosable thresholds. For example, Section 29 of the Danish Securities Trading Act required shareholders holding over 5% of Danish-listed stock to be publicised. Similarly Belgian law requires pursuant to Article 6 of the 'Law of 2 May 2007 on disclosure of major holdings in issues whose shares are admitted to trading on a regulated market and laying down miscellaneous provisions' requires holders of more than 5% of the existing voting rights to notify the issuer and the Belgian Financial Services Markets Authority of the number and proportion of voting rights that he/she holds.

4.117 Bastion has confirmed that it was aware of the large size of the trading, but did not consider whether the size and volume of the transactions were in line with expectations of the Solo Clients. In this context, it believed that 'no trade was too big' and that large trade sizes could not be indicative of market abuse. Furthermore, the Firm did not consider that it was part of its role to consider whether trades were too large for the customer type. This was notwithstanding

that the purported trades for the Solo Clients were larger than the Firm had executed for its institutional clients.

- 4.118 A possible explanation suggested by Bastion for the large sizes of the purported trades was that they were highly leveraged, however there is no evidence that Bastion was told by the Solo Group or the Solo Clients that the trades would be leveraged.
- 4.119 Bastion has stated that it would check the volumes of shares it had purportedly traded against the number of shares outstanding in the market on a daily basis, and was aware that they regularly exceeded 8%. However, the volumes did not concern the firm as it considered that an unrealistic volume would be "maybe 101%". Instead, the firm took comfort from the fact that the high volume trades were transaction reported by a FCA regulated firm and continued over a period of 18 months.
- 4.120 The issue that did concern Bastion once trading commenced was the level of commission received, which was dependent upon the brokerage level and volume. Bastion was not concerned with other aspects of the trading including the impact the trades had on the market on either an individual or cumulative basis.
- 4.121 Bastion took the view that because they were executing brokers, and the trades were subject to custodian approval, the size of trades was not their risk responsibility. Although execution-only broking may have reduced counterparty risk, all regulated firms must consider and mitigate the risk that they could be used to facilitate financial crime, even if client monies do not flow through the firm.
- 4.122 As the Firm perceived that it bore no risk of loss, it failed to recognise more general risks, including financial crime risk, which applies to all regulated firms. Consequently, there is no evidence that the Firm appreciated the potential risk that the Firm might be used to 'further money laundering'. The Authority has published considerable guidance on managing the risk of financial crime, particularly in its Financial Crime Guide which was first published in December 2011 and which Bastion ought to have been aware of.

B. Trading Red Flags

4.123 Once the purported Solo Trading commenced, a number of red flags in relation to the trading ought to have alerted Bastion to the risk that it could be used for the purposes of financial crime and prompted it to obtain explanations from the Solo Group or the Solo Clients on a number of matters, decline to execute particular trades, or cease its trading relationship with the Solo Clients:

- The Solo Clients placed extremely high value trades, yet most of them had only been recently incorporated, were based in non-EU/EEA countries and in a number of instances, were managed or owned by a single shareholder and/or UBO or former employees of the Solo Group.
- For the recently incorporated 401(k) pension plans, the value of the purported trades far exceeded the investment amounts which could reasonably have accrued given the annual contribution limits and limited number of ultimate beneficial owners, which should have alerted Bastion as to the unrealistic nature of the trades.
- The Solo Group purported to have sourced a custom automatic trade matching and settlement platform from an entity owned by Mr Shah. Brokermesh was able to locate liquidity for OTC trades worth over £36.5 billion that were purportedly executed by Bastion, even though access to the platform was limited to a closed pool of clients introduced to the Brokers Firms by the Solo Group.
- Bastion purportedly traded an average of 14.98% of the shares outstanding in the market on major listed Danish stocks, in circumstances where share ownership over 5% required publication. This was an average of 40 times higher than were reported on European exchanges for the same Danish stocks.

4.124 Bastion failed to identify or mitigate any red flags arising from the Solo Trading and as a consequence of this, failed to sufficiently address the risk that it might be used for the purposes of financial crime.

The Ganymede trades

Summary

4.125 As part of assessing how the Firm might likely be used for the purposes of money laundering and financial crime, Bastion was required to assess the risks posed

by its clients' trading behaviours, particularly in instances where there was no apparent economic or lawful purpose.

- 4.126 Firms must have adequate policies and procedures, systems and controls which provide for the identification and scrutiny of complex or large transactions; unusual patterns of transactions which have no apparent economic or visible lawful purpose; and any other activity which may be related to money laundering.
- 4.127 As set out in further detail below, on 18, 19 and 30 June 2014 and 20 May 2015, Bastion executed a series of trades in German and Belgian listed stocks on behalf of 11 Solo Clients. Together these trades (the "Ganymede trades") resulted in a single client entitled Ganymede Cayman Ltd ("Ganymede"), owned by Sanjay Shah, making a loss of EUR €22,729,508.15 million to the benefit of the remaining 10 clients. The Ganymede trades had no apparent economic purpose except to transfer funds from a Sanjay Shah controlled entity to his associates and individuals connected with the Solo Group.
- 4.128 The Ganymede trades materially differed from the Solo Trading for the following reasons, as they:
- a) were not executed based on cum-dividend dates;
 - b) were executed using intraday prices, instead of end of day prices;
 - c) were executed on behalf of a small number of new clients to Bastion, from high risk jurisdictions, who were 'urgently' onboarded at the request of the Solo Group in the days before the transactions took place;
 - d) were reversed by the same clients within hours, at different prices, meaning a substantial net loss for one client and profits for the other parties, therefore making the economic rationale for the transactions unclear and/or highly suggestive of money laundering.
 - e) trades had been carried out between clients with Bastion as the only broker executing the buy and sell orders.

Chronology of the Ganymede Trades

- 4.129 On 16 June 2014, Bastion received onboarding requests from four new clients, as set out below.

- Client A was a private company that had been incorporated in the British Virgin Islands on 3 June 2014. The sole director and shareholder of Client A was a Dubai based individual who had held a senior position at SCP. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.
- Client B was a private company that had been incorporated in the British Virgin Islands on 5 June 2014. The CV supplied for the director of Client B showed that he was a current employee of SCP. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.
- Client C was a private company incorporated in the Cayman Islands on 18 February 2013. The client's KYC documents showed that one of the two directors was 21 years old and had a total of four months experience working at a financial services firm that was subsequently purchased by the Solo Group on 6 July 2015. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.
- Client D was a private company that had been incorporated in the Cayman Islands on 4 October 2013. The sole director and shareholder was a Dubai based individual. The email from SCP attaching the KYC documents stated that it was an 'urgent onboarding'.

4.130 On 17 June 2014, Bastion received onboarding requests from a further three clients:

- Client E was a private company incorporated in the Seychelles on 28 April 2014. The sole director and shareholder was an individual who held a senior position at SCP until 2013.
- Client F was a private company incorporated in the Seychelles on 25 March 2014. The sole director and shareholder was a Hong Kong based individual who was a current employee of SCP.
- Ganymede was a private company incorporated in the Cayman Islands on 16 June 2010. The sole director and shareholder was Sanjay Shah.

4.131 Bastion stated that it felt pressured by SCP to urgently onboard these clients, particularly as it was told that one of the client entities was owned by Sanjay Shah. On the morning of 18 June 2014, Bastion confirmed to SCP that it had onboarded six of the entities but was yet to receive KYC documents for Client F.

SCP thanked Bastion for onboarding the entities so quickly and sent the remaining KYC documents to the Firm at 09:16 on 18 June 2014.

- 4.132 Three hours later, between 12:49 and 13:29, Bastion received a series of trade orders via email from Clients A to F requesting to buy equity shares in varying volumes in a German listed stock ("German stock A"). All of the orders requested an identical specific intraday purchase price of €160.1, which was around the same as the market closing price on 17 June 2014 of €160.12, but below the exchange price at 12:49 of €160.95. One of the orders from Client E was written as if the trade had already been agreed, which was also suggestive of the coordinated nature of the trades. It stated "[Client E] buys [German stock A], 668,521 160.1". This was subsequently corrected by the client, who re-sent the order in a "more cleanly written" format.
- 4.133 At 13:12, Bastion sought liquidity from Ganymede and stated "I have some form on [German stock A], are you in the market today for this?" A few minutes later another email from Bastion to Ganymede stated "I need to buy 3303496, can you show me an offer please?". At 13:47 Ganymede responded and stated that it could sell 3,964,905 shares at a price of €160.10. This in fact corresponded to the total number of shares in German stock A requested by Clients A to F and at the requested identical specific intraday purchase price of €160.1.
- 4.134 At 14:23, approximately an hour after the trades had been agreed, Ganymede indicated that it wanted to buy back the 3,964,905 shares in German stock A, equivalent to the amount it had just sold. Bastion approached Clients A to F who all replied agreeing to sell the shares they had just purchased. Five of the six clients proactively offered an identical price of €160.97, which was accepted by Ganymede. This price was €0.87 above the price Ganymede had sold the shares for, but was below the current exchange price of €161.05. At 15:10, Bastion confirmed to Ganymede that it had purchased all 3,964,905 German stock A shares at a price of €160.97.
- 4.135 The result of the trading was that Ganymede sold 3,964,905 shares in German stock A for consideration of €634,781,290.50 to six clients (Clients A to F). It then re-purchased the same shares an hour later at a higher price for consideration of €638,230,757.85, resulting in a net loss to Ganymede of €3,449,467.35, to the benefit of Clients A to F.

The timing of the orders was as follows:

| Time of order | Buyer | Time of Trade | Seller | Quantity | Unit Price (€) | Consideration (€) |
|---------------|----------|---------------|----------|----------|----------------|-------------------|
| 12:49:53 | Client E | 13:47 | Ganymede | 668,521 | 160.1 | 107,030,212.10 |
| 12:55:53 | Client B | 13:47 | Ganymede | 653,125 | 160.1 | 104,565,312.50 |
| 12:55:54 | Client F | 13:47 | Ganymede | 658,963 | 160.1 | 105,499,976.30 |
| 12:57:36 | Client A | 13:47 | Ganymede | 673,505 | 160.1 | 107,828,150.50 |
| 13:00:58 | Client D | 13:47 | Ganymede | 649,382 | 160.1 | 103,966,058.20 |
| 13:29:19 | Client C | 13:47 | Ganymede | 661,409 | 160.1 | 105,891,580.90 |
| 14:23 | Ganymede | 14:36 | Client D | 649,382 | 160.97 | 104,531,020.54 |
| 14:23 | Ganymede | 14:36 | Client A | 673,505 | 160.97 | 108,414,099.85 |
| 14:23 | Ganymede | 14:38 | Client E | 668,521 | 160.97 | 107,611,825.37 |
| 14:23 | Ganymede | 14:42 | Client B | 653,125 | 160.97 | 105,133,531.25 |
| 14:23 | Ganymede | 14:52 | Client F | 658,963 | 160.97 | 106,073,274.11 |
| 14:23 | Ganymede | 15:05 | Client C | 661,409 | 160.97 | 106,467,006.73 |

4.136 Another possible indicator of the co-ordinated nature of these Ganymede trades was that at 16:16 Ganymede indicated to Bastion that it wanted to trade again and would be “*send[ing] something through shortly*”. However, at 16:29, it was not Ganymede but Client E that sent through an order to buy German stock A at a specific price of €160.25. This was quickly followed by similar trade orders from Client F and Client A, which prompted Bastion to email Ganymede at 16:44 asking if it had any German stock A to sell. At 16:55, Ganymede replied offering to sell 11,279,140 shares (which was the exact cumulative total of the trade orders from Clients E, F and A to whom it had sold and then repurchased the shares from just ninety minutes earlier) at the same specific price of €160.25. At 16:58, Bastion confirmed to Ganymede that the order had been filled.

4.137 Just two minutes later, Ganymede began the process of unwinding the trade and buying back the shares at a higher price, as it had done earlier that day. This time, the price Ganymede specified was €161.25, which was €1 more per share

than it had sold them for, and above the market closing price of €161. After receiving the order from Ganymede, Bastion approached Clients A, E and F and re-purchased the shares, resulting in a loss of €11,279,140 for Ganymede.

The timing of the orders was as follows:

| Time of order | Buyer | Time of Trade | Seller | Quantity | Unit Price (€) | Consideration (€) |
|---------------|----------|---------------|----------|-----------|----------------|-------------------|
| 16:29 | Client E | 16:58 | Ganymede | 4,657,387 | 160.25 | 746,346,266.75 |
| 16:31 | Client F | 16:58 | Ganymede | 4,107,702 | 160.25 | 658,259,245.50 |
| 16:39 | Client A | 16:58 | Ganymede | 2,514,051 | 160.25 | 402,876,672.75 |
| 17:00 | Ganymede | 17:07 | Client A | 2,514,051 | 161.25 | 405,390,723.75 |
| 17:00 | Ganymede | 17:13 | Client F | 4,107,702 | 161.25 | 662,366,947.50 |
| 17:00 | Ganymede | 17:17 | Client E | 4,657,387 | 161.25 | 751,003,653.75 |

4.138 The methodology described above was again employed by Ganymede and other Solo Clients linked to the Solo Group in a series of trades executed by Bastion on 19 June 2014, 30 June 2014 and 20 May 2015, resulting in a total loss to Ganymede of €22,729,508.15 across the four days.

Analysis of the Ganymede Trades

4.139 All of the Ganymede trades involved the shares purportedly being repurchased by Ganymede the same day, within the T+2 or T+3 settlement period, and therefore the shares did not need to be transferred. The net result of the trading was that a total of €22,729,508.15 was owed by Ganymede to the other clients.

4.140 Bastion has confirmed that it was aware that the Ganymede trades resulted in losses to Ganymede. However, it failed to question the rationale for the trading as it considered that there might have been other simultaneous transactions involving the same clients, that the Firm was not privy to. However, Bastion was the only broker involved in these trades and in each instance arranged the buy and sell transactions. Even if there had been other legs of the transactions that

Bastion was not aware of, Bastion ought to have recognised from the buy and sell transactions that the losses to Ganymede resulted in direct profits for the other counterparties. At a minimum, this should have caused the Firm to question the clients about the rationale for the trading and consider whether the nature of these series of transactions were suspicious.

4.141 Furthermore, if Bastion had examined the trade orders prior to trading on 18 June 2014, or for the purpose of transaction monitoring and post trade surveillance after trading, it ought to have noticed that the requested volume of 11,279,140 shares on 18 June 2014 was 17 times the Average Daily Volume (ADV) of German stock A shares sold on European exchanges. If Bastion had noticed this red flag on receiving the trade order, it should have declined to execute the trade, or at a minimum queried the volumes with the clients.

4.142 Instead, Bastion failed to identify and/or flag any queries in relation to the unusual features of the Ganymede trades, either internally, or with the clients, or the Solo Group, including:

- a) why the clients had to be urgently onboarded;
- b) why the majority of the clients' directors/UBOs were connected to the Solo Group;
- c) why the shares were purchased and sold at intraday prices, instead of the usual end of day price;
- d) why the trades were unwound on the same day;
- e) why the orders from clients A, B, D, E and F specified identical prices;
- f) why the specified price was below the current intraday market price;
- g) why the volume of shares transacted was 17 times the ADV of German Stock A shares sold on European exchanges;
- h) why Ganymede would want to buy back the shares it had sold a short while earlier at a higher price, resulting in a loss for it on each occasion; and
- i) why the Ganymede trades on 20 May 2015 took place by email, even though all other Solo Trading took place on Brokermesh at that time;

4.143 At a minimum, these red flags should have prompted Bastion to question the clients about the purpose of the trading, however Bastion did not query the

Ganymede trades with Ganymede or flag the potential loss to the client before or after execution.

4.144 Bastion ought to have queried how these clients would have been able to source such sizeable liquidity in such short order, whether this liquidity was in line with the trading levels which could be expected from these clients, given the information previously obtained through CDD.

4.145 Bastion has stated that it did not have any suspicions about the Ganymede trades as it trusted Sanjay Shah's reputation. This raises serious concerns about the firm's risk appetite and the extent and effectiveness of its transaction monitoring.

End of the Purported Solo Trading

4.146 Bastion executed its last trade for a Solo Client on 29 September 2015. The Solo Clients ceased the purported trading with all the six Broker Firms after unannounced visits by the Authority to the offices of the Solo Group entities and the Broker Firms between 2 – 4 November 2015.

Bastion failed to Identify Any of the Above Issues

4.147 Bastion failed to identify any of the above issues. With respect to AML, in both 2014 and 2015, Bastion did not identify any transactions raising any suspicions and no breaches were reported or observed.

5. FAILINGS

5.1 The statutory and regulatory provisions relevant to this Notice are referred to in Annex B.

5.2 The JMLSG Guidance has also been included in Annex B, because in determining whether breaches of its rules on systems and controls against money laundering have occurred, and in determining whether to take action for a financial penalty or censure in respect of a breach of those rules, the Authority has also had regard to whether Bastion followed the JMLSG Guidance.

Principle 3

5.3 Principle 3 requires a firm to take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.

5.4 Bastion breached this requirement during the Relevant Period, in relation to business related to the Solo Group, as its policies and procedures were inadequate for identifying, assessing and mitigating the risk of financial crime as they failed to:

5.4.1 Establish the requirement for risk assessments to be documented, as well as to document the rationale for any due diligence measures the firm waived when compared to its standard approach, in view of its risk assessment of a particular customer;

5.4.2 Set out adequate processes and procedures for EDD;

5.4.3 Set out adequate processes and procedures for client categorisation;

5.4.4 Set out adequate processes and procedures for transaction monitoring, including how transactions are monitored, and with what frequency, and set out adequate processes and procedures for how to identify suspicious transactions.

Principle 2

5.5 The Authority considers that Bastion failed to act with due skill, care and diligence as required by Principle 2 to properly assess, monitor and manage the risk of financial crime associated with the business related to the Solo Group in that the Firm:

- a) Failed to properly conduct customer due diligence prior to onboarding, and consequently failed to identify that the Solo Clients presented a higher risk of financial crime before they started trading;
- b) Failed to gather adequate information to enable it to understand the purpose and intended nature of the business that the Solo Clients were going to undertake, the likely size or frequency of the purported trading intended by the Solo Clients or their source of funds;
- c) Failed to undertake and document a risk assessment for each of the Solo Clients prior to onboarding and trading for the Solo Clients;
- d) Failed to complete EDD for any of the Solo Clients despite the fact that none of the Solo Clients were physically present for identification purposes and a number of other risk factors were present;

- e) Failed to assess each of the Solo Clients against the categorisation criteria set out in COBS 3.5.2R and failed to record the results of such assessments, including sufficient information to support the categorisation, contrary to COBS 3.8.2(2)(a);
- f) Failed to conduct transaction monitoring of the Solo Clients' purported trades;
- g) Failed to recognise numerous red flags with the purported trading, including failing to consider whether it was plausible and/or realistic that sufficient liquidity was sourced within a closed network of entities for the size and volumes of trading conducted by the Solo Clients. Likewise, failing to consider or recognise that the profiles of the Solo Clients meant that they were highly unlikely to meet the scale and volume of the trading purportedly being carried out, and/or failed to at least obtain sufficient evidence of the clients' source of funds to satisfy itself to the contrary; and
- h) Failed to recognise numerous red flags arising from the purported Ganymede trades and adequately consider financial crime and money laundering risks they posed to the Firm.

6. SANCTION

- 6.1 The Authority has considered the disciplinary and other options available to it and has concluded that a financial penalty is the appropriate sanction in the circumstances of this particular case.
- 6.2 The Authority's policy on the imposition of financial penalties is set out in Chapter 6 of DEPP. In determining the proposed financial penalty, the Authority has had regard to this guidance.
- 6.3 DEPP 6.5A sets out a five-step framework to determine the appropriate level of financial penalty.

Step 1: disgorgement

- 6.4 Pursuant to DEPP 6.5A.1G, at Step 1 the Authority seeks to deprive a firm of the financial benefit derived directly from the breach where it is practicable to quantify.
- 6.5 The financial benefit associated with Bastion's failings is quantifiable by reference to the revenue it derived from the business related to the Solo Group as described in the Notice.

6.6 The figure after Step 1 is therefore **£1,554,855.40**.

Step 2: the seriousness of the breach

6.7 Pursuant to DEPP 6.5A.2G, at Step 2 the Authority determines a figure that reflects the seriousness of the breach. Where the amount of revenue generated by a firm from a particular product line or business area is indicative of the harm or potential harm that its breach may cause, that figure will be based on a percentage of the firm's revenue from the relevant products or business area.

6.8 The Authority considers that the revenue generated by Bastion is indicative of the harm or potential harm caused by its breach. The Authority has therefore determined a figure based on a percentage of Bastion's revenue during the period of the breach.

6.9 Bastion's revenue is the revenue derived from business associated with the Solo Group. The period of Bastion's breach was between 29 January 2014 and 29 September 2015. The Authority considers Bastion's revenue for this period to be £1,554,855.40.

6.10 In deciding on the percentage of the revenue that forms the basis of the step 2 figure, the Authority considers the seriousness of the breach and chooses a percentage between 0% and 20%. This range is divided into five fixed levels which represent, on a sliding scale, the seriousness of the breach; the more serious the breach, the higher the level. For penalties imposed on firms there are the following five levels:

Level 1 – 0%

Level 2 – 5%

Level 3 – 10%

Level 4 – 15%

Level 5 – 20%

6.11 In assessing the seriousness level, Authority takes into account various factors which reflect the impact and nature of the breach, and whether it was committed deliberately or recklessly. DEPP 6.5A.2G lists factors likely to be considered 'level 4 or 5 factors'. Of these, the Authority considers the following factors to be relevant:

1. The breaches revealed serious or systemic weaknesses in both the Firm's procedures and the management systems or internal controls relating to all or part of the Firm's business; and
 2. The breaches created a significant risk that financial crime would be facilitated, occasioned or otherwise occur.
- 6.12 Taking all of these factors into account, Authority considers the seriousness of the breach to be level 4 and so the Step 2 figure is 15% of £1,554,855.40.
- 6.13 Step 2 is therefore **£233,228.31**.

Step 3: Mitigating and aggravating factors

- 6.14 Pursuant to DEPP 6.5A.3G, at Step 3, the Authority may increase or decrease the amount of the financial penalty arrived at after Step 2, but not including any amount to be disgorged as set out in Step 1, to take into account factors which aggravate or mitigate the breach.
- 6.15 The Authority considers that the following factors aggravates the breach:
- (1) The Authority and the JMLSG have published numerous documents highlighting financial crime risks and the standards expected of firms when dealing with those risks. The most significant publications include the JMLSG Guidance and Financial Crime Guide (including the thematic reviews that are referred to therein) which was first published in December 2011. These publications set out good practice examples to assist firms, for example in managing and mitigating money laundering risk by (amongst other things) conducting appropriate customer due diligence, monitoring of customers' activity and guidance of dealing with higher-risk situations. Given the number and detailed nature of such publications, and past enforcement action taken by the Authority in respect of similar failings by other firms, Bastion should have been aware of the importance of appropriately assessing, managing and monitoring the risk that the Firm could be used for the purposes of financial crime.
- 6.16 Having taken into account these aggravating and mitigating factors, the Authority considers that the Step 2 figure should be increased by 10%.
- 6.17 Step 3 is therefore **£256,551.14**.

Step 4: adjustment for deterrence

- 6.18 Pursuant to DEPP 6.5A.4G, if the Authority considers that the figure arrived at after Step 3 is insufficient to deter the firm who committed the breach, or others, from committing further of similar breaches, then the Authority may increase the penalty.
- 6.19 The Authority considers that DEPP 6.5A.4G(1)(a) is relevant in this instance and has therefore determined that this is an appropriate case where an adjustment for deterrence is necessary. Without an adjustment for deterrence, the financial penalty would be £256,551.14. In the circumstances of this case, the Authority considers that a penalty of this size would not serve as a credible deterrent to Bastion and others. This small penalty does not meet the Authority's objective of credible deterrence. As a result, it is necessary for the Authority to increase the penalty to achieve credible deterrence.
- 6.20 Having taken into account the factor outlined in DEPP 6.5A.4G, the Authority considers that a multiplier of five should be applied at Step 4.
- 6.21 Step 4 is therefore **£1,282,755.71**.

Step 5: settlement discount

- 6.22 Pursuant to DEPP 6.5A.5G, if the Authority and the firm on whom a penalty is to be imposed agree the amount of the financial penalty and other terms, DEPP 6.7 provides that the amount of the financial penalty which might otherwise have been payable will be reduced to reflect the stage at which the Authority and the firm reached agreement. The settlement discount does not apply to the disgorgement of any benefit calculated at Step 1.
- 6.23 The Authority and Bastion did reach agreement to settle so a 30% discount applies to the Step 4 figure.
- 6.24 The total financial penalty (that would have been imposed) is therefore **£2,452,700**.

7. PROCEDURAL MATTERS

- 7.1 This Notice is given to Bastion under and in accordance with section 390 of the Act.
- 7.2 The following statutory rights are important.

Decision maker

7.3 The decision which gave rise to the obligation to give this Notice was made by the Settlement Decision Makers.

Manner and time for payment

7.4 The financial penalty must be admitted in the liquidation of the Firm by no later than 14 days from the date of the Final Notice. The financial penalty will be ranked with other creditors of the Firm but the Authority will keep it under review in order that legitimate creditors are satisfied prior to any funds realised in the liquidation being used to pay some, or all, of the financial penalty.

Publicity

7.5 Sections 391(4), 391(6) and 391(7) of the Act apply to the publication of information about the matter to which this notice relates. Under those provisions, the Authority must publish such information about the matter to which this notice relates as the Authority considers appropriate. The information may be published in such manner as the Authority considers appropriate. However, the Authority may not publish information if such publication would, in the opinion of the Authority, be unfair to you or prejudicial to the interests of consumers or detrimental to the stability of the UK financial system.

7.6 The Authority intends to publish such information about the matter to which this Final Notice relates as it considers appropriate.

Authority contacts

7.7 For more information concerning this matter generally, contact Giles Harry (direct line: 020 7066 8072) at the Authority.

Mario Theodosiou

Head of Department

Financial Conduct Authority, Enforcement and Market Oversight Division

ANNEX A: CHRONOLOGY

| | |
|------------------------------|---|
| 2004 | Bastion was incorporated and authorised by the Authority. |
| January 2014 | Initial discussions took place with SCP. |
| 19 February 2014 | Bastion signed a custody agreement with SCP. |
| 29 January-April 2014 | Initial onboarding of Solo Clients. |
| 26 February 2014 | Trading commenced in Danish stocks. |
| 17 April 2014 | Trading commenced in Belgian stocks. |
| 16/17 June 2014 | "Urgent" onboarding of 7 new clients. |
| 18/19/30 June 2014 | Trades in German and Belgian stocks via the 7 recently onboarded clients, resulting in total losses to Ganymede Cayman of €18.52 million. |
| 27 January 2015 | Further services agreement with Solo Group signed by Bastion. |
| 28 January 2015 | Services Agreements and Transaction Reporting Notices signed with West Point and Telesto. |
| 3 February 2015 | Services Agreement signed with OPL. |
| 18 February 2015 | Brokermesh licence agreement signed. |
| 25 February 2015 | Trading on Brokermesh commenced. |
| 20 May 2015 | Further trade in German stock resulting in a loss of €1.86m for Ganymede Cayman. |
| 1 June 2015 | Last cum-dividend trade in Belgian stock by Bastion on Brokermesh. |
| 6 August 2015 | Last batch of Solo Clients onboarded by Bastion. |
| 7 August 2015 | Last cum-dividend trade in Danish stock by Bastion on Brokermesh |
| 29 September 2015 | Last instance of Unwind Trading by Bastion for Solo Clients. |
| 3 November 2015 | Unannounced visit by the Authority. |

ANNEX B: RELEVANT STATUTORY AND REGULATORY PROVISIONS

RELEVANT STATUTORY PROVISIONS

- 1.1 Pursuant to sections 1B and 1D of the Act, one of the Authority's operational objectives is protecting and enhancing the integrity of the UK financial system.
- 1.2 Pursuant to section 206 of the Act, if the Authority considers that an authorised person has contravened a requirement imposed on it by or under the Act, it may impose on that person a penalty in respect of the contravention of such amount as it considers appropriate.

THE 2007 REGULATIONS

- 1.3 Regulation 5 provides:

Meaning of customer due diligence measures

"Customer due diligence measures" means—

- (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;*
- (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and*
- (c) obtaining information on the purpose and intended nature of the business relationship."*

- 1.4 Regulation 6 provides:

Meaning of beneficial owner

In the case of a body corporate, "beneficial owner" means any individual who—

- (a) as respects any body other than a company whose securities are listed on a regulated market, ultimately owns or controls (whether through direct or indirect ownership or control, including through bearer share holdings) more than 25% of the shares or voting rights in the body; or*
- (b) as respects any body corporate, otherwise exercises control over the management of the body.*

In the case of a trust, "beneficial owner" means—

- (a) any individual who is entitled to a specified interest in at least 25% of the capital of the trust property;*

(b) as respects any trust other than one which is set up or operates entirely for the benefit of individuals falling within sub-paragraph (a), the class of persons in whose main interest the trust is set up or operates;

(c) any individual who has control over the trust.

1.5 Regulation 7 provides:

Application of customer due diligence measures

(1) ..., a relevant person must apply customer due diligence measures when he—

(a) establishes a business relationship;

(b) carries out an occasional transaction;

(c) suspects money laundering or terrorist financing;

(d) doubts the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(2) Subject to regulation 16(4), a relevant person must also apply customer due diligence measures at other appropriate times to existing customers on a risk-sensitive basis.

1.6 Regulation 8 provides:

Ongoing monitoring

"(1) A relevant person must conduct ongoing monitoring of a business relationship.

(2) "Ongoing monitoring" of a business relationship means—

(a) scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the relevant person's knowledge of the customer, his business and risk profile; and

(b) keeping the documents, data or information obtained for the purpose of applying customer due diligence measures up-to-date.

(3) Regulation 7(3) applies to the duty to conduct ongoing monitoring under paragraph (1) as it applies to customer due diligence measures. "

1.7 Regulation 14 provides:

Enhanced customer due diligence and ongoing monitoring

"(1) A relevant person must apply on a risk-sensitive basis enhanced customer due diligence measures and enhanced ongoing monitoring—

(a) in accordance with paragraphs (2) to (4);

(b) in any other situation which by its nature can present a higher risk of money laundering or terrorist financing.

(2) Where the customer has not been physically present for identification purposes, a relevant person must take specific and adequate measures to compensate for the higher risk, for example, by applying one or more of the following measures—

(a) ensuring that the customer's identity is established by additional documents, data or information;

(b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the money laundering directive;

(c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution."

1.8 Regulation 17 provides:

Reliance

"(1) A relevant person may rely on a person who falls within paragraph (2) (or who the relevant person has reasonable grounds to believe falls within paragraph (2)) to apply any customer due diligence measures provided that—

(a) the other person consents to being relied on; and

(b) notwithstanding the relevant person's reliance on the other person, the relevant person remains liable for any failure to apply such measures.

(2) The persons are—

(a) a credit or financial institution which is an authorised person;

...

*(4) Nothing in this regulation prevents a relevant person applying customer due diligence measures by means of an outsourcing service provider or agent provided that the relevant person remains liable for any failure to apply such **measures.**"*

1.9 Regulation 20 provides:

Policies and Procedures

"(1) A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to—

(a) customer due diligence measures and ongoing monitoring;

(b) reporting;

(c) record-keeping;

(d) internal control;

(e) risk assessment and management;

(f) the monitoring and management of compliance with, and the internal communication of, such policies and procedures,

in order to prevent activities related to money laundering and terrorist financing.

(2) The policies and procedures referred to in paragraph (1) include policies and procedures—

(a) which provide for the identification and scrutiny of—

(i) complex or unusually large transactions;

(ii) unusual patterns of transactions which have no apparent economic or visible lawful purpose; and

(iii) any other activity which the relevant person regards as particularly likely by its nature to be related to money laundering or terrorist financing;”

RELEVANT REGULATORY PROVISIONS

2.1 In exercising its powers to impose a financial penalty, the Authority has had regard to the relevant regulatory provisions published in the Authority’s Handbook. The main provisions that the Authority considers relevant are set out below.

Principles for Business (“Principles”)

2.2 The Principles are a general statement of the fundamental obligations of firms under the regulatory system and are set out in the Authority’s Handbook.

2.3 Principle 2 provides:

“A firm must conduct its business with due skill, care and diligence.

2.4 Principle 3 provides:

“A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.”

SENIOR MANAGEMENT ARRANGEMENTS, SYSTEMS AND CONTROLS (“SYSC”)

2.5 SYSC 3.2.4G provides:

“The guidance relevant to delegation within the firm is also relevant to external delegation (‘outsourcing’). A firm cannot contract out its regulatory obligations. So, for example, under Principle 3 a firm should take reasonable care to supervise the discharge of outsourced functions by its contractor.

A firm should take steps to obtain sufficient information from its contractor to enable it to assess the impact of outsourcing on its systems and controls."

2.6 SYSC 3.2.6E provides:

"The FCA, when considering whether a breach of its rules on systems and controls against money laundering has occurred, will have regard to whether a firm has followed relevant provisions in the guidance for the UK financial sector issued by the Joint Money Laundering Steering Group".

2.7 SYSC 3.2.6R provides:

"A firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime."

2.8 SYSC 6.1.1R provides:

"A firm must establish, implement and maintain adequate policies and procedures sufficient to ensure compliance of the firm including its managers, employees and appointed representatives (or where applicable, tied agents) with its obligations under the regulatory system and for countering the risk that the firm might be used to further financial crime."

2.9 SYSC 6.3.1R provides:

A firm must ensure the policies and procedures established under SYSC 6.1.1 R include systems and controls that:

(1) enable it to identify, assess, monitor and manage money laundering risk; and

(2) are comprehensive and proportionate to the nature, scale and complexity of its activities.

2.10 SYSC 6.3.2G provides:

"Money laundering risk" is the risk that a firm may be used to further money laundering. Failure by a firm to manage this risk effectively will increase the risk to society of crime and terrorism.

2.11 SYSC 6.3.6 provides:

"In identifying its money laundering risk and in establishing the nature of these systems and controls, a firm should consider a range of factors, including:

(1) its customer, product and activity profiles;

(2) its distribution channels;

(3) the complexity and volume of its transactions;

(4) *its processes and systems; and*

(5) *its operating environment”.*

2.12 SYSC 6.3.7 provides:

“A firm should ensure that the systems and controls include:

(3) appropriate documentation of its risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies;

(4) appropriate measures to ensure that money laundering risk is taken into account in its day-to-day operation, including in relation to:

(a) the development of new products;

(b) the taking-on of new customers; and

(c) changes in its business profile”.

2.13 SYSC 9.1.1 R provides:

“A firm must arrange for orderly records to be kept of its business and internal organisation, including all services and transactions undertaken by it, which must be sufficient to enable the appropriate regulator or any other relevant competent authority under MiFID or the UCITS Directive to monitor the firm's compliance with the requirements under the regulatory system, and in particular to ascertain that the firm has complied with all obligations with respect to clients.”

CONDUCT OF BUSINESS SOURCEBOOK (COBS)

2.14 COBS 3.3.1A(EU) provides:

“Articles 45(1) and (2) of the MiFID Org Regulation require firms to provide clients with specified information concerning client categorisation.

45(1) Investment firms shall notify new clients, and existing clients that the investment firm has newly categorised as required by Directive 2014/65/EU, of their categorisation as a retail client, a professional client or eligible counterparty in accordance with that Directive.

(2) Investment firms shall inform clients in a durable medium about any right that client has to request a different categorisation and about any limitations to the level of client protection that a different categorisation would entail.

[Note: articles 45(1) and (2) of the MiFID Org Regulation]”

2.15 COBS 3.3.1B(R) provides:

"The information referred to in article 45(2) of the MiFID Org Regulation (as reproduced at COBS 3.3.1AEU) must be provided to clients prior to any provision of services.

[Note: paragraph 2 of section I of annex II to MiFID]"

2.16 COBS 3.5.2 provides:

Per Se Professional Clients

"Each of the following is a per se professional client unless and to the extent it is an eligible counterparty or is given a different categorisation under this chapter:

(1) an entity required to be authorised or regulated to operate in the financial markets. The following list includes all authorised entities carrying out the characteristic activities of the entities mentioned, whether authorised by an EEA State or a third country and whether or not authorised by reference to a directive:

- (a) a credit institution;*
- (b) an investment firm;*
- (c) any other authorised or regulated financial institution;*
- (d) an insurance company;*
- (e) a collective investment scheme or the management company of such a scheme;*
- (f) a pension fund or the management company of a pension fund;*
- (g) a commodity or commodity derivatives dealer;*
- (h) a local;*
- (i) any other institutional investor;*

(2) in relation to MiFID or equivalent third country business a large undertaking meeting two of the following size requirements on a company basis:

- (a) balance sheet total of EUR 20,000,000;*
- (b) net turnover of EUR 40,000,000;*
- (c) own funds of EUR 2,000,000;*

(3) in relation to business that is not MiFID or equivalent third country business a large undertaking meeting any¹of the following conditions:

- (a) a body corporate (including a limited liability partnership) which has (or any of whose holding companies or subsidiaries has) (or has had at any time during the previous two years) ¹called up share capital or net*

assets of at least £51 million (or its equivalent in any other currency at the relevant time);

(b) an undertaking that meets (or any of whose holding companies or subsidiaries meets) two of the following tests:

(i) a balance sheet total of EUR 12,500,000;

(ii) a net turnover of EUR 25,000,000;

(iii) an average number of employees during the year of 250;

(c) a partnership or unincorporated association which has (or has had at any time during the previous two years) net assets of at least £5 million (or its equivalent in any other currency at the relevant time) and calculated in the case of a limited partnership without deducting loans owing to any of the partners;

(d) a trustee of a trust (other than an occupational pension scheme, SSAS, personal pension scheme or stakeholder pension scheme) which has (or has had at any time during the previous two years) assets of at least £10 million (or its equivalent in any other currency at the relevant time) calculated by aggregating the value of the cash and designated investments forming part of the trust's assets, but before deducting its liabilities;

(e) a trustee of an occupational pension scheme or SSAS, or a trustee or operator of a personal pension scheme or stakeholder pension scheme where the scheme has (or has had at any time during the previous two years):

(i) at least 50 members; and

(ii) assets under management of at least £10 million (or its equivalent in any other currency at the relevant time);

(f) a local authority or public authority.

(4) a national or regional government, a public body that manages public debt, a central bank, an international or supranational institution (such as the World Bank, the IMF, the ECP, the EIB) or another similar international organisation;

(5) another institutional investor whose main activity is to invest in financial instruments (in relation to the firm's MiFID or equivalent third country business) or designated investments (in relation to the firm's other business). This includes entities dedicated to the securitisation of assets or other financing transactions."

2.17 COBS 3.5.3 provides:

Elective professional clients

A firm may treat a client other than a local public authority or municipality³ as an elective professional client if it complies with (1) and (3) and, where applicable, (2):

(1) the firm undertakes an adequate assessment of the expertise, experience and knowledge of the client that gives reasonable assurance, in light of the nature of the transactions or services envisaged, that the client is capable of making his own investment decisions and understanding the risks involved (the "qualitative test");

(2) in relation to MiFID or equivalent third country business in the course of that assessment, at least two of the following criteria are satisfied:

(a) the client has carried out transactions, in significant size, on the relevant market at an average frequency of 10 per quarter over the previous four quarters;

(b) the size of the client's financial instrument portfolio, defined as including cash deposits and financial instruments, exceeds EUR 500,000;

(c) the client works or has worked in the financial sector for at least one year in a professional position, which requires knowledge of the transactions or services envisaged; (the "quantitative test"); and

(3) the following procedure is followed:

(a) the client must state in writing to the firm that it wishes to be treated as a professional client either generally or in respect of a particular service or transaction or type of transaction or product;

(b) the firm must give the client a clear written warning of the protections and investor compensation rights the client may lose; and

(c) the client must state in writing, in a separate document from the contract, that it is aware of the consequences of losing such protections.

2.18 COBS 3.8.2R provides:

(2) A firm must make a record in relation to each client of:

(a) the categorisation established for the client under this chapter, including sufficient information to support that categorisation;

...

DECISION PROCEDURE AND PENALTIES MANUAL (“DEPP”)

2.19 Chapter 6 of DEPP, which forms part of the Authority’s Handbook, sets out the Authority’s statement of policy with respect to the imposition and amount of financial penalties under the Act. In particular, DEPP 6.5A sets out the five steps for penalties imposed on firms.

ENFORCEMENT GUIDE

2.20 The Enforcement Guide sets out the Authority’s approach to taking disciplinary action. The Authority’s approach to financial penalties and suspensions (including restrictions) is set out in Chapter 7 of the Enforcement Guide.

JMLSG GUIDANCE– PART I (published 20 November 2013)

Outsourcing

3.16 Where AML/CTF tasks are delegated by a firm’s MLRO, the FCA will expect the MLRO to take ultimate managerial responsibility.

Risk-based approach

4.14 A risk-based approach starts with the identification and assessment of the risk that has to be managed. Examples of the risks in particular industry sectors are set out in the sectoral guidance in Part II, and at www.jmlsg.org.uk.

4.8 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the firm. These steps are to:

- identify the money laundering and terrorist financing risks that are relevant to the firm;
- assess the risks presented by the firm’s particular
 - customers and any underlying beneficial owners*;
 - products;
 - delivery channels;
 - geographical areas of operation;
- design and implement controls to manage and mitigate these assessed risks, in the context of the firm’s risk appetite;
- monitor and improve the effective operation of these controls; and
- record appropriately what has been done, and why.

* In this Chapter, references to ‘customer’ should be taken to include beneficial owner, where appropriate.

- 4.9 Whatever approach is considered most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who their customers are, what they do, their expected level of activity with the firm and whether or not they are likely to be engaged in criminal activity. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions or activity that may be suspicious.
- 4.12 A risk assessment will often result in a stylised categorisation of risk: e.g., high/medium/low. Criteria will be attached to each category to assist in allocating customers and products to risk categories, in order to determine the different treatments of identification, verification, additional customer information and monitoring for each category, in a way that minimises complexity.
- 4.15 While a risk assessment should always be performed at the inception of the customer relationship (although see paragraph 4.16 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.
- 4.34 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.
- 4.39 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.
- 4.40 Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious. Examples of EDD measures that could be applied for higher risk business relationships include:
- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
 - Obtaining additional information on the intended nature of the business relationship

- Obtaining information on the source of funds or source of wealth of the customer
- Obtaining information on the reasons for intended or performed transactions
- Obtaining the approval of senior management to commence or continue the business relationship
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

4.50 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

4.52 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Customer due diligence

5.1.5 The CDD measures that must be carried out involve: (a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff); (b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff); and (c) obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.3.20ff).

5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm (a) must not carry out a transaction with or for the customer through a bank account; (b) must not establish a business relationship or carry out an occasional transaction with the customer; (c) must terminate any existing business relationship with the customer; (d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.

5.3.21 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.

5.3.261 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money

laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Enhanced due diligence

- 5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner, where applicable, and the purpose and intended nature of the business relationship.
- 5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons: to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.
- 5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc., of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.
- 5.5.5. A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.
- 5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending on the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The firm should consider whether, in some circumstances, evidence of source of wealth or

income should be required (for example, if from an inheritance, see a copy of the will). The firm should also consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.

- 5.5.9 The ML Regulations prescribe three specific types of relationship in respect of which EDD measures must be applied. These are:
- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
 - in respect of a correspondent banking relationship (see Part II, sector 16: *Correspondent banking*);
 - in respect of a business relationship or occasional transaction with a PEP (see paragraphs 5.5.18ff).

Reliance on third parties

- 5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is listed in Regulation 17(2), and that consent to being relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

- 5.6.14 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:
- its public disciplinary record, to the extent that this is available;
 - the nature of the customer, the product/service sought and the sums involved;
 - any adverse experience of the other firm's general efficiency in business dealings;
 - any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

- 5.6.16 In practice, the firm relying on the confirmation of a third party needs to know:
- the identity of the customer or beneficial owner whose identity is being verified;
 - the level of CDD that has been carried out; and
 - confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance

is given in paragraphs 5.6.30 to 5.6.33 below on the use of pro-forma confirmations containing the above information.

- 5.6.24 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 17(2). This is particularly important where the firm relied upon is situated outside the EEA.
- 5.6.25 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 17(2) (see paragraph 5.6.6).

Monitoring customer activity

- 5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:
- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile;
 - Ensuring that the documents, data or information held by the firm are kept up to date.
- 5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers, assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.
- 5.7.3 The essentials of any system of monitoring are that:
- it flags up transactions and/or activities for further examination;
 - these reports are reviewed promptly by the right person(s); and
 - appropriate action is taken on the findings of any further examination.
- 5.7.4 Monitoring can be either:
- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
 - after the event, through some independent review of the transactions and/or activities that a customer has undertaken
- and in either case, unusual transactions or activities will be flagged for further examination.
- 5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.

- 5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.
- 5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

JMLSG Part II – Wholesale Markets

Types of Risk

- 18.14 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in equivalent jurisdictions, are transparent and have a central counterparty to clear trades, can largely be seen as carrying a lower generic money laundering risk. OTC business may, generally, be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products... Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

JMLSG GUIDANCE– PART I (published 19 November 2014)

Risk-based approach

- 4.5 A risk-based approach requires the full commitment and support of senior management, and the active co-operation of business units. The risk-based approach needs to be part of the firm's philosophy, and as such reflected in the procedures and controls. There needs to be a clear communication of policies and procedures across the firm, along with the robust mechanisms to ensure that they are carried out effectively, weaknesses are identified, and improvements are made wherever necessary.
- 4.6 Although the ML/TF risks facing the firm fundamentally arise through its customers, the nature of the business and their activities, it is important that the firm considers its customer risks in the context of the wider ML/TF environment inherent in the jurisdictions in which the firm and its customers operate. Firms should bear in mind that some jurisdictions have close links with other, perhaps higher risk jurisdictions, and where appropriate and relevant regard should be had to this.

- 4.9 The procedures, systems and controls designed to mitigate assessed ML/TF risks should be appropriate and proportionate to these risks, and should be designed to provide an effective level of mitigation.
- 4.12 A risk-based approach takes a number of discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks based by the firm. These steps are to:
- identify the money laundering and terrorist financing risks that are relevant to the firm;
 - assess the risks presented by the firm's particular
 - customers and any underlying beneficial owners*;
 - products;
 - delivery channels;
 - geographical areas of operation;
 - design and implement controls to manage and mitigate these assessed risks, in the context of the firm's risk appetite;
 - monitor and improve the effective operation of these controls; and
 - record appropriately what has been done, and why.
- * *In this Chapter, references to 'customer' should be taken to include beneficial owner, where appropriate.*
- 4.13 Whatever approach is considered the most appropriate to the firm's money laundering/terrorist financing risk, the broad objective is that the firm should know at the outset of the relationship who their customers are, where they operate, what they do, their expected level of activity with the firm and whether or not they are likely to be engaged in criminal activity. The firm then should consider how the profile of the customer's financial behaviour builds up over time, thus allowing the firm to identify transactions that may be suspicious.
- 4.20 In reaching an appropriate level of satisfaction as to whether the customer is acceptable, requesting more and more identification is not always the right answer – it is sometimes better to reach a full and documented understanding of what the customer does, and the transactions it is likely to undertake. Some business lines carry an inherently higher risk of being used for ML/TF purposes than others.
- 4.21 However, as stated in paragraph 5.2.6, if a firm cannot satisfy itself as to the identity of the customer; verify that identity; or obtain sufficient information on the nature and intended purpose of the business relationship, it must not enter into a new relationship and must terminate an existing one.
- 4.22 While a risk assessment should always be performed at the inception of a customer relationship (although see paragraph 4.16 below), for some customers a comprehensive risk profile may only become evident once the customer has begun transacting through an account, making the monitoring of transactions and on-going reviews a fundamental component of a

reasonably designed RBA. A firm may also have to adjust its risk assessment of a particular customer based on information received from a competent authority.

- 4.25 For firms which operate internationally, or which have customers based or operating abroad, there are additional jurisdictional risk considerations relating to the position of the jurisdictions involved, and their reputation and standing as regards the inherent ML/TF risk, and the effectiveness of their AML/CTF enforcement regime.
- 4.45 Based on the risk assessment carried out, a firm will determine the level of CDD that should be applied in respect of each customer and beneficial owner. It is likely that there will be a standard level of CDD that will apply to the generality of customer, based on the firm's risk appetite.
- 4.50 Where a customer is assessed as carrying a higher risk, then depending on the product sought, it will be necessary to seek additional information in respect of the customer, to be better able to judge whether or not the higher risk that the customer is perceived to present is likely to materialise. Such additional information may include an understanding of where the customer's funds and wealth have come from. Guidance on the types of additional information that may be sought is set out in section 5.5.
- 4.51 Where the risks of ML/TF are higher, firms must conduct enhanced due diligence measures consistent with the risks identified. In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear unusual or suspicious. Examples of EDD measures that could be applied for higher risk business relationships include:
- Obtaining, and where appropriate verifying, additional information on the customer and updating more regularly the identification of the customer and any beneficial owner
 - Obtaining additional information on the intended nature of the business relationship
 - Obtaining information on the source of funds or source of wealth of the customer
 - Obtaining information on the reasons for intended or performed transactions
 - Obtaining the approval of senior management to commence or continue the business relationship
 - Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination
 - Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards
- 4.61 Firms must document their risk assessments in order to be able to demonstrate their basis, keep these assessments up to date, and have appropriate mechanisms to provide appropriate risk assessment information to competent authorities.

- 4.63 In addition, on a case-by-case basis, firms should document the rationale for any additional due diligence measures it has undertaken (or any it has waived) compared to its standard approach, in view of its risk assessment of a particular customer.

Customer due diligence

- 5.1.5 The CDD measures that must be carried out involve: (a) identifying the customer, and verifying his identity (see paragraphs 5.3.2ff); (b) identifying the beneficial owner, where relevant, and verifying his identity (see paragraphs 5.3.8ff); and (c) obtaining information on the purpose and intended nature of the business relationship (see paragraphs 5.3.20ff).
- 5.2.6 Where a firm is unable to apply CDD measures in relation to a customer, the firm (a) must not carry out a transaction with or for the customer through a bank account; (b) must not establish a business relationship or carry out an occasional transaction with the customer; (c) must terminate any existing business relationship with the customer; (d) must consider whether it ought to be making a report to the NCA, in accordance with its obligations under POCA and the Terrorism Act.
- 5.3.20 A firm must understand the purpose and intended nature of the business relationship or transaction to assess whether the proposed business relationship is in line with the firm's expectation and to provide the firm with a meaningful basis for ongoing monitoring. In some instances this will be self-evident, but in many cases the firm may have to obtain information in this regard.
- 5.3.253 For situations presenting a lower money laundering or terrorist financing risk, the standard evidence will be sufficient. However, less transparent and more complex structures, with numerous layers, may pose a higher money laundering or terrorist financing risk. Also, some trusts established in jurisdictions with favourable tax regimes have in the past been associated with tax evasion and money laundering. In respect of trusts in the latter category, the firm's risk assessment may lead it to require additional information on the purpose, funding and beneficiaries of the trust.

Enhanced due diligence

- 5.5.1 A firm must apply EDD measures on a risk-sensitive basis in any situation which by its nature can present a higher risk of money laundering or terrorist financing. As part of this, a firm may conclude, under its risk-based approach, that the information it has collected as part of the customer due diligence process (see section 5.3) is insufficient in relation to the money laundering or terrorist financing risk, and that it must obtain additional information about a particular customer, the customer's beneficial owner,

where applicable, and the purpose and intended nature of the business relationship.

- 5.5.2 As a part of a risk-based approach, therefore, firms should hold sufficient information about the circumstances and business of their customers and, where applicable, their customers' beneficial owners, for two principal reasons: to inform its risk assessment process, and thus manage its money laundering/terrorist financing risks effectively; and to provide a basis for monitoring customer activity and transactions, thus increasing the likelihood that they will detect the use of their products and services for money laundering and terrorist financing.
- 5.5.4 In practice, under a risk-based approach, it will not be appropriate for every product or service provider to know their customers equally well, regardless of the purpose, use, value, etc. of the product or service provided. Firms' information demands need to be proportionate, appropriate and discriminating, and to be able to be justified to customers.
- 5.5.5 A firm should hold a fuller set of information in respect of those business relationships it assessed as carrying a higher money laundering or terrorist financing risk, or where the customer is seeking a product or service that carries a higher risk of being used for money laundering or terrorist financing purposes.
- 5.5.6 When someone becomes a new customer, or applies for a new product or service, or where there are indications that the risk associated with an existing business relationship might have increased, the firm should, depending upon the nature of the product or service for which they are applying, request information as to the customer's residential status, employment and salary details, and other sources of income or wealth (e.g., inheritance, divorce settlement, property sale), in order to decide whether to accept the application or continue with the relationship. The firm should consider whether or not there is a need to enhance its activity monitoring in respect of the relationship. A firm should have a clear policy regarding the escalation of decisions to senior management concerning the acceptance or continuation of high-risk business relationships.
- 5.5.9 The ML Regulations prescribe three specific types of relationship in respect of which EDD must be applied. They are:
- where the customer has not been physically present for identification purposes (see paragraphs 5.5.10ff);
 - in respect of a correspondent banking relationship (see Part II, sector 16: Correspondent banking);
 - in respect of a business relationship or occasional transaction with a PEP (see paragraph 5.5.18ff).

Reliance on third parties

- 5.6.4 The ML Regulations expressly permit a firm to rely on another person to apply any or all of the CDD measures, provided that the other person is

listed in Regulation 17(2), and that consent to be relied on has been given (see paragraph 5.6.8). The relying firm, however, retains responsibility for any failure to comply with a requirement of the Regulations, as this responsibility cannot be delegated.

5.6.14 Whether a firm wishes to place reliance on a third party will be part of the firm's risk-based assessment, which, in addition to confirming the third party's regulated status, may include consideration of matters such as:

- its public disciplinary record, to the extent that this is available; the nature of the customer, the product/service sought and the sums involved; any adverse experience of the other firm's general efficiency in business dealings; any other knowledge, whether obtained at the outset of the relationship or subsequently, that the firm has regarding the standing of the firm to be relied upon.

5.6.16 In practice, the firm relying on the confirmation of a third party needs to know:

- the identity of the customer or beneficial owner whose identity is being verified; the level of CDD that has been carried out; and confirmation of the third party's understanding of his obligation to make available, on request, copies of the verification data, documents or other information.

In order to standardise the process of firms confirming to one another that appropriate CDD measures have been carried out on customers, guidance is given in paragraphs 5.6.30 to 5.6.33 below on the use of pro-forma confirmations containing the above information.

5.6.24 A firm must also document the steps taken to confirm that the firm relied upon satisfies the requirements in Regulation 17(2). This is particularly important where the firm relied upon is situated outside the EEA.

5.6.25 Part of the firm's AML/CTF policy statement should address the circumstances where reliance may be placed on other firms and how the firm will assess whether the other firm satisfies the definition of third party in Regulation 17(2) (see paragraph 5.6.6).

Monitoring customer activity

5.7.1 Firms must conduct ongoing monitoring of the business relationship with their customers. Ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, his business and risk profile; Ensuring that the documents, data or information held by the firm are kept up to date.

5.7.2 Monitoring customer activity helps identify unusual activity. If unusual activities cannot be rationally explained, they may involve money laundering or terrorist financing. Monitoring customer activity and transactions that take place throughout a relationship helps firms know their customers,

assist them to assess risk and provides greater assurance that the firm is not being used for the purposes of financial crime.

- 5.7.3 The essentials of any system of monitoring are that:
- it flags up transactions and/or activities for further examination;
 - these reports are reviewed promptly by the right person(s); and
 - appropriate action is taken on the findings of any further examination.
- 5.7.4 Monitoring can be either:
- in real time, in that transactions and/or activities can be reviewed as they take place or are about to take place, or
 - after the event, through some independent review of the transactions and/or activities that a customer has undertaken
- and in either case, unusual transactions or activities will be flagged for further examination.
- 5.7.7 In designing monitoring arrangements, it is important that appropriate account be taken of the frequency, volume and size of transactions with customers, in the context of the assessed customer and product risk.
- 5.7.8 Monitoring is not a mechanical process and does not necessarily require sophisticated electronic systems. The scope and complexity of the process will be influenced by the firm's business activities, and whether the firm is large or small. The key elements of any system are having up-to-date customer information, on the basis of which it will be possible to spot the unusual, and asking pertinent questions to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious.
- 5.7.12 Higher risk accounts and customer relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring.

JMLSG Part II – Wholesale Markets

Types of Risk

- 18.14 OTC and exchange-based trading can also present very different money laundering risk profiles. Exchanges that are regulated in equivalent jurisdictions, are transparent and have a central counterparty to clear trades, can largely be seen as carrying a lower generic money laundering risk. OTC business may, generally, be less well regulated and it is not possible to make the same generalisations concerning the money laundering risk as with exchange-traded products. For example, trades that are executed as OTC but then are centrally cleared, have a different risk profile to trades that are executed and settled OTC. Hence, when dealing in the OTC markets firms will need to take a more considered risk-based approach and undertake more detailed risk-based assessment.

ANNEX C - 401(k) Funds

Employer Created 401(k) Plans

A 401(k) is a qualified profit sharing plan that allows employees to contribute a portion of their wages to individual retirement accounts. Employers can also contribute to employees' accounts. Any money that is contributed to a 401(k) below the annual contribution limit is not subject to income tax in the year the money is earned, but then is taxable at retirement. For example, if John Doe earns \$100,000 in 2018, he is allowed to contribute \$18,500, which is the 2018 limit, to his 401(k) plan. If he contributes the full amount that he is allowed, then although he earned \$100,000, his taxable income for income tax purposes would be \$81,500. Then, he would pay income tax upon any money that he withdraws from his 401(k) at retirement. If he withdraws any money prior to age 59 1/2, he would be subject to various penalties and taxes.

Contribution to a 401(k) plan must not exceed certain limits described in the Internal Revenue Code. The limits apply to the total amount of employer contributions, employee elective deferrals and forfeitures credits to the participant's account during the year. The contribution limits apply to the aggregate of all retirement plans in which the employee participates. The contribution limits have been increased over time. Below is a chart of the contribution limits:

| Year | Employee Contribution Limit | Employer Contribution Limit | Total Contribution | Catch Up Contribution (only for individuals Age 50+) |
|------|-----------------------------|-----------------------------|--------------------|--|
| 1999 | \$10,000 | \$20,000 | \$30,000 | 0 |
| 2000 | \$10,500 | \$19,500 | \$30,000 | 0 |
| 2001 | \$10,500 | \$24,500 | \$35,000 | 0 |
| 2002 | \$11,000 | \$29,000 | \$40,000 | \$1,000 |
| 2003 | \$12,000 | \$28,000 | \$40,000 | \$2,000 |
| 2004 | \$13,000 | \$28,000 | \$41,000 | \$3,000 |
| 2005 | \$14,000 | \$28,000 | \$42,000 | \$4,000 |
| 2006 | \$15,000 | \$29,000 | \$44,000 | \$5,000 |
| 2007 | \$15,500 | \$29,500 | \$45,000 | \$5,000 |
| 2008 | \$15,500 | \$30,500 | \$46,000 | \$5,000 |
| 2009 | \$16,500 | \$32,500 | \$49,000 | \$5,500 |
| 2010 | \$16,500 | \$32,500 | \$49,000 | \$5,500 |
| 2011 | \$16,500 | \$32,500 | \$49,000 | \$5,500 |
| 2012 | \$16,500 | \$33,500 | \$50,000 | \$5,500 |
| 2013 | \$17,000 | \$34,000 | \$51,000 | \$5,500 |
| 2014 | \$17,500 | \$34,500 | \$52,000 | \$5,500 |
| 2015 | \$18,000 | \$35,000 | \$53,000 | \$6,000 |

If an individual was aged 30 in 1999, the absolute maximum that he could have contributed including the maximum employer contributions would be \$746,000.

Minimum Age Requirements

In the United States, the general minimum age limit for employment is 14. Because of this, an individual may make contributions into 401(k) plans from this age if the terms of the plan allow it. The federal government does not legally require employers to include employees in their 401(k) plans until they are at least 21 years of age. If you are at least 21 and have been working for your employer for at least one year, your employer must allow you to participate in the company's 401(k) plan. As a result, some employers' plans

will not allow individuals to invest until they are at least 18 or 21 depending upon the terms of the plan.

One-Participant 401(k) Plans

A one-participant 401(k) plan are sometimes called a solo 401(k). This plan covers a self-employed business owner, and their spouse, who has no employees. These plans have the same rules and requirements as other 401(k) plans, but the self-employed individual wears two hats, the employer and the employee.