# MLROs.com
# Conference Three 2017

*Hosted with* ***Gordon Dadds***

**Delegate Handout**
Tuesday, 12th September 2017

GORDON DADDS

# Index

# Agenda

| | |
|---|---|
| **08:30 - 09:00** | **Registration & Coffee** |
| **09:00 - 09:10** | **Welcome & Introduction**<br>**David Pelled, CEO, MLROs.com** |
| **09:10 - 09:55** | **Data Driven Risk Technologies**<br>**Gavin Proudley, Global Director- Due Diligence, Dow Jones** |
| **09:55 - 10:40** | **Employee Screening- A Hole in your Defences**<br>**Michael Whittington, Head of Employee Screening, The Risk Advisory Group** |
| **10:40 – 11:00** | **Morning Coffee** |
| **11:00 - 11:40** | **GDPR – Myths, Mystique and Market Perceptions**<br>**Adam Wiseman Barrister, New Leaf Advisory in conjunction with Gordon Dadds Financial Markets** |
| **11:40 - 12:20** | **The Changing Landscape of AML Regulations in the UK and the EU**<br>**John Karantzis, CEO and Managing Director, iSignthis** |
| **12:20 - 13:00** | **MLD4/5 Risk Assessment- Failure to Comply and Enforcement**<br>**Andrew Tait & Alex Ktorides, Partners, Gordon Dadds** |
| **13:00 - 14:00** | **Lunch** |

| | |
|---|---|
| **14:00 - 14:45** | **Criminal Finance Act 2017- Failure to Prevent Tax Evasion**<br>**Simon Airey, Partner, Paul Hastings** |
| **14:45 – 15:30** | **The Impact of Terrorist Financing**<br>**Andrew McDonald, Former Head of the NTFIU** |
| **15:30 - 15:50** | **Afternoon Coffee** |
| **15:50 - 16:40** | **Panel Session- Regulatory Conflicts**<br>**Jonathan Williams, Former Head of Payments & Strategy, Experian**<br>**Roy Ramm, Former Head of SOCA & Chairman, Comsec**<br>**Dominic Thorncroft, Chairman, AUKPI**<br>**Colin Darby, Managing Consultant, Bovill**<br>**Emma Lindley, Director Innovate Identity** |
| **16:40 - 17:20** | **Keynote Speaker**<br>**JMLIT- Daesh Finance- Dual Use Goods**<br>**Patrick Rarden MBE, City of London Police** |
| **17:22 - 17:30** | **Panel Q&A** |
| **17:30 – 19:30** | **Evening Reception & Networking Opportunities** |

# About MLROs.com

MLROs.com is your specialist, industry-led community, both online and at our hosted events all over the UK. Our members include representatives from a wide range of financial institutions, regulatory bodies, law enforcement agencies and industry sectors.

MLROs.com is eager to help our members stay abreast of the changing Anti-Money Laundering, Financial Crime Risk & Regulatory landscape – we aim to spark debate, to provide opportunities to learn and to help you navigate these changing times with MLROs.com as your trusted companion.

We exist to support and challenge our members to remain at the fore of our industry. Our offerings strive to keep our members abreast of the evolving regulatory landscape, to aid professional development and to host events with specialist networking opportunities. Our members come from a range of industries but all share a passion and commitment to effectively combat the advancement of financial criminals. Our speakers are leading experts, again from a multitude of backgrounds – each with a unique perspective to share. This special combination provides our members with access to expert insights and collaborative sessions that empower us to boldly lead in the fight against financial crime.

MLROs.com delivers a collaborative online forum that also hosts regular, informative events offering a unique perspective and a safe place to enquire together on the issues we face across industry. MLROs.com offers a website with tailored sections for richer content for our members. For those who register for free, you will have access to the wealth of members-only content and be able to avail of the early notice and/ or discounted pricing for all upcoming events.

We expect to journey together with our members to empower you to manage the pressures of the tasks ahead. The holistic requirements expected of professionals in the field continue to grow at an ever increasing pace, driven by the continued growth of the regulatory burden and the financial criminals ongoing determination to ply their nefarious trade with increasing sophistication and regularity; MLROs.com is stepping up to the task to ensure that each and every financial crime professional is educated, supported and empowered.

If you have not done so already, please spread the word to your colleagues/contemporaries to register for free on MLROs.com, so they too can participate and benefit from our member-led exciting and enriching forum.

# Partners and Sponsors

## Hosting Partner

GORDON DADDS

## Platinum Sponsors

DOW JONES

iSignthis®

## Gold Sponsors

compliancematters from WealthBriefing

LYSIS FINANCIAL

## Bronze Sponsors

comsec

COMPLIANCE RECRUITMENT SOLUTIONS
by former Compliance Officers

# About Gordon Dadds

Gordon Dadds is one of London's top 100 and most future-focused law firms, with a growing global footprint. Over the past few years it has expanded from a highly regarded but modestly sized practice to become one of the UK's most ambitious full-service firms, with over 100 fee-earners specialising in every major area of law.

Gordon Dadds was founded in 1920, with an office in Piccadilly, by divorce lawyer George 'Tim' Gordon on leaving the army after the First World War. The firm has since developed in ways its founder could scarcely conceive, though its growth remains consistent in that it still prizes ambition and respect, still insists upon excellence in everything it does and still offers clients a uniquely personal service. In short, Gordon Dadds builds on its past to define its future. Since 2013 the firm has expanded from a highly regarded but modestly sized practice to become one of the UK's most ambitious full-service firms, with fee-earners specialising in every major area of law.

Its legal services are also complemented by its consulting arm, GD Financial Markets, a growing and important part of Gordon Dadds' service. The firm has made significant investment in technology, enabling it to serve and support clients around the clock and around the world.

The firm's diversity as a business is a reflection of the various agendas of ambitious and successful people, high-growth businesses and major corporations. Many of its clients have family relationships, holdings or other interests in more than one country.

GORDON DADDS

# About Dow Jones

Since 1882, Dow Jones has been finding new ways to bring information to the world's top business entities. Beginning as a niche news agency in an obscure Wall Street basement, Dow Jones has grown to be a worldwide news and information powerhouse, with prestigious brands including The Wall Street Journal, Dow Jones Newswires, Factiva, Barron's, MarketWatch and Financial News.

This longevity and success is due to a relentless pursuit of accuracy, depth and innovation, enhanced by the wisdom of past experience and a solid grasp on the future ahead. More than its individual brands, Dow Jones is a modern gateway to intelligence, with innovative technology, advanced data feeds, integrated solutions, expert research, award-winning journalism and customizable apps and delivery systems to bring the information that matters most to customers, when and where they need it, every day.

Dow Jones Risk & Compliance is a global provider of third party risk management and regulatory compliance solutions. Working with clients across the globe, we have created products and services to help companies evaluate third party risks faster and with more confidence. We deliver research tools and outsourced services for on-boarding, vetting and investigation to help companies comply with anti-money laundering, anti-bribery, corruption and economic sanctions regulation in mitigating third party risk. With a global team of expert researchers, flexible delivery options and enriched third party risk data, our suite of compliance solutions empower compliance professionals to quickly and efficiently reduce risks while conserving limited resources.

# About iSignthis

Australian Securities and Frankfurt Stock Exchange listed iSignthis Ltd (ASX : ISX / FRA : TA8) is the global leader in remote identity verification, payment authentication and payment processing to meet AML/CFT requirements. iSignthis provides an end-to-end on-boarding service for merchants, with a unified payment and identity service via our PaydentityTM and ISXPay® solutions.

By converging payments and identity, iSignthis delivers regulatory compliance to an enhanced customer due diligence standard. We offer global reach to any of the world's 3.5Bn 'bank verified' card or account holders, that can be remotely on-boarded to regulated merchants in as little as 3 to 5 minutes.

iSignthis is the trusted back office solution for regulated entities, allowing our customers to stay ahead of the regulatory curve and focus on growing their core business.

Founded in 2013, our initial goal was to develop a means of preventing Card Not Present (CNP) fraud in order to protect consumers and merchants from the growing challenge of online fraud. Our research has led to patents being granted in a number of jurisdictions, and we have developed our services to encompass payments, antifraud and remote Customer Identification to a KYC standard.

The iSignthis solution serves all sectors of the digital economy involved in online transactions and purchases, with specific focus on the regulated sectors such as gaming, gambling, remittance, trading, forex, CFD, wagering, card issue and e-wallet markets, where identity proofing is a regulatory requirement.

We also offer UBO/Director/Key Controller verification to compliment your KYB service provider.

iSignthis®

# About Compliance Matters

Whether you're a wealth management or a compliance professional, you know that failure to understand and adhere to current financial regulation and laws carries potentially severe penalties in the form of imprisonment and large-scale fines. Therefore, the gravity of non-compliance cannot be underestimated by compliance professionals, relationship managers and the C-level executives who hold ultimate responsibility.

You know yourself how the need to understand the latest regulation has impacted on your daily workload. *Compliance Matters* provides readers with exclusive access to specific expert analysis and advice on how best to operate a wealth management business within the legal bounds.
With breaking news and in-depth features explaining the complexities of regulation, this essential yet affordable resource provides the reader with unique and detailed knowledge, accumulated by our editorial team from many years analysing the impact of regulatory changes in both the wealth management and compliance industries.

Supported by a daily-updated website this monthly publication offers you:
An essential and timely round-up of private client specific legislative, compliance and regulatory changes, as well as articles detailing the wider regulatory issues affecting you

Coverage of: FATCA, RDR, banking secrecy, anti-money laundering regimes, AIFMD, UCITS rules.

In-depth analysis and comment from our specialist editorial team – Including as Editor, well-known compliance commentator, Chris Hamblin, and many other global experts and private banking practitioners.
An easy-to-access electronic format – daily updated news site supported by monthly newsletter

Handy and specific compliance hints, how-to-do-its and best practice
Moves and hires in the compliance area as well as recruitment trends
Results and commentary from regular polls revealing the wealth management industry's regulatory concerns
Back-to-basics training tools

compliancematters from WealthBriefing

# About Lysis

Lysis Financial delivers innovative business change management consultancy to the financial services market. We provide expert strategy, change management and project execution services to senior compliance, operations and IT management across their core areas of expertise. Our clients include investment banks, financial institutions and insurance companies.

Lysis Financial is a boutique City-of-London-based consulting firm providing strategy and execution services to the global financial services market across the disciplines of Governance, Risk and Compliance.
Our governance risk and compliance teams aim to provide peace of mind that strategy, risk and regulation support and enable your people, culture and values. We help you embed governance at all levels of your business, ensuring everyone is clear about their roles and responsibilities. We help you meet the challenge of developing a holistic and resilient approach to Governance, Risk and Compliance that embraces change and the risks that it invariably brings.
Across the Lysis team we have in excess of two hundred man-years experience of shaping, designing and implementing Client On-Boarding (COB), Know Your Customer (KYC) and Anti-Money Laundering (AML) Transaction Monitoring frameworks and target operating models for global financial institutions.
Lysis has run a number of major global change programmes including:
60-project Board-sponsored Section 166 for a FTSE 100 financial services firm
Global Client On-Boarding Target Operating Model design and implementation across 60 countries
Set-up of a new off-shore operating centre for global KYC
We shape and design change programmes via a series of workshops with stakeholders and then deploy effective programme planning and management techniques to structure and run the resulting activities.

LYSIS FINANCIAL

# About Comsec

Comsec is an independent specialist in all areas of corporate security. We help private, commercial and government clients safeguard the integrity and value of their operations.

Their team are recognised as world-class investigators and have successfully handled some of the most complex cases to emerge over the last few decades; they have recovered millions of pounds and have been commended for their skills, dedication and integrity.

# About Compliance Recruitment Solutions

All our consultants are former full time Compliance practitioners and since 1996 we have developed a reputation with our clients as the most professional recruitment consultancy in service as well as technical knowledge, whilst at the same time candidates learnt that more than any other competitor we put their career planning and interests first as well as being able to bring our experience of working in the role to bear. We are pleased to say our team have unusually all been with us at least 10 years!

# Session 1
# 09:10-09:55

# Data Driven Risk Technologies

## Gavin Proudley

*Global Director- Due Diligence,*

*Dow Jones*

**Data Driven Risk Technologies**

Gavin will be looking into data driven risk mitigation technologies and how this can improve the speed and accuracy of the due diligence process.

# Gavin's Bio

Gavin has supported clients involved in high risk transactions, providing anti-bribery due diligence, as well as helping others design and implement broader due diligence programs. He works with large financial institutions, particularly with IPO and other investment banking teams, as well as supporting businesses in onboarding high risk and high value clients.

Prior to joining Dow Jones, Gavin was a director in EY's forensic practice where he created and led the UK corporate intelligence team. He has experience working on investigations and advisory projects.

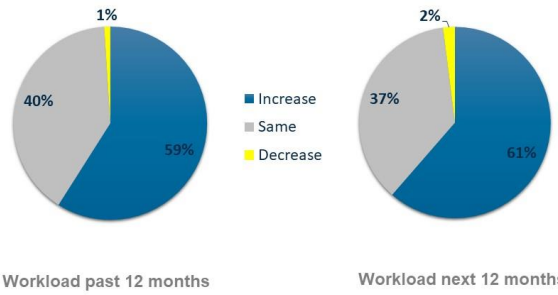
Gavin was also a Civil Servant for 11 years, working for the Ministry of Defence, the FCO and the Joint Intelligence Committee. He focused on international security and terrorism issues, advising senior officials, ministers and the Prime Minister's office.

# Due Diligence

**Asking the right questions at the right time….**
**…And getting answers from the right places**

DOW JONES

## MLROs
*– if you felt like you needed a summer holiday….*




DOW JONES

## Regulatory Backdrop
*– more rules, encompassing more organisations and greater scrutiny*

**How laundered money shapes London's property market**

Panama Papers bring ownership via offshore companies back into focus

HM Revenue & Customs

Solicitors Regulation Authority

GAMBLING COMMISSION

**2017 No. 692**

**FINANCIAL SERVICES**

The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017

*Made* - - - - *at 9.20 a.m. on 22nd June 2017*
*Laid before Parliament* *at 4.30 p.m. on 22nd June 2017*
*Coming into force* - - *26th June 2017*

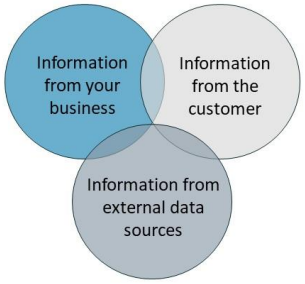
DOW JONES

## Due Diligence
*– the heart of a Financial Crime programme*

An assessment of money laundering risks will result in the application of appropriate due diligence when entering into a relationship and ongoing due diligence and monitoring of transactions throughout the course of the relationship.


DOW JONES

## Where does my data come from?




- Client selection
- Risk Assessment
- Due Diligence and Acceptance
- Name Screening
- Transaction Monitoring
- Transaction Screening
- Ongoing Screening

DOW JONES

## Where does my data come from?

- PEP
- Country Risk
- Adverse Media
- Source of Wealth / Funds
- Sanctions exposure
- Tax Evasion
- Ultimate Beneficial Ownership

"…operators should satisfy themselves that the sources are suitable to mitigate the full range of risks [including] money laundering and social responsibility risks…

Local or open source information, such as press reports, may be particularly helpful in carrying out these checks. However, operators should ensure that they are not placing an overreliance on one source of information to conduct these checks…"

DOW JONES

## An effective risk-based approach requires high quality data at every stage

- Is access to data slowing down my onboarding?
- Am I at risk of too many results? Or too few?
- Have I got the right mix of automation and human analysis?
- Where am I spending my time – collection or analysis?

In House? | Managed service? | Technology enabled? | Technology driven?

Dispersed operating model? | Centralized?

DOW JONES

# Session 2
# 09:55-10:40

# Employee Screening

## Michael Whittington

*Head of Employee Screening,*

*The Risk Advisory Group*

**Employee Screening- A Hole in your Defences**

Michael will talk about how employee screening has been specifically referenced in recently introduced MLRO industry related standards, legislation and regulations. These include; ISO 37001- Anti-Bribery Management Systems, the Money Laundering Regulation 2017 and the Financial Conduct Authority's Senior Manager and Certification Regime, and what this means for MLROs.

# Michael's Bio

Michael joined the Risk Advisory Group in 2013 as Head of the Employee Screening practice. Michael has over 20 years' experience in the employee screening industry at senior management level and spent several years in a global HR Risk and Governance role.

Michael started working in the employee screening sector when he was a co-owner and director of Financial & Personnel Research Limited (FPR), a commercial investigations company. FPR was acquired by Kroll Inc. in 2004 and Michael went on to become a senior managing director with Kroll Background Screening, covering EMEA & APAC.

In 2008, Michael took a break from the screening industry and joined Barclays Bank plc, working in the Global HR Risk & Governance team. During this time, Michael supported the bank's in-country HR teams to ensure that they had appropriate controls in place to comply

with the group HR policies, particularly in regard to their recruitment and employee screening policies. Michael returned to the employee screening industry in 2011, as managing director for G4S Employee Screening before joining Risk Advisory.

As Chair of the European Chapter of the National Association of Professional Background Screeners (NAPBS), Michael is active in the background screening community. Michael is a member of the Institute of Directors (MIoD) and a member of the Institute of Professional

Investigators (MIPI).

# The Risk Advisory Group

## Employee Screening

**MLRO.com conference**

## Leading global risk management


## Employee screening practice

- Over 19 years providing bespoke employee screening service
- Client base; financial services, legal, technology, construction, engineering
- London based team
- Extensive language capability
- Technology led solution
- 250+ clients
- ISO 27001 Information Security Management accredited

RISKADVISORY

# Case studies

## Case studies

RISKADVISORY

Action Fraud: Nearly 1 in 5 small businesses have been defrauded by an employee at some point in their trading history

- Overseas Bank (London office) - Deputy CEO
- Finance Director lied about having ACCA qualifications - Joined firm in 2001
- Chairman of two NHS Trusts and Chief Executive of a hospice
- Wealth management candidate failed to disclose a conviction for Robbery
- An individual used a virtual office to support a fake employment period
- Compliance candidate failed to disclose a £40k CCJ

RISKADVISORY

# ISO 37001 - Anti-Bribery Management Systems

## Purpose

- In October 2016 - International Organisation for Standardization (ISO) published ISO 37001 Anti-Bribery Management Systems
- The standard is intended to help an organisation to implement an effective anti-bribery management system
- It can be used internationally
- They promote internationally recognised good practice
- It is applicable to small, medium and large organisations in the public, private and voluntary sectors.
- All firms should have a robust employee screening programme, which not only helps prevent fraud and theft, but enables organisations to demonstrate that strong Anti-Bribery controls are in place.

## ISO 37001 - section 7

- Standard directs organizations to conduct due diligence on employees during hiring and promotion processes
- Organisations accredited to, or working towards accreditation of ISO 37001 should also consider extending its due diligence requirement to supply chains and other counterparties or intermediaries
- ISO 37001 suggests verification of qualifications and employment history
- ISO 37001 recommends checking whether individuals have direct links to public officials or evidence of previous involvement in bribery

## Accreditation

- Achieving ISO accreditation takes a lot of effort
- Maintaining accreditation takes more effort
- You will be subject to an independent audit at least annually
- Creating and updating policies
- Developing and rolling out adequate training
- Conformance test your controls
- Employee screening is not my area of responsibility!

RISKADVISORY

# Money Laundering Regulation 2017

## Money Laundering Regulation 2017

RISKADVISORY

- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 came into force on the 26th June 2017
- Strengthened risk mitigation policies and controls requirements
- In particular for employee screening:
  - Section 21 (1) (b) states "carry out screening of relevant employees and agents appointed by the relevant person, before both the appointment is made and at regular intervals during the course of the appointment
  - Section 21 (2)(a)(i) requires you to assess 'the skills, knowledge and expertise of the individual…'
  - Section 21 (2)(a)(ii) requires you to assess 'the conduct and integrity of the individual'.

## Money Laundering Regulation 2017

RISKADVISORY

- What does this mean in reality?
  - You need to appoint a senior person to be responsible for compliance
  - You need to carry out screening on your employees prior to appointment
  - You need to implement an ongoing Fitness and Propriety screening solution

# FCA Regulatory Regime

## FCA Senior Manager & Certification Regime

- In March 2016 the Senior Manager and Certification Regime came into force
- It impacted nearly 900 significant financial institutions
- It was designed to create greater accountability across the industry
- In 2018, the regime will be rolled out to over 47,000 other firms.

## Regulatory reference regime

- To underpin the SMCR the regulator also introduced the Regulatory Reference Regime
- This regime introduced a number of new requirements:
  - Standardise regulatory reference template
  - Turnaround time over up to 6 weeks
  - Reference period to extend to 6 years
  - Any disciplinary matters to be taken into consideration when responding to a reference

RISKADVISORY

# Screening minimum standards

## Minimum screening standards

RISKADVISORY

- Identity check
- Highest education verification
- Professional qualifications verification
- Employment references
- Criminal record check
- Credit check
- Watchlist, sanctions and PEP checks

RISKADVISORY

# Q&A

RISKADVISORY

**WASHINGTON DC**
1717 K Street NW
Suite 900
Washington DC 20006
United States

+1 202 349 4040

**LONDON**
3 More London Riverside
London
SE1 2AQ
United Kingdom

+44 20 7578 0000

**DUBAI**
PO Box 502952
Dubai Knowledge Park
Dubai
United Arab Emirates

+971 4 375 4013

**BEIRUT**
Suite 2029, 2nd floor
Louis Vuitton Building
Allenby Street
Beirut Souks
Lebanon

+961 1 957 722

**MOSCOW**
Suite 11, 4th Floor
7 Glazovskiy Pereulok
Moscow 119002
Russia

+7 495 937 7080

**HONG KONG**
Level 15
Nexxus Building
41 Connaught Road
Central
Hong Kong

+852 3757 9901

www.riskadvisory.com

# Session 3
# 11:00-11:40

# GDPR- Myths, Mystique and Market Perceptions

## Adam Wiseman

*Barrister, New Leaf Advisory in conjunction with Gordon Dadds Financial Markets*

**GDPR – Myths, Mystique and Market Perceptions**

With well under a year to go until GDPR D-Day, Adam Wiseman (Barrister-at-Law) provides a unique insight into the upcoming General Data Protection Regulation (GDPR).

Adam's presentation will cover the legal view, practical application of the rules, typical challenges firms are facing and also take questions from the audience.

**Please note there is no handout material for this session, we have added some extra notes pages for your convenience.**

# Adam's Bio

Recommended by the Directories: Legal 500 and Chambers & Partners

Member of the Criminal Bar Association and South Eastern Circuit

Adam is a highly experienced barrister who has been in practice for over 20 years. He is a senior member of Red Lion Chambers – one of the leading criminal and regulatory Chambers in the UK. He has a strong track record in defending in all types of high profile, complex and serious crime. He specialises in cyber security, data management, financial crime; fraud, confiscation, money laundering and corruption, acting for both corporate clients and individuals.

Adam has defended in prosecutions brought by the SFO, RCPO, HMRC, NCS, DWP, FCA and the CPS. He has appeared in the Judicial Committee of the Privy Council on pro bono appeals against the death penalty.

He recently defended at the Old Bailey in the News International phone-hacking and corruption case.

Adam is qualified to accept instructions on a direct access basis and is responsible for overseeing our team of instructed barristers.

# Notes

# Notes

## Session 4
## 11:40-12:20

# The Changing Landscape of AML Regulations in the UK and the EU


## John Karantzis

*CEO and Managing Director, iSignthis Ltd*
*(ASX : ISX)*

**The Changing Landscape of AML Regulations in the UK and the EU**

John will be presenting on the changes and challenges faced with AML regulations in both the UK, focusing on the latest JMLSG draft and the European Union, with the introduction of the 4th AML Directive, Payment Service Directive 2 and the General Data Protection Regulations.

This presentation should give attendees an up-to-date view of the regulatory landscape in both the UK and EU, and what regulated merchants need to be doing to prepare..

# John's Bio

John has had a career in private practice in a number of areas, including adjudication, intellectual property, regulatory and management consulting; until in 2011 he patented a process for payment instrument verification (PIV). The PIV process was originally intended to solve the challenge associated with identifying persons offering credit cards remotely, minimising the opportunity for chargebacks whilst allowing customers to purchase products on his wife's online store. Following grant of patents in late 2013, and John's consulting work in payments during 2013 involving him with the lead up to the Payment Services Directive 2 and discussions on the upcoming 4th AML Directive, John recognised that an adaption of PIV could serve the dual purpose of Strong Customer Authentication for the PSD2, in addition to proving control of a regulated account for the purpose of customer due diligence.

Australian Securities and Frankfurt Stock Exchange listed, iSignthis Ltd (ASX : ISX / FRA : TA8) was listed in March 2015, off the back of a number of agreements for payment processing and payment instrument verification. John has been responsible for the listing, capital raising, strategy, regulatory management, legal affairs and executive management of iSignthis, in addition to architecting the technical framework. iSignthis is now an enhanced due diligence platform, serving some of the world's largest FX firms, with a reach of circa 3.5Bn persons whose identities can be verified dynamically and on request. iSignthis is also recently an EEA authorised eMoney Monetary Financial Institution, and a payment facilitator for the National Australia Bank (ASX : NAB).

# Remote IDV & Due Diligence:

## Embracing Technology as a Tool to Optimise KYC/AML Compliance Procedures whilst Minimising Costs.

iSignthis Ltd (ASX:ISX / FRA : TA8)
(SWIFT BIC : ISEMCY21)

N J (John) Karantzis
B.E. LL.M M.Ent FIEAust CPEng EurIng Adj
Managing Director & Group CEO

## Contents

- The introduction of the PSD2 & 4th AML Directive / 2017 MLR's
- (Enhanced) Customer Due Diligence (remote operations)
- Solving the KYC compliance via RegTech



## 1. What do we do?

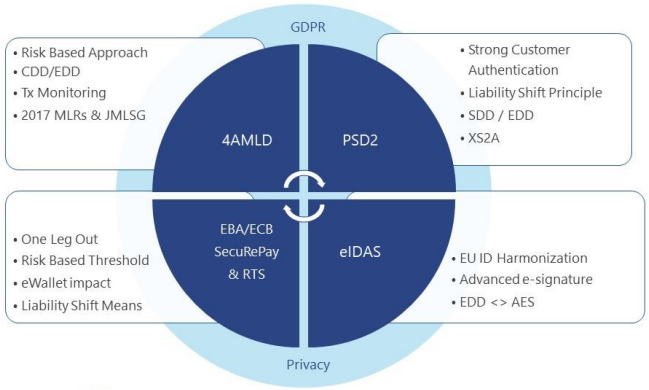
### iSignthis automates AML/CTF KYC and transaction processing

iSignthis Ltd is an EEA authorised EMI/MFI which automates AML/CTF Enhanced Due Diligence KYC & transaction monitoring via its payments and identity processing platform (Paydentity™) for AML regulated sector businesses including:

- Financial Institutions,
- banks, lending, crowdfunding, pension funds,
- securities / equities,
- FX, CFD, binaries, and futures traders,
- gaming, wagering, betting, casino's,
- money services businesses,
- payment service providers,
- insurance providers,
- real estate,
- digital currency platforms,
- eWallets, Fintech,
- other AML/Patriot Obligated businesses, and
- ***Ourselves, as an EU regulated Monetary Financial Institution!***

GDPR READY · PCI DSS · ISO/IEC 27001 · ico. · BÖRSE FRANKFURT · JCB · MasterCard Principal Member · ECSG Foundation Member Board Member

## 2. The EU Identity and Payment Landscape






## 3. PSD2 : Regulatory evolution is driving change

### 4AMLD and PSD2 require a more rigorous approach to IDV & Authentication

PSD2 & transactional payment processing authentication

- PSD2 is technological and business case neutral – this is a central tenet of the directive.
- All online payments > €30 required to undergo Strong Customer Authentication (SCA) using a method of Two Factor Authentication (2FA) to be linked to the card's owner. (EBA RTS, e-verification, ECB KC6.1)
- SCA does not necessarily mean 3DSecure! Other options available. PSD2 Liability Shift is via ECB Governance framework of card schemes (See SecurityofIPayments, KC7.6 & ECB Card Governance Framework)
- SCA not required for MOTO (See EBA RTS Comments [73])
- The use of 2FA without proving a persons identity first, is known as Strong Authentication (SA) – this is commonly used by some tech companies and is not compliant under the current PSD2 regulations. (See PSD2 Article 4, (29) & (30), EBA RTS Comments [1] and [274])



## 4. PSD2: Regulatory evolution is driving change

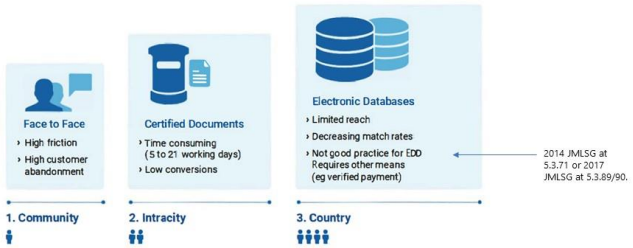
### 4AMLD and PSD2 are requiring a more rigorous approach

PSD2 & transactional payment processing authentication

- The risk based approach allowed for by the EBA in its RTS at Article 16 are set between 0.13% fraud on € 100 average to 0.01% to €500 average, with € 500 being the cap after which SCA must apply.
- The risk based approach allowed for by the EBA in its RTS is farcical, and was a late addition to the RTS based upon industry lobbying. The fraud rates specified are required to be so low, that PSP's will simply apply SCA rather than risk liability. (See ECB 4th Card Fraud report – .57% / 0.45% is more likely when 3DS not applied)
- One leg out transactions will present a massive challenge for Payment Service Providers (PSPs) to overcome. Verifying transactions of cards issued outside the EEA, when 3DSecure is not available will cause massive abandonment, as PSP unlikely to accept liability (RTS Rationale [16] and Comments [295], FCA Daft PSR Guidance )

## 5. 4AMLD / 2017 MLR's : Establishing Identity

Three main accepted means to perform **enhanced due diligence** Know Your Customer (KYC), all of which **rely on banking or government (original) sources.**






## 6. Cysec, Austrac & UK JMLSG Requirements


**Satisfying Regulations:**

Either Doc Uploads or Electronic Verification AND one of the second line.

By verifying payment, we confirm:

a) Source of funds
b) that funding is available
c) Instantly for cards or within 2 business days for SWIFT/SEPA : completing enhanced CDD of customer whilst onboarding customer and taking payment!
d) Paydentity™ incorporates bank issued credit and debit cards, as they are not only the leading online payment source, but also the largest single source of KYC data accessible globally.



## 7. 2017 Revised JMLSG – Remote Customer

- 5.3.90 The additional verification check may consist of robust anti-fraud checks that the firm routinely undertakes as part of its existing procedures, or may include:
- **requiring the first payment to be carried** out through an account in the customer's name with a UK or EU regulated credit institution, or an assessed low risk jurisdiction;
- verifying additional aspects of the customer's identity (see paragraph 5.3.29);
- telephone contact with the customer prior to opening the account on a home or business number which has been verified (electronically or otherwise), or a "welcome call" to the customer before transactions are permitted, using it to verify additional aspects of personal identity information that have been previously provided during the setting up of the account;
- communicating with the customer at an address that has been verified (such communication may take the form of a direct mailing of account opening documentation to him, which, in full or in part, is required to be returned completed or acknowledged without alteration);
- requiring copy **documents to be certified by an appropriate person.**

## 7. 2017 Revised JMLSG – Remote Customer

5.3.89 Where identity is verified electronically, [or] copy documents are used, or the customer is not physically present, a firm should apply an additional verification check to manage the risk of impersonation fraud. In this regard, firms should consider:

verifying with the customer additional aspects of his identity (or biometric data) which are held electronically; or

requesting the applicant to **confirm a secret code or PIN**, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, **PINs or other secret data** may be set up within the electronic/digital identity, or may be supplied to a **verified mobile phone**, or through a **verified bank account**, on a one-time basis, or

following the guidance in paragraph 5.3.90.



## 8. 'Recency' of data

What does "recency" mean? In practice? From a regulatory perspective?

**CySec, June 2016, Appendix IV, paragraph c:**
Electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information and negative information.
and
electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter.

**Austrac Regulations :**
Rule 4.10.2 (c) "how the data is kept up-to-date; "

**2017 Revised UK JMLSG :**
5.3.51 "for example, in relation to data sources used, or recency of information"
5.3.52 "The information maintained should be kept up to date, and the organisation's verification – or re-verification - of different aspects of it should not be older than an agreed set period."



## 9. Lets look at Electronic Verification – UK+AUS style – Historic Credit Reference File

JOAN LOUISE SMITH
REFERENCE: PAS 1234567

veda

### Personal Information

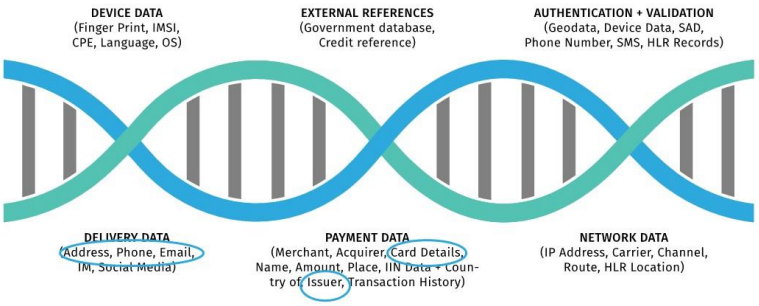
| Identity Details | |
|---|---|
| Name: | Joan Louise Smith |
| AKA (Also Known As) | Joan Louise Harrison |
| Date of Birth: | 15 Jan 1975 |
| Gender: | Female |
| Driver's Licence Number: | 12364578 |
| Address History: | 15 Tree Avenue RANDWICK NSW 2031<br>1/63 View Street CURL CURL NSW 2096<br>29/90 Fuller Street KENSINGTON NSW 2033<br>10 Beach Street MOOLOOLABA QLD 4557 |
| Employment History: | EASTFIELD PRIMARY SCHOOL<br>THE DEPARTMENT STORE |

### Financial Account – Express Bank

| Consumer Credit Liability Information | |
|---|---|
| Name of Provider | EXPRESS BANK |
| Account Type | Credit Card |
| Account Number | EPB0075 |
| Account Open Date | 11 Apr 2013 |
| Loan Payment Method | |
| Term Type | Revolving |
| Term of Loan | Unspecified |
| Relationship | Principal's Account (sole or joint borrower) |
| Secured or Unsecured | Unsecured |
| Balance Limit | $10,000 |
| Closed Date | |

## 9. DNA of a 'Real time' Electronic Payment Message

Card DNA



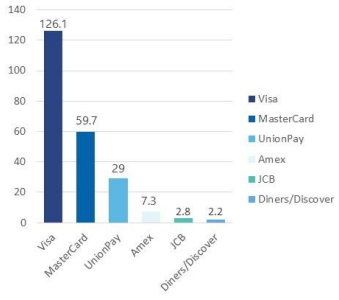

**Swift / SEPA DNA :** Originating Bank, Name, Amount, Currency

Shared with CRA File

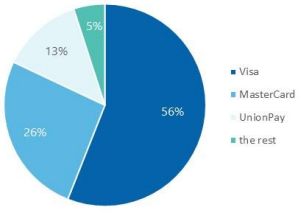


## 10. Cards – The Largest Payment & KYC Source

Purchase Transactions on Global Cards in 2015 (Bil.)



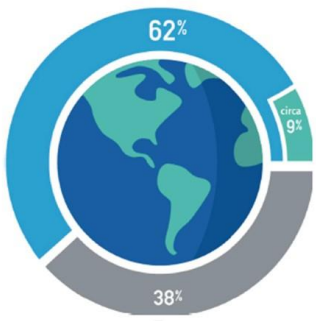

Market Share




- 9.5Bn cards on issue, globally
- According to Nilson, 3.5Bn are unique
- McKinsey estimates that 51% of the world's population is "banked" – corresponding also to ~3.5Bn persons.



## 11. World Population – 62% Banked / 38% Unbanked, with CRA Data accessible for ~ 9%




**62% Financially Included (banked)**

62% of the world's population are banked, making 'bank verified' persons the largest electronically accessible 'reliable and independent' source of KYC data.

**circa 9% Data Brokers Circa**

Data brokers can only identify Circa 9% of the world's population, providing merchants with a limited reach and low conversion rates.

**38% Unbanked**

38% of the world's population don't have a bank account and are unable to pay for services via a electronic payment, credit or debit card.

Source: World bank 2015 Findex, http://datatopics.worldbank.org/financialinclusion

## 12. Verifying a Customer through Creating a 'Secret'

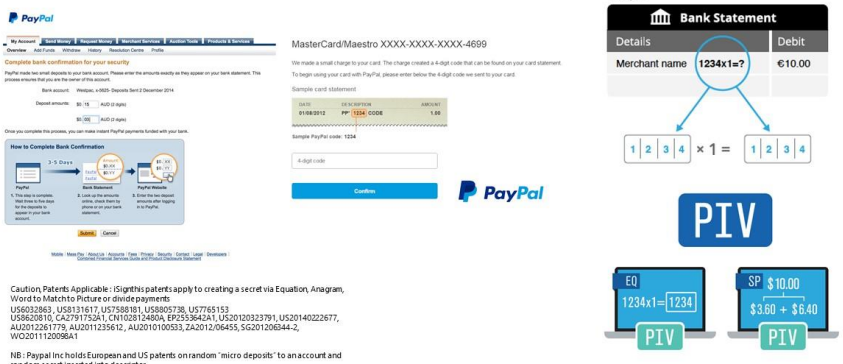
**5.3.89 Where identity is verified electronically, [or] copy documents are used, or the customer is not physically present……..**
requesting the applicant to confirm a secret code or PIN, or biometric factor, that links him/her incontrovertibly to the claimed electronic/digital identity – such codes, PINs or other **secret data** may be set up within the electronic/digital identity, or may be **supplied to a verified mobile phone, or through a verified bank account,** on a one-time basis, or following the guidance in paragraph 5.3.90.

**Commentary**
What's a 'verified' mobile phone?
The UK has no register of owners of mobiles,
purchasing prepaid does not require ID,
sending a SMS proves – what?
Even countries like Germany that require ID to purchase have difficult access to register of ownership
China has a register of owners of phone …but you'd expect that.

Bank and Credit Cards – several methods (many patented) exist to verify – beware of their use!
Eg Paypal https://www.epo.org/law-practice/case-law-appeals/recent/t090844eu1.html



## 12. Examples of Creating Dynamic Secrets to satisfy Key parts of 2017 JMLSG & PSD2 SCA Registration

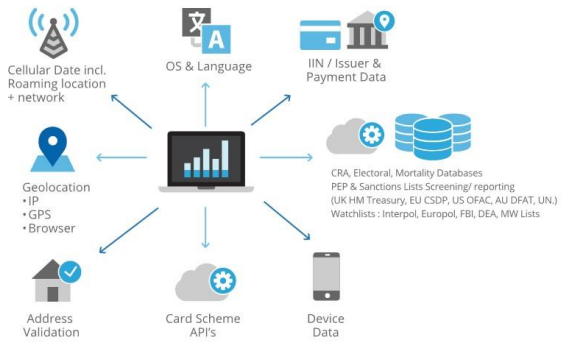



Caution, Patents Applicable : iSignthis patents apply to creating a secret via Equation, Anagram, Word to Matchto Picture or divide payments
US6032863 , US8131617, US7588181, US8805738, US7765153
US8620810, CA2791752A1, CN102812480A, EP2533642A1, US20120323791, US20140222677, AU2012261779, AU2011235612, AU2010100533, ZA2012/06455, SG201206344-2, WO2011120090A1

NB : Paypal Inc holds European and US patents on random "micro deposits" to an account and random secret inserted into descriptor.



## 13. Real Time Analytics – Screening and Reporting



## 14. Questions you should be considering

**For your PSP under the PSD2:**

- Will your PSP impose 3D Secure on all transactions?
- How will your PSP satisfy the 'one leg out' requirements, so you can accept cards from outside the EEA?

**For your KYC Electronic Verification Provider**

- How is 2+2 achieved outside the UK and Australia?
- What dynamic/real time element is used to satisfy 'recency' / 'up to date' requirements?
- What are your 'reliable and independent' data sources outside UK and Australia?
- Who are these sources shared with and are they registered with ICO equivalent?
- How often are they updated, and how are you alerted if they are / are not?

**Where document uploading is used**

- Uploaded Copy documents are not sufficient by themselves to satisfy UK, Australia, Cyprus, US or any EU regulatory regime for CDD – how do you verify to an enhanced due diligence standard per 4AMLD/JMLSG/CySec etc?



## Questions?

iSignthis®

- iSignthis Ltd (ASX:ISX / FRA : TA8)
- SWIFT/BIC : ISMCY21
- Contact @ iSignthis.com

# Notes

# Session 5
# 12:20-13:00

## 4MLD Preventative Measures- Risk Assessment

## Andrew Tait

*Partner, Gordon Dadds*

## Failure to Comply- Enforcement & Penalties

## Alex Ktorides

*Partner, Gordon Dadds*

**MLD4/5 Risk Assessment- Failure to Comply and Enforcement**

Andrew will be presenting on preventive measures required under the 4AMLD. with a strong focus on AML Risk Assessment – What it is? What's new? How to quantify risk, how to address change of control as well as going through audits and reviews.

Alex will then take us through Failure to Comply: disciplinary enforcement and white collar penalties. What should you be aware of and where should your focus lie in this matter. With all the new regulations coming through and the changing landscape, this is becoming more important that it has been before.

# Andrew's Bio

Andrew is a UK and Irish qualified solicitor and partner in the Gordon Dadds' regulatory solutions team. His key specialisms include AML policies and procedures, data protection and privacy, governance and risk management, gambling law and regulation. He is a member of the International Compliance Association and former Chief Compliance Officer, General Counsel and MLRO for ten years in a large Online Gaming Company.

He also has a technology and intellectual property background practicing as legal counsel in software licensing, telecommunications, entertainment and media sectors across Europe.

# Alex's Bio

Recognised in the Legal 500 as a recommended gaming lawyer, Alex advises and support clients on regulatory issues in sectors including accountancy, legal, property and gaming. The sorts of issues he deals with are anti-money laundering, bribery and corruption, defense to investigations/responding to unauthorized visits and criminal/civil aspects arising, as well as being the Head of Gordon Dadds own ethics and risk management function; he is the firms' MLRO.

Other matters that Alex deals with for clients are financial crime risk management strategies and technology solutions for the client on boarding process and lean process improvements.

GORDON DADDS

# MLROs.com & Gordon Dadds

Current preventive measures required under the 4AMLD

**Andrew Tait**
Partner

12 September 2017

## Prevention is the cure

- Corporate & Personal Liability for failing to take the necessary measures to help keep proceeds of crime out of the financial system
- Failures will result in the types of issues & enforcement which will be addressed by Alex Ktorides
- The cure for this potential liability is take the necessary preventative measures in the first place
- Prevention is broadly accomplished by Screening, Detection, Analysis, Intervention and Reporting
- The foundation for all this prevention is the **AML & TF Risk Assessment**

## Building the Foundation: AML & TF Risk Assessment

Legal Providence:

- **2005**: 3AMLD – Article 34 "Institutions …establish adequate and appropriate processes and procedures of …… risk assessment"
- **2007**: AML Regulations – Article 20 "A relevant person must establish and maintain appropriate and risk-sensitive policies and procedures relating to— (e) risk assessment and management"
- **2012**: FATF International recommendations improving money laundering and terrorist financing standards: identification process should be **comprehensive** and also **dynamic**
- **2015**: 4AMLD - Article 8 is dedicated to Risk Assessment for Obliged Entities
- **2017**: The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations, Article 18
- **2018**: 5AMLD – Requires further specific risks to be addressed

# AML & TF Risk Assessment: Regulatory Requirements

2017 AML Regulation: **Articles:** 16(2); 18; 19(1,4); 21(7,10); 28(12); 33(6); 37 (4,7)

Review risks by taking into account:

- Information made available by the relevant Supervisory Authority
- Group Entity's:

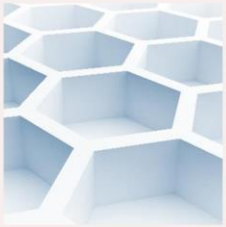
*customer base, geographical reach, transactions, products, services, delivery channels*

- Record all steps to achieve the above
- Provide a documented Risk Assessment to Supervisory Body upon request
- Update the Risk Assessment in line with the entity's changing risk landscape
- Carry out CDD in line with Risk Assessment

4

# Supervisory Bodies Requirements & Guidance

- Supervisory Bodies Requirements / Guidance
  - FCA: Supervise 7 categories of financial & credit institutions
    - JMLSG June 2017 Guidelines, Chapter 4
  - Gambling Commission
    - AML Guidance under consultation : Oct 2017
  - HMRC: Supervise of 7 diverse categories, incl Estate Agents, TCSPs, High Value Dealers
    - HMRC Guidance
    - RICS, NFOPP, ARP,ARMA
  - Approved Professional Bodies:
    - CCAB
    - Law Society



5

# 5AMLD: Additional Risk to be Factored in

- High Risk 3rd Countries
- Prepaid Cards
- Cyber currencies
- Beneficial Ownership Registers
- CDD Refreshers

6

# How: Research

Risk Identification

**Generic**

SA's own Risk Assessments & Guidance - Art17(9), Published failings, FATF Reports, 5AMLD specific risks:

- Geographical, Product, Delivery channel & Transactional

**Entity Specific**

Historical SAR Analysis, AML Flow Analysis, Operational, IT Systems, 3rd party verification providers:

- Customer base & services/operations
- Create questionnaire, broken down into the 5 categories

| Question | Answer |
|---|---|
| Describe your country blocking system, giving specifics of platform (web, mobile, flash, download, etc) orientated controls, proxy server identification, amazon cloud, etc | |
| Which countries do you block players from holding a real money gambling account & why (i.e. rogue/terrorist state, weak AML regime, strict prohibition against privately operated gambling with no license in place/ not possible etc) | |
| Do you have fraud rules in your (automated) risk system which prioritises increased due diligence/checks on players per country | |
| What Definition of Sanctioned countries do you use | |
| How & when do you screen for sanctioned countries | |

7

# Risk Evaluation

Review completed questionnaire & conduct a follow up session to evaluate the current controls by further questioning to determine the extent to which each existing control mitigates the risk of money laundering & terrorist financing – helps identify the gaps.

| Category | Risk Factor | Current Status | Evaluation Action to determine control gap | Results of evaluation – Identification of Actions to closer control gap. |
|---|---|---|---|---|
| Geographical | Players based in certain countries may pose greater inherent ML & Terrorism Financing (TF) risk given higher levels of corruption | On boarding processes do not highlight / have extra DD for high risk countries | Rank Countries according to international recognised corruption indexes | According to the Corruption Perception Index – the following counties were ranked in 2016- as having the highest corruption:<br><br>Somalia, S.Sudan, N.Korea, Syria, Yemen, Sudan, Libya, Afganistan, Guinea- Bissau,Venezuela, Iraq, Eritea, Angola, Republic of Congo<br><br>Supporting Documentation: Sch 1 |

8

# Risk Quantification

Quantify the risks and control gaps using an AML Risk Scoring Matrix.

| Risk Factor | Frequency | Impact | Score | Gap | Control Priority |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |

| Description | Score |
|---|---|
| Involves 75% of all transactions / continuous | 3 |
| Involves 5-75% of all transactions | 2 |
| Involves less than 5% of all transactions | 1 |

| Description | Cumulative Score |
|---|---|
| Involves Criminal (4) Reputational (3) & Financial risk (1) | 10 |
| Involves Reputational (3) Regulatory (2) & Financial risk (1) | 6 |
| Involves Regulatory (2) & Financial risk (1) | 3 |
| Involves Financial Risk (1) | 1 |

9

# AML & TF Risk Assessment

The AML & TF Risk Assessment Spreadsheet:

| EVALUATION ACTION TO DETERMINE CONTROL GAP | RESULTS OF EVALUATION - IDENTIFICATION OF ACTIONS TO CLOSE CONTROL GAP | Quantification<br>Freq x Impact = Total Risk Score<br>TRS x Gap Score = Gap Priority | | | | 0 – 20 Very Low<br>21 – 35 Low<br>36 – 59 Medium<br>60 – 75 High<br>76 – 90 Critical |
|---|---|---|---|---|---|---|
| | | FREQUENCY (3) | IMPACT (10) | TOTAL RISK SCORE (30) | GAP SCORE (3) | GAP PRIORITY (90) |
| **Investigate whether the backend admin system can support the generation of tasks/ emails/ prompts if not or too difficult then are 3rd party systems an option? Otherwise will need to rely on manual checks and be subject to human error and inconsistency where high turnover of staff. In addition out of office high alerts would help mitigate suspicious activity arising during these times.**<br><br>**See if the backend admin system can create reminders to assigned tasks (also to be determined).**<br><br>**This will be necessary in the future for the UKGC upgraded complaints handling requirements.** | Purely manual communication via email, phone. Admin Back end is used to denote "Fraud" status when player accounts are sanctioned<br><br>No possibility of adapting admin to create tasks, escalations, etc.<br><br>Links into GRPR consolidation, record keeping, information request | 3 | 10 | 30 | 3 | 90 |

10

# Control Gap Analysis

The final step is to create an AML controls project scoring to prioritise those controls in most need of fixing taking into account the entity's risk appetite. This needs to be signed off by senior management (Art 19 (2))

| RISK FACTOR | GAP PRIORITY | What do we need to do? | How do we need to do it? | Timeframe/ implementation – how we get there | Resource/ Time/ Cost | Actions | Actionee |
|---|---|---|---|---|---|---|---|
| **CB 18. Customers who are financial officers/ directors/ corporate controllers/ accountants may have access to corporate funds where they could easily misuse the same & be able to hide their activity by changing records/ accounts** | 60 | Focus on finding out VIP customer job title & employer | Customise VIP information cards to ensure that as player rises through VIP levels job description fields will need to be completed | Q1/17 – manual processes & may require changes to CRM | Minimal Time & Cost | Set up meeting with to discuss the CRM VIP card, amend to add AML requirements, discuss incentivisation for agents to complete | XX |
| **O. 10 Lack of internal controls and measure of effectiveness and meeting requirement** | 54 | Need to create self-audit and annual AML review & Report | Draft self-audit methodology & process | Q4 – Manual process | Minimal Time & Cost – internally<br><br>1st year cost for external audit | Design a process of a self-audit/ mystery shopper | XX |
| **T 6. Use of payment systems which allow easy P2P transfers as part of collusion ca be indicative of AML** | 54 | Need to review which payment methods allow inter-wallet transfers | Conduct a survey of current payment methods | Q4 | Minimal Time & Cost | This will form part of Threshold Scoring Matrix | XX |

11

# Control Gap Analysis

This ensures compliance with:

Article 19(1)

(1) A relevant person must—

- (a) Establish and maintain policies, controls and procedures to mitigate and manage effectively the risks of money laundering and terrorist financing identified in any *risk assessment undertaken by the relevant person under regulation 18(1)*

(2) Article 18(4)

- A relevant person must keep an up-to-date record in writing of all the steps it has taken under paragraph (1), unless its supervisory authority notifies it in writing that such a record is not required.

12

# Change Control

AML & TF Policies & Procedures

- Article (19 (1) (b). Where material changes in risk landscape need to trigger re-assessment of existing or new risks & subsequent changes to policies & procedures: signed off by Senior Management.
- Annual review of Risk Assessment & Audit of performance & efficiency of policy and procedures. Report prepared by MLRO with recommendations. Senior Management meeting.
- Shifting Risk Appetite will need to be factored into the Risk Assessment
- The introduction of new technology needs to be taken into account (Article 19(4)(c))

13

# Proportionality

Risk Assessments must take into account the nature and size of the Business (Art 18 (3)

- AML & TF Controls need to be proportionate (Article 19 (2))

14

# International AML & TF Risk Assessments

- Article 20: Group Company Application of all UK compliant Policies & Procedures required under Article 19 (1) across all subsidiaries & branches
- Must factor in EEA requirements
- Must adopt UK standard in third countries where group companies are based unless prohibited from doing so, in which case - report to SA & take additional measures

15

# The Benefits

- You are now compliant in this regard
- You have seriously mitigated the risk of Personal and Corporate Liability
- Your AML & TF Controls are now directly relevant and tailored for your business
- You have streamlined existing controls, potentially reducing costs & introducing greater efficiencies (i.e. use of newer verification technologies)
- You are now future proof by continually evaluating and reviewing your controls
- You have centralised your AML & TF controls across your group making oversight and management much easier
- Your whole organisation is now aware of AML &TF risks and is in some way contributing to the fight against money laundering and terrorist financing
- Your senior management are involved and responsible for the success of your AML & TF controls, so will need to ensure this is properly resourced



GORDON DADDS

# Thank you

If you would like more information please contact:

**Andrew Tait | Partner**
e: andrewtait@gordondadds.com
t: +44 (0) 20 7759 1587

GORDON DADDS

# MLROs.com & Gordon Dadds

Financial crime update and regulation overlap

**Alex Ktorides**
Partner, Head of Ethics and Risk Management

12 September 2017

## Background

- Overlap between financial crime and regulatory investigations and breaches
- Why should we care?
- Overlap
- Case Study
- Recent trends



## Overlap

- Financial crimes include:

  Bribery and corruption, cartel and price fixing, money laundering, terrorist financing, operating scams, insider dealing etc.

- Regulatory breaches include:

  Causing harm to customers from mis-selling, misleading accounting, poor systems and controls, bringing the profession or sector into disrepute, acting in own interests, breaching fiduciary duties etc.

# Why do we care?

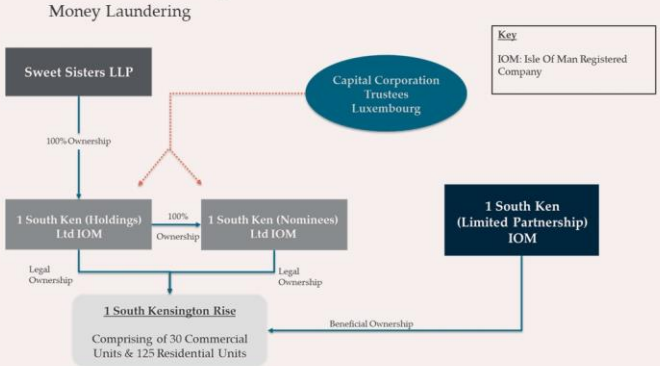
- GDPR – 4% turnover or £20m
- Competition law – 10% of annual group turnover and jail time
- Proceeds of crime – unlimited fine and jail time
- Bribery and corruption – unlimited fine and jail time
- Reputation, management time, legal costs, share price, loss of income or liberty

# Examples of Overlap

- Powers:
  - FCA – criminal and regulatory
  - HMRC - criminal and regulatory
  - Gambling Commission – criminal and regulatory
- Information sharing:
  - Memorandum of Understanding e.g. HMRC, PRA, FCA
  - Crime Agencies sharing techniques and information
  - Super SARs

# Case Study

Money Laundering



# THE ADVERSE PRESS

www.adversedubaipress.ae Dubai's Favourite Newspaper 1st April 2016

Dubai Police have arrested Mr Aban Abbar as part of a probe into a price fixing and bribery scandal involving the oil refining industry and Government officials. Mr Abbar was arrested at Dubai International Airport upon his return from London, England. He is said to have been accompanied by various luxurious items from a spending spree in London.

The police say that they are investigating allegations of a secret price fixing arrangement and bribery by companies in Dubai who provide the hire of refining machinery to other refinery companies. It is said that the arrangement of the price fixing and bribery is so entrenched that the provision of hire contracts have only ever come from 3 companies in the last 5 years. The value of contracts alleged to be obtained as a consequence of corrupt activity is said to be in excess of $30 million.

The alleged bribes were paid to top government officials who have the influence to award state led contracts to these private entities.

One of these companies in the spotlight, AB Refinery Services LLC, is owned by Mr Abbar. Incidentally, the company has always secured the most lucrative contract.

Investigators raided the home of Mr Abbar yesterday morning in an effort to obtain more incriminating evidence and there is allegedly a vast array of evidence to incriminate him in the scandal. It is said that there was a briefcase containing $100,000 found at his home.

Mr Abbar lives in Dubai with his wife. They have two children, Ameer and Fatima.

7

# Recent Case/Trends

- FCA penalties lumpy but rising trend
- Regulators get a second wind? E.g. Gambling Commission, 888.com
- Rolls Royce, Tesco, Deutsche Bank
- Azerbaijan Laundromat
- De-risking by financial institutions

8

# Steps to take when the inspector calls

- Legal hold
- Scope any investigation (people, issues, risk of repeating, period)
- Self-report
- Co-operate
- Assess merits
- Fund/insure
- Dialogue
- PR/reputation damage limitation
- Consider conflicts
- Settle or fight

9

GORDON DADDS

# Thank you

If you would like more information please contact:

**Alex Ktorides| Partner**
e: alexktorides@gordondadds.com
t: +44 (0) 20 7759 1584

# Session 6
# 14:00-14:45

# Criminal Finance Act 2017- Failure to Prevent Tax Evasion

## Simon Airey

*Partner, Paul Hastings*

**Criminal Finance Act 2017- Failure to Prevent Tax Evasion**

Simon Airey will outline the key aspects of the new corporate criminal offence of failing to prevent the facilitation of tax evasion. He will highlight important features of the related Guidance and what companies need to be doing now. He will focus on the importance of a properly constructed risk assessment, an analysis of the risks related to certain categories of "associated person" and the need for tailored training for senior management, staff and relevant third parties. He will point out likely pitfalls for the unwary, provide examples of taxes and duties that may give rise to particular problems and will suggest what are to be likely areas of focus for HMRC and the SFO in investigating and prosecuting companies who fall foul of the law.

# Simon's Bio

Simon Airey is a Partner in the London office of Paul Hastings. Mr. Airey specialises in global investigations, financial and regulatory crime, bribery and corruption, money laundering, tax and fraud inquiries, dawn raids and corporate compliance. Mr. Airey has conducted a wide range of investigations in different sectors, principally construction, defence, financial services, gambling, oil and gas, logistics, pharmaceuticals, and telecommunications. He advises a large number of multinational groups in relation to their global Anti-Bribery & Corruption (ABC) compliance programmes and has lectured extensively in the U.S., Europe and Asia in relation to the UK Bribery Act and related matters. Mr. Airey started his career as a barrister in private practice during which time he gained experience of a broad range of regulatory, criminal, and civil litigation at all levels of the court system.

# FAILURE TO PREVENT THE FACILITATION OF TAX EVASION

**The Corporate Criminal Offence**

Simon Airey

PAUL HASTINGS

## OVERVIEW



- The UK *Criminal Finances Act 2017* introduces new criminal offences where a company fails to prevent its 'associated persons' from facilitating tax evasion by a third party.
- Associated persons is defined broadly as any person or entity that provides services "for or on behalf of" the company. This can include a company's employees, agents, intermediaries, subsidiaries, JV partners etc.
- The Act applies to the evasion of both UK and non-UK **tax** and **duties**.
- The domestic offence will apply to any company, even if they have no connection to the UK, where their associated persons facilitate the evasion of a UK tax or duty.
- The overseas offence will apply to any company that is incorporated in the UK or is carrying on a business - or part of a business - in the UK.

PAUL HASTINGS

## OVERVIEW



- The legislation comes into force on **30 September 2017**, which coincides with the first data exchanges under the Common Reporting Standard.
- The legislation resembles the UK *Bribery Act 2010* by
  - (i) holding corporations liable for acts of their associated persons; and
  - (ii) having extensive extra-territorial application.
- The **only defence** is for a company to show that it had "reasonable procedures" in place to prevent the facilitation of tax evasion (as opposed to "adequate" procedures under the Bribery Act), or that it was reasonable, in the circumstances, not to have any such procedures.

PAUL HASTINGS

## THE DOMESTIC OFFENCE



- A failure (1) by a company or partnership (a "relevant body") incorporated anywhere in the world; (2) to prevent the criminal facilitation; (3) by one of its associated persons (see further below); (4) of the criminal evasion of a **UK tax or duty**, payable by another person or entity.
- There is no need for the company to have any presence in or relationship with the UK for it to be caught by the legislation.
- The domestic offence will be prosecuted by HM Revenue & Customs.

PAUL HASTINGS

## THE OVERSEAS OFFENCE



- A failure (1) by a relevant body; (2) to prevent the criminal facilitation; (3) by one of its associated persons; (4) of the criminal evasion of a **non-UK tax or duty** payable by another person or entity.
- This offence applies to a relevant body incorporated in the UK or carrying on a business - or part of a business - in the UK (for example, via a subsidiary or sales operations in the UK, or even via a listing on the London Stock Exchange).
- A company will also be caught where it does not have a UK presence of this type but any part of the criminal facilitation takes place in the UK.
- The overseas offence will be prosecuted by the Serious Fraud Office.

PAUL HASTINGS

## REMEMBER....



- There is no need for there to have been an actual prosecution/conviction for tax evasion for either the domestic or overseas offence.
- There is no need for the person facilitating the tax evasion to have intended or delivered any benefit to the company.
- There is no need for the company to have intended to play any role in the tax evasion, the focus of the offence is the failure to prevent.

**The new offence is therefore broader in its scope than the Bribery Act.**

PAUL HASTINGS

## 'ASSOCIATED PERSONS'

7

- Any person or entity that provides services "for or on behalf of" the company.
- Can include employees, agents, JV partners, contractors or subsidiaries of the company.
- To be determined by reference to "all the relevant circumstances", i.e. not just by the formal legal relationship between the company and party in question.
- The Draft Guidance* does however make clear that an assessment of whether 'reasonable procedures' (see below) were in place will take into account the level of control which a corporation exercised over an associated person.
- Importantly, for both offences, the associated person must be acting **in that capacity** whilst committing the facilitation. Companies cannot be liable for the actions of an associated person who is on a 'frolic of their own' (i.e. a rogue employee who facilitates another persons' tax evasion in circumstances where their actions have nothing to do with the conduct of their job).

*Finalised Guidance not yet available at time of writing but expected imminently.

PAUL HASTINGS

## PENALTIES

8

- Unlimited fines
- Increased scrutiny from other regulators (FCA / SFO etc.)
  - Might a tax issue indicate broader fraud/bribery issues?
- Reputational risk
- Risk of debarment / difficulty winning government contracts
- Loss of licences / regulatory authorisations
- Risk of sanction
  - FCA approved persons?
  - Senior Managers?
  - Civil litigation against management by shareholders for breach of duty?

PAUL HASTINGS

## DEFENCE OF REASONABLE PROCEDURES

9

- The defence of 'reasonable procedures', rather than 'adequate' procedures, suggests a slightly less onerous standard than that which applies under the Bribery Act.
- The Draft Guidance does not seek to define 'reasonable procedures'. Instead, it suggests that reasonable procedures might be based upon the following six key principles:

1. a risk assessment;
2. procedures that are proportionate to risk;
3. top (board) level commitment;
4. communication and training;
5. due diligence; and
6. monitoring and review.

PAUL HASTINGS

## DEFENCE OF REASONABLE PROCEDURES

10

- The most important requirement is arguably the risk assessment, without which it will be difficult to show that any related procedures are proportionate and have been tailored to relevant risks.
- The absence of a proper risk assessment will make it difficult for a company to take advantage of the 'reasonable procedures' defence.
- The first thing a prosecutor is likely to ask for is a copy of the company's risk assessment. It should therefore be carefully constructed and drafted.
- Do not accidentally create a 'road map' to potentially incriminating issues within your company.

PAUL HASTINGS

## DO NOT UNDERESTIMATE THE SCOPE OF THE OFFENCE….

11

- Companies need to consider the new offence carefully when preparing their risk assessments.
  - What products and services does your company **offer** which have a tax angle?
  - What products and services does your company **receive** which have a tax angle?
  - Who are your associated persons?
  - Which of your associated persons might have the skills or knowledge to aid someone in their criminal tax evasion?
  - Which of your associated persons might unwittingly help facilitate tax evasion?
- Remember that subsidiaries can be associated persons.
  - Does your company use any aggressive intra group tax mitigation structures / schemes?

**THE NEW OFFENCE IS NOT JUST A MATTER FOR THE FINANCIAL SERVICES SECTOR**

PAUL HASTINGS

## DO NOT UNDERESTIMATE THE RANGE OF TAXES TO WHICH THE NEW OFFENCE APPLIES…

12

- **VAT**
  - Does your company ever pre or post-date sales receipts or purchase invoices?
  - Might good or services (sold or purchased) be described creatively to minimise a potential VAT liability?
  - Are invoices directed to overseas companies to avoid VAT?
- **Corporation Tax**
  - Does your company ever manipulate dates of asset acquisitions or adjust the value of assets to claim tax reliefs?
  - What about over or under stating stock valuations in year-end accounts to reduce Corporation Tax liabilities?
  - Have your employees ever taken steps to help a supplier minimise their Corporation Tax liability?
- **Import / Export duties**
  - Could colleagues be adjusting figures to minimise import or export duties, either for the benefit your suppliers or another group entity?

PAUL HASTINGS

## DO NOT UNDERESTIMATE THE RANGE OF TAXES TO WHICH THE NEW OFFENCE APPLIES…

13

- **Income Tax**
  - Do you, or your associated persons on your behalf, offer products or services designed to reduce your client's Income Tax liabilities?
  - Could these be used inappropriately by your clients?
- **Stamp Duty?**
- **Property Taxes?**
- **Industry specific taxes?**

PAUL HASTINGS

## LEGACY CASES

14

- Although the new offence is not retrospective, there is a risk in 'legacy' cases that a company could still be exposed to prosecution.
- This could occur where an employee has set up an arrangement before 30 September 2017 that was intended to facilitate tax evasion; that employee then leaves the company and the company continues to provide services to the client, ignorant of the tax fraud that is continuing.
- If another employee discovers the fraud after 30 September 2017 but continues to provide services, the authorities in the UK might consider commencing a criminal investigation on the basis that reasonable procedures were not in place to prevent the fraud from continuing.
- It is irrelevant that the company didn't know about the fraud – the offence is failing to prevent it.
- The employee may also be guilty of an aiding and abetting offence and/or may be guilty of an offence under the *Proceeds of Crime Act* 2002 if they fail to fulfil a statutory obligation e.g. to report the fraud, or if they become involved in an arrangement relating to the proceeds.

PAUL HASTINGS

## CRIMINAL LAW NOT TAX LAW

15

- The offences are a matter of criminal law, not tax law.
- Accordingly, legal advice should be sought from suitably qualified professionals with relevant experience. Where appropriate, this can be done in conjunction with tax experts (either within the company or externally).
- Seeking preliminary advice within a legally privileged environment may also encourage open discussion so that the subsequent risk assessment is more fruitful.

PAUL HASTINGS

## ANY QUESTIONS?

PAUL HASTINGS



Simon Airey
Partner
Tel: +44 (0)20 3023 5156
Mob: +44 (0)7738 295 326
simonairey@paulhastings.com

PAUL HASTINGS

# Session 7
# 14:45-15:30

# The Impact of Terrorist Financing

## Andrew McDonald

*Former Head of the NTFIU*

***The Impact of Terrorist Financing***

**Why we need to remain vigilant**

- Current terrorist threat and CTF issues
- What are we experiencing in the UK and how it differs in Europe / other global areas.
- Factors that might affect the overall threat – why CTF is different from other financial crime.

**Good news despite the threat**

How financial intelligence and contextual information is so valuable to CTF effort

The importance of developing the Public/Private sector partnerships

Positive impact of the UK JMLIT

**How Board members or senior managers can ensure that the firm is compliant with law and regulations**

- Understand the Risk Based Approach recommended by FATF
- Ensure the responsibilities of the Board in conjunction with the MLRO
- What processes are in place to ensure that suspicious activity is identified, understood and reported via SARs to the NCA

# Andrew's Bio

Andrew retired in January 2017 as Head of Specialist Investigations and National Terrorist Financial Investigation Unit (NTFIU) at SO15 Counter Terrorism Command at New Scotland Yard. He had strategic and tactical oversight for all financial and crime disruption investigations to identify, arrest and charge or disrupt terrorist offenders and their associates. He served over 30 years within the Metropolitan Police Service; 20 years were with specialist covert and overt operations within a counter-terrorist and organised crime environment in New Scotland Yard detective teams.

In a previous role as Head of Metropolitan Police Fraud Squad, Andrew was responsible for designing the current operating model for fraud and cyber-crime and assisted in its implementation.

In January 2017, Andrew was appointed as the Compliance Officer for the Independent Parliamentary Standards Authority; a role that he undertakes on a part-time basis.

In addition to his policing career, Andrew has delivered bespoke training and consultancy as a subject matter expert or specialist advisor to individuals from many law enforcement and commercial organisations within the UK and overseas. He specialises in deliveries to understand and manage illicit finance, compliance responsibilities for senior executives, crisis and risk management, decision-making and the management of intelligence.

He holds Batchelor of Science and Master of Business Administration degrees and is a fellow of the Chartered Institute of Management.

## Andy McDonald

- 30.10 years service with Metropolitan Police Service
- 26 years substantive detective
- 20 years in New Scotland Yard specialist covert and overt teams
- Financial Crime a 'constant' and cross-cutting theme
- DSU at Counter Terrorism and UK NTFIU to finish
- Previously Head of Fraud Squad
- Now a Public Servant and Specialist Advisor/Consultant

- Cant wait to finally retire.... at some point
- ..... but will really miss it..... If it ever actually happens!!

## Agenda

2

Why CTF - In addition to everything else?

Some Good News

Key Take Aways and Q&A

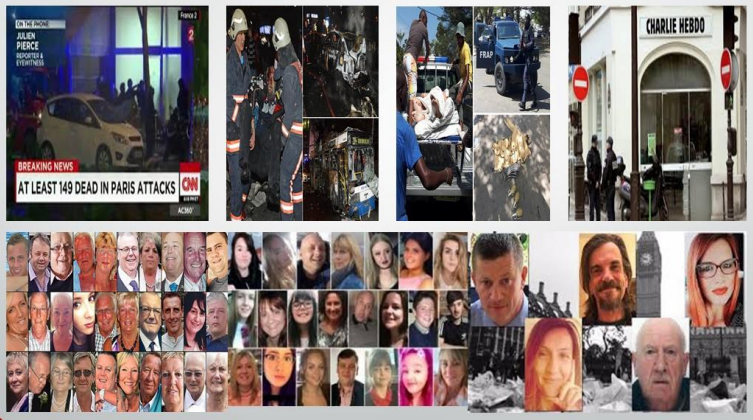
Current Terrorist Threat

Importance of SARs

## "Threat" - No 'Safe' Continents – No One Method


... AND FINLAND, RUSSIA, BARCELONA... AND ALL THOSE RARELY REPORTED

## The Victims – TF has Devastating Effect




## Threat Level

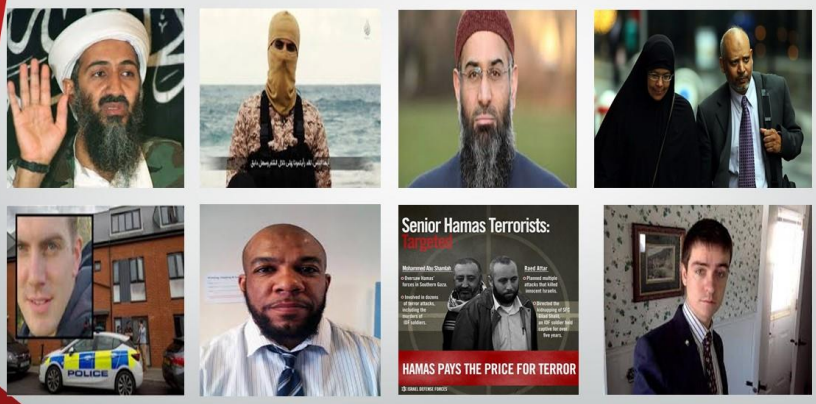
| | |
|---|---|
| The threat level in the UK from international terrorism | SEVERE |
| The threat level in Great Britain (England, Wales and Scotland) from Northern Ireland -related terrorism | SUBSTANTIAL |
| The threat level in Northern Ireland from Northern Ireland-related terrorism | SEVERE |

- Critical – An Attack is Expected Imminently BRIEFLY!
- **Severe – An Attack is Highly Likely**
- Substantial – An Attack is a Strong Possibility
- Moderate – An Attack is Possible but not Likely
- Low – An Attack is Unlikely

MAINLAND EUROPE IS VERY DIFFERENT – MANY AT CRITICAL

AN ISLAND EXISTENCE MAY HAVE SOME SECURITY ADVANTAGES!

## Spot the Terrorist – Easy to do??




What about an 'extremist' – what *can* you do?

## Nature of the Threat – It's Different to AML/Fraud

1. The **three 'F'** – FTF's / Facilitators / Financiers
2. The **Syria/Iraq** factor – unifying disparate groups
3. The threat posed by **returning fighters**
4. Sophistication of the recruitment operation – **online**
5. **Radicalisation** of the **young** (More 'F's' – females / families)
6. **Safeguarding** and Mental Health issues
7. Links to **chaotic** criminals – **Criminal access to firearms**
8. **Fraud** is a really big 'F'! – up 53%; reinforcing key messages
9. **Financial Intelligence and Evidence crucial to all above - TF Hard to Prove!**

INPUT TO AMLP FORUM IN 2013:

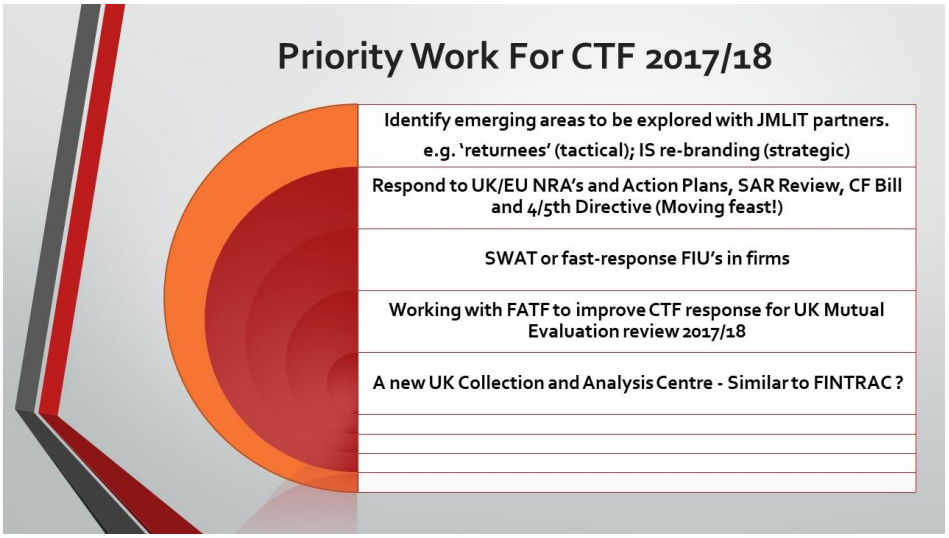
" THE UNKNOWN THREAT FROM NEW START-UPS AND FINTECH……
BUT I BELIEVE THERE MAY BE SOME REAL BENEFITS"

## UK Citizens - Syria Travellers two year focus – now returnees is key issue

## Don't Take Our Eyes Off The (Other) Ball(s) !


Some Good News!
GCHQ
SECURITY SERVICE MI5
MINISTRY OF DEFENCE
SIS SECRET INTELLIGENCE SERVICE
NTFIU
NCA National Crime Agency
CHARITY COMMISSION
HM Revenue & Customs
DWP Department for Work and Pensions
Financial Intelligence Permeates ALL CT Investigations


More Good News!
jmlit Joint Money Laundering Intelligence Taskforce
MINISTRY OF DEFENCE
WESTERN UNION
Lloyds
RBS The Royal Bank of Scotland
citi
Home Office
HSBC
NCA National Crime Agency
MoneyGram
NTFIU
BNP PARIBAS
RUSI www.rusi.org
FCA
Santander
Foreign & Commonwealth Office
POST OFFICE
Standard Chartered
Bank of America Merrill Lynch
bba
BARCLAYS


Priority Work For CTF 2017/18
Identify emerging areas to be explored with JMLIT partners.
e.g. 'returnees' (tactical); IS re-branding (strategic)
Respond to UK/EU NRA's and Action Plans, SAR Review, CF Bill and 4/5th Directive (Moving feast!)
SWAT or fast-response FIU's in firms
Working with FATF to improve CTF response for UK Mutual Evaluation review 2017/18
A new UK Collection and Analysis Centre - Similar to FINTRAC ?

## Issues for Board Members – new and established

**Accepting that there is a frequently changing landscape:**

**Are you satisfied with / have training for the following?:**

- **Your firm's approach to Understanding, Accepting, Managing and Mitigating RISK**
- **How your firm identifies and reports 'suspicious activity' – People and Systems**
- **What the impact is for 'getting it right…. Or wrong'? – Legal or Reputational issues**
- **How the firm is accountable re procedures and reporting or risk and suspicion?**
- **The contingency plans in place if things don't go as expected**

## The Importance of Suspicious Activity Reports

**Most Frequently Used Indicators in TF Case Disclosures:**

- **International transfers** to or from locations of specific concern
- ATM Withdrawals, often linked to MSB or other platform transfers
- Retail Transactions – Outdoor supplies, knives, bomb-making components, VEHICLE HIRE!
- Charity/Relief organisation linked to transactions – who are donors/trustees?
- Transaction References
- Dormant Account – Think Manchester – Abedi
- Customer Behaviour – Think Funding - Gollamully's
- **Media coverage** of account holder's activities - £66 to 'bomb' Manchester - Sun/Times
- **Law Enforcement enquiries – Every CT investigation has FI strategy**

**Large percentage of SARS submitted under TACT are because of LEA enquiries or Media**

***Ie Defensive and Reactive; rather than Proactive***

## Potential Intelligence Within a SAR

- **Names**
- **Dates of Birth**
- **Addresses**
- **Associates**
- **Identity documents – TRAVEL/BORDERS**
- **Occupation**
- **Places frequented**
- **Vehicles – TRAVEL/BORDERS**
  **130 KILLED BY VEHICLES 2017**

- **Account numbers**
- **Associated / joint accounts**
- **Transactions**
- **Transfers**
- **Account turnover**

- **IP Addresses**
- **Telephone no's**
- **Email addresses**

**If possible, please discuss what you propose to include in SARs – LEA's can worry about sanitisation and disclosure.**

**Help with terrorist 'lifestyle' via Finint and Comms Data**

## Key CTF (and Other Illicit Finance) Take-Aways

1. Red Flags / Indicators? – Not obvious…. But typical
2. Some guidance issued via FATF and Law Enforcement via FIU's
3. Terrorists can be vulnerable through available Finint and Comms. Data
4. Recognise Risk at 'On-boarding' stage / EDD stage – 'UNDERSTAND'
5. Ensure appropriate accountability and documentation
6. If you are suspicious – REPORT IT ! – LEA's will help and work with you

## DISCUSSION POINTS
(My Selfish Ones!)

- What could you do if that FINTRAC-style facility were available?
- The over-arching, forthcoming regulation by OPBAS
- Does the legal and regulatory environment support new business models?
- What can new firms do to assist understanding and acceptance?
- How can current or potential technologies assist AML/CTF requirements
- How do you link with or rely on 3rd party data and assurance?
- ie… how can you nurture confidence in your offerings to established financial and public sectors that does not understand technology?
- Plus numerous 'off topic' questions!

# Session 8
# 15:50-16:40

## Panel Discussion
## Regulations: Synergies, Conflicts & AML

### Jonathan Williams

*Former Head of Payments & Strategy, Experian*

### Roy Ramm

*Former Head of SOCA & Chairman, Comsec*

### Dominic Thorncroft

*Chairman, AUKPI*

### Colin Darby

*Managing Consultant, Bovill*

### Emma Lindley

*Director, Innovate Identity*

**Panel Discussion– Regulations: Synergies, Conflicts and AML**

The panel will be looking at how the various new pieces of legislation such as PSD2, GDPR and UK's data protection bill overlap; and what to do when they do! The panel will also be addressing the issues of how different stakeholders are affected by each of these contradictions and how that can lead to conflicts of interest. This promises to be a lively discussion from a diverse panel of significant SME's each bringing a wealth of experience and a different perspective on regulation, Regtech, financial crime and compliance.

# Jon's Bio

Jonathan Williams is an independent consultant in payments, identity and fraud prevention working for advisory firm Mk2 Consulting. Jonathan also brings experience in cybersecurity, telecommunications and software to his clients. Areas of special interest are PSD2, Identity Assurance, financial crime and ACH fraud.

Jonathan joined Mk2 from a role as head of Strategy and Product for Payments at Experian. Prior to this he was responsible for the product propositions which took two start-ups to IPO and one to acquisition: Content Technologies, Virata Corporation and Eiger Systems. He has also held engineering and IT roles at British Aerospace (now BAE Systems), the University of Cambridge and Advanced Telecommunications Modules Ltd

Jonathan speaks at many conferences worldwide and has recently addressed audiences for the Association of Corporate Treasurers, the Federal Reserve's conference on payments and EuroFinance. He also writes for trade journals including The Treasurer and Future Finance.

Jonathan holds an MA in Theoretical Physics and a postgraduate qualification in Computer Science from the University of Cambridge and is a member of the Payment Strategy Forum's Financial Crime, Data and Security working group and the Open Forum on Open Banking.

# Roy's Bio

Roy retired from public service in 1996 as Commander of Specialist Operations at New Scotland Yard with an 'exemplary' record and having been, at the time, the youngest Commander to be appointed.

He has worked extensively with UK government departments, including the Home and Foreign Offices and with UK and US specialist military and intelligence agencies. He has conducted security assessments on behalf of the British Government and reviewed serious crimes investigations in British Protected Territories.

He also offers high-level advice to major gaming companies on compliance and security issues, AML and Assurance Statements. He has led the industry's engagement with the UK government at ministerial level. He has given evidence to numerous parliamentary enquiries and committees.

# Dominic's Bio

Dominic has been chairman of the Association of UK Payment Institutions since 2005. The Association aims to provide a forum for information sharing and thought leadership in the payments space, primarily as it relates to FCA authorised and registered payments institutions. Compliance with regulatory issues are at the top of Association's agenda (including payments, financial crime, data protection legislation, etc). All payment firms need access to banking facilities, and there are new legal requirements in PSD2 which oblige banks to provide such access on a 'proportionate, objective and non-discriminatory basis'. The key challenge now is to create a framework for dialogue across all stakeholders which can make this an operational reality.

# Colin's Bio

Colin is a specialist financial crime regulatory adviser with 10 years' experience across the banking and asset management sectors.

He's currently working on the Court appointed Corporate Compliance Monitor overseeing HSBC's implementation of the US Department of Justice deferred prosecution agreement.

Before joining Bovill in 2015, Colin worked in a big 4 firm as an AML subject matter expert. He delivered a wide range of projects for banks and asset managers. Colin also worked at the FSA for nearly seven years.

Through his career to date, Colin had gained valuable insight and experience of establishing financial crime regulatory requirements, enforcing those requirements and advising authorised firms regarding compliance with them.

# Emma's Bio

Emma has been instrumental in the development of the UK digital identity market since 2003, initially working for GBG plc as part of the team that developed and took to market ID3 (then called URU) and latterly leading the development of the ID3 service globally.

In 2012, she founded Innovate Identity an independent consulting firm. She now acts as an advisor to many global brands, enabling identity as part of their digital transformation strategies. She also holds several board level advisory roles including Open Identity Exchange.

Emma is recognised in the Innovate Finance Powerlist for Women in Fintech 2016, Know Identity Top 100 Leaders in Identity 2017 and was voted CEO of the Year at the One World Identity Awards.

She studied identity, security and privacy at Harvard, has an MBA from Manchester Business School and completed her thesis on competitive strategy in the identity market place.

# Notes

# Notes

# Session 9- Keynote Speaker 16:40- 17:20

# JMLIT- Daesh Finance- Dual Use Goods

## T S/Chief Inspector Patrick Rarden MBE

*City of London Police Economic Crime Directorate*

Patrick will be presenting on the challenges that countering Daesh with their territorial controls and pseudo state structures have represented and how the international community has reacted to the challenge. He will be discussing the issues that the different nature of Daesh's economic activities presented and how these are likely to change as they lose control of the self-proclaimed Caliphate. In addition, Patrick will provide an insight into the importance of the public private partnership through the JMLIT in the UK as well as working with other industries to prevent the inadvertent helping of terrorist activities. The discussion will be under Chatham House rules.

**Please note there is no handout material for this session, we have added some extra notes pages for your convenience.**

**Patrick's content is under strict Chatham House Rule**

# Patrick's Bio

Patrick is a T S/Chief Inspector in the City of London Police Economic Crime Directorate and represents the City of London Police on the 'Terrorist Finance Experts Working Group' of the Joint Money Laundering Intelligence Task Force (JMLIT). He was the first reservist police officer to join the Economic Crime Directorate working on major financial system related cases in 2010 and was appointed MBE for Services to Policing in 2014. He is an officer in the British Army Reserve.

Patrick is a senior consultant who was Finance Lead in the HMG C-Daesh Taskforce from October 2015 to end of March 2017. This involved providing subject matter expertise on counter threat/terrorist finance from a government and private sector perspective taking into account the particular challenges that Daesh represented. He represented HMG at the Counter ISIL Finance Group Coalition meetings in addition to giving evidence before the Foreign Affairs Committee investigation into Daesh Finance and presenting at the UN Counter Terrorism Conference in New York in December 2016. He has worked closely with the United States Treasury and other co-leads in the C-ISIL Coalition. In particular he worked with the US State Department and the oil industry in putting together a list of spare parts that the Daesh needed for their hydrocarbon activities and has an extensive knowledge of the issues of dual use goods and the challenges that regulating these in regard to non-state actors bring.

Before 2015, Patrick worked in the front office, institutional side of investment banking as an equity trader, sales person and sales trader after graduating from Worcester College, Oxford in 1989 and has extensive experience in the trading and managing of asset classes and working across Europe with a multi jurisdictional client base. He is a fluent German speaker and has worked in Germany, France, Switzerland, Ireland and the UK in his 26 year career in banking

Patrick was a Trustee Director of the national Fraud Advisory Panel from 2011 to 2015 and is a member of the Institute of Directors.

# Notes

# Notes

# Session 10
# 17:20- 17:30

# Panel Q&A

*As usual we will form a small panel from the day's speakers and key delegates from the audience to have a final question and answer discussion to deal with any outstanding issues from the day that have been left unresolved.*

# Notes

# MLROs.com Latest News

1. MLROs.com Member Events
2. Compliance matters event offer
3. Current News on MLROs.com
4. MLROs.com Advisory board
5. Social Media
6. LinkedIn Community
7. Upcoming Events

# MLROs.com Member Events

**MLROs.com Full Day Conferences**

Our conferences provide an unparalleled opportunity to get informed on the very latest trends with information from the industry experts working at the cutting edge of our shared profession. These are always extremely popular and usually sell out weeks before the event. Conferences provide an unmissable opportunity for targeted education and networking with peers, industry vendors and service providers at minimum cost. Our suggestion is to register early and join our mailing list!

**Free Practitioner Member Briefings**

Our free to attend members meetings are accepted through the industry as an essential forum that helps members keep fully informed of the latest trends and information, whilst providing a pleasant and positive environment for networking geared to fit in with the busy financial professionals day. These briefing sessions are run by the leading lights in the industry to give you a hands-on update and helping hand with the latest changes, developments on key topics and what is coming over the horizon. These meetings are usually only two or three hours in length so that they minimise the impact on member's busy working days.

**Regulatory Roundups**

Ok, so we are all aware of the increasing regulatory appetite of our regulators. In 2017 alone we have had the Criminal Finances Bill and the new UK Money Laundering Regulations. With the ink still drying on AMLD4 we are already anticipating AMLD5. In 2018 we have MiFID II and GDPR coming into force. But what do these regulations all mean? How do you keep up with what is now in force and keep your eye on what is coming over the hill ?

Many questions abound with such a changing landscape and our Regulatory Roundups are designed to address the most pressing questions we all share such as:

- What is the real impact of each regulation to YOUR day to day function?
- If there is more than one way of interpreting the regulation, how is the regulator likely to decide to deal with things?
- How are other companies balancing the requirements with business demand for reduced red-tape and lower budgets?

At our Regulatory Roundup's, our members will get specific practitioner guidance and opinions from leading SME's on how the regulatory change is likely to impact our industry.

Places for all of these sessions will be restricted to members of MLROs.com so no recruiters or salesmen! All our events run under the Chatham house rule. Therefore we encourage everyone to speak openly knowing it will never be attributed to you or your organisation.

The Regulatory Roundup Programme is Kindly Lead for MLROs.com by Emma Radmore

**Summit Conferences**

There are times when an issue is both pressing and important enough that it cannot be adequately covered in a single session at a conference!

To give these issues proper coverage MLROs.com will be running half and full day Summits on these key areas.

Ensuring adequate time and the specific specialised expertise, from all of the relevant experts and key players; in one place.

In a safe and conducive setting to be able to deal with the issue at hand in depth and breadth.

**Summit Dinners**

MLROs.com Summit Dinners are exclusive, small, invitation only events; where invited members will be able to interact with key technical SMEs from the top of the community to gain real in depth knowledge on a specific topic in a group session.

The group session is followed by a sit down high quality dinner with each table having one or more of the SMEs on it to allow the conversation and knowledge to flow and for the members to network and build deeper relationships with each other and the SMEs.

**MLROs.com ROASTS!**

At MLROs.com we believe that knowledge and networking don't have to be boring dull dry experiences. Different people learn and interact in different ways.

ROASTS are informal irreverent evening sessions with buffet food and a few drinks (or sometimes more than a few drink's) on specific topics of interest to the community, where members get to listen to and interrogate a small panel of experts whilst standing with a drink in one hand and food in the other.

Our pilot events were very well received and members found them to be loads of fun, very informative and a fantastic networking opportunity.

# Compliance Matters - Special Offer to Conference Delegates!

MLROs.com is delighted to announce that we have managed to negotiate a special discount to Clearview publishing's flagship publication for GRC and compliance professionals "Compliance Matters"

There is a 50% discount off the normal price of an annual subscription only available to delegates physically at this conference today.

To take up this fantastic offer, please see on of the Compliance Matters staff and they will sign you up for a 14 day free trial and give you eligibility for this offer.

# Current News on MLROs.com

As part of the enhancement of our online services, MLROs.com is delighted to announce the addition of a new news section to the MLROs.com website!

There will be both a public facing open section and a secure members only news portal. With special bulletins for it's members on the topics that matter to you.

Access to the members only news portal which is where the bulk of the content will be placed, is only available to registered members who have been through the re-registration process and have a new secure username and password!

So don't forget, re-register today and gain access to an ever-growing range of features, services and content → www.mlros.com/register

We are delighted to announce, that Chris Hamblin, Editor of Compliance Matters has agreed to help with editing the site and will be a contributing editor! Chris as many of you know is a much respected time served investigative journalist and editor with a significant reputation in financial crime journalism and we are very lucky to have his personal help and support in this endeavour.

**We are always looking for new and unique content; if you have something to contribute, please get in touch, we would love to hear from you!**

# MLROs.com Advisory Board

As the fastest growing members lead forum for AML and financial crime professionals MLROs.com has always striven to provide forward looking, relevant content driven, conferences, events and services. To ensure that everything we do accurately reflects the needs of our members and to provide a stable and long lasting environment of operational excellence we have decided that it is time for MLROs.com to take the next step and enhance our internal management structure to give us breadth and balance in content provision across the board.

We are therefore delighted to announce the formation of the MLROs.com Advisory Board!

The board will be chaired by Two Co – Chairpersons who will act as the new chairs of the MLROs.com forum. We envisage a board of between 15 and 20 members selected from significant SME volunteers within the industry. We are putting together a board that has representation in each important area of specialisation that affects the community.

The Board will oversee the development of the content of the MLROs.com forum - ensuring it is always independent, best in industry, relevant and disseminated in a timely manner to enhance and empower the membership we serve.

We want to strengthen the impact we have on the profession and the service we provide to our members by utilising our most valuable assets properly – our members!

We are looking for a representative mix of professionals to ensure that everything we do is unrivalled and makes a lasting contribution to our industry. If you have something to contribute, please make your interest known to our CEO, David Pelled, by calling him on his mobile +44 7956877806 or by email at david.pelled@mlros.com We look forward to hearing from you!

# MLROs.com Advisory Board

## Simon Airey

We welcome Simon as the chairman of the board. Simon recently joined Paul Hastings from his role as MLRO and one of the founding investigations department partners at DLA Piper; to head their new investigations department in London. Simon specialises in global investigations, financial and regulatory crime, bribery and corruption, money laundering, tax and fraud inquiries, dawn raids and corporate compliance. Mr. Airey has conducted a wide range of investigations in different sectors, principally construction, defence, financial services, gambling, oil and gas, logistics, pharmaceuticals, and telecommunications. He advises a large number of multinational groups in relation to their global Anti-Bribery & Corruption (ABC) compliance programmes and has lectured extensively in the U.S., Europe and Asia in relation to the UK Bribery Act and related matters. Mr. Airey started his career as a barrister in private practice during which time he gained experience of a broad range of regulatory, criminal, and civil litigation at all levels of the court system.

## Siân Jones

Siân heads COINsult, a regulatory compliance consultancy focused on digital currencies and consensus-based technologies. She advises fintech startups worldwide on regulatory, compliance and jurisdictional strategy, and helps governments and enterprises evaluate cryptocurrencies, blockchain and distributed ledgers.

Siân also heads EDCAB, the European Digital Currency and Blockchain Technology Forum, an independent Brussels-based public policy platform where she helps EU policymakers and legislators shape sound policy and regulation relating to virtual currencies and distributed ledger technology. In January 2016, she addressed the European Parliament's public hearing on virtual currencies and, later, organised a series of roundtables bringing global and financial institutions, academics, lawyers and industry stakeholders together with EU legislators and representatives from the European Commission and institutions.

Siân is a founder member of the UK Digital Currency Association and co-led its Regulation and Banking Group from 2014 to 2016. She contributes regularly to leading blockchain podcast, EpicenterBitcoin, and frequently speaks and sits on panels at conferences. Siân is an Ambassador for the Emerging Payments Association and also works with Credits, the first and only blockchain platform provider awarded a UK Government G-Cloud framework agreement.

## Andrew McDonald

Andrew retired in January 2017 as Head of Specialist Investigations and National Terrorist Financial Investigation Unit (NTFIU) at SO15 Counter Terrorism Command at New Scotland Yard. He had strategic and tactical oversight for all financial and crime disruption investigations to identify, arrest and charge or disrupt terrorist offenders and their associates. He served over 30 years within the Metropolitan Police Service; 20 years were with specialist covert and overt operations within a counter-terrorist and organised crime environment in New Scotland Yard detective teams.

In a previous role as Head of Metropolitan Police Fraud Squad, Andrew was responsible for designing the current operating model for fraud and cyber-crime and assisted in its implementation.

In January 2017, Andrew was appointed as the Compliance Officer for the Independent Parliamentary Standards Authority; a role that he undertakes on a part-time basis.

In addition to his policing career, Andrew has delivered bespoke training and consultancy as a subject matter expert or specialist advisor to individuals from many law enforcement and commercial organisations within the UK and overseas. He specialises in deliveries to understand and manage illicit finance, compliance responsibilities for senior executives, crisis and risk management, decision-making and the management of intelligence.

He holds Batchelor of Science and Master of Business Administration degrees and is a fellow of the Chartered Institute of Management.

## Wendy Langridge

Wendy Langridge is the Head of Compliance and Corporate Governance at BCS Global Markets where she has been involved in the development and management of UK and international compliance activities since 2012. Wendy has over 20 years compliance experience working in exchange, trading platforms, investment banking and fund environments. Wendy's product knowledge extends to high and low latency trading products, capital markets, corporate banking, treasury and research functions and she has assisted a number firms obtain regulatory approval. Prior to BCS, Wendy held Head of Compliance and Senior Compliance roles at Commerzbank, Steubing AG and WMG Advisors LLP as well as working for both Market Supervision and Investigations at the London Stock Exchange. Wendy has degrees in business and linguistics having studied at universities in both the UK and Germany.

## Andrew Fleming

Global AML Risk Framework Manager at HSBC Global Banking and Markets

Andrew Fleming was a Detective Inspector with the Metropolitan Police for thirty years and has been involved in the investigation of financial crime for over twenty years including fraud, AML and sanction breaches, as well as bribery and corruption cases involving Presidents and government ministers. In his last posting at New Scotland Yard he ran the Cross Border Financial Investigation Team at SCD6 where he investigated cross-border financial crime involving organised crime networks, including terrorist organisations and financial institutions on behalf of foreign governments under the Crime (international co-operation) Act 2003. In this role he was involved in multi-million pound financial investigations with law enforcement organisations and regulatory authorities around the world, which were principally centred on AML, sanctions, fraud, bribery and corruption.
At Westminster he set up and ran the Economic and Complex Crime Unit, which specialised in investigating high risk financial crimes involving high profile organisations and individuals. In this role he conducted reviews of company's governance and control functions and designed structures and systems to design out internal fraud and other financial crime vulnerabilities such as AML, bribery and corruption.
Since leaving the police he has worked for a number of companies, including HSBC, the Co-op bank and Tori Global conducting AML and sanction assurance reviews, which included reviews of their KYC, CDD and transaction monitoring departments to ensure that their policies, procedures and processes met regulatory requirements. He also provided lectures and training to government agencies and financial institutions on financial crime, cybercrime, risk management and New Payments Products and Services, highlighting vulnerabilities and methods used to detect and prosecute external and internal offenders.
Andrew is passionate about financial crime and ensuring that his clients receive up to date information of current financial crime trends to ensure that they are protected from both financial sanction and financial predation.

## Peter Wilson

Peter is the current MLRO at Capital Index, the international CFD and Financial Spread Betting specialists. His experience, in another important sector to our members, will only strengthen the ability of the board to provide the best advice helping us curate the best events possible. Peter with his usual humility feels he is best placed to represent the rank and file membership who are under the same day to day pressures he faces in his work environment.

## Jonathan Williams

Jonathan Williams is an independent consultant in payments, identity and fraud prevention working for advisory firm Mk2 Consulting. Jonathan also brings experience in cybersecurity, telecommunications and software to his clients. Areas of special interest are PSD2, Identity Assurance, financial crime and ACH fraud.

Jonathan joined Mk2 from a role as head of Strategy and Product for Payments at Experian. Prior to this he was responsible for the product propositions which took two start-ups to IPO and one to acquisition: Content Technologies, Virata Corporation and Eiger Systems. He has also held engineering and IT roles at British Aerospace (now BAE Systems), the University of Cambridge and Advanced Telecommunications Modules Ltd

Jonathan speaks at many conferences worldwide and has recently addressed audiences for the Association of Corporate Treasurers, the Federal Reserve's conference on payments and EuroFinance. He also writes for trade journals including The Treasurer and Future Finance. Jonathan holds an MA in Theoretical Physics and a postgraduate qualification in Computer Science from the University of Cambridge and is a member of the Payment Strategy Forum's Financial Crime, Data and Security working group and the Open Forum on Open Banking.

## Helena Fearon

Helena is the Director of Risk and Compliance for Auto Trader and will give the board another alternate viewpoint into the world of compliance. Her fantastic experience is mostly in a field that will benefit a lot of our members.

## David Nordell

David is an expert on the confluence of technology, financial and economic crime, cybersecurity and international security. He is one of the leaders of the Centre for Strategic Cyberspace and Security Science, an international cyber think tank, and also a contributing editor of the Terror Finance Blog, one of the leading sources of expert analysis on terror financing and sanctions.

## Peter Haines

Global Head of GRC Training, CCL Academy

Peter Haines is a chartered accountant who has specialised in Regulation and Compliance since 1986. He has worked for European, Japanese and American financial institutions in senior Compliance roles, as well as for one of the UK regulators in a senior policy role. From 1997 to 2003, Peter was Chairman of the Securities Houses Compliance Officers' Group (SHCOG), the most prestigious Compliance Officers' group in Europe for the wholesale markets.

In June 2006, Peter set up Peter Haines Compliance Consultancy Limited and has been involved in numerous Compliance training and consultancy initiatives, as well as assisting clients with projects relating to conflicts of interest, governance, AML and regulatory visit preparation. Peter has partnered with institutions such as SHCOG, the ICMA Centre and Henley Business School at the University of Reading in delivering training programmes to senior management, compliance officers and client and market-facing financial services employees. Peter has also been involved in four s.166 reports for the UK regulator and in expert witness work. He has sat on a number of senior level committees and boards during the past twenty years, is a regular speaker at industry conferences and has articles published periodically on issues relating to regulation, compliance and governance. Since August 2011, Peter has served as a non-executive director of Ghana International Bank and is Chairman of its Audit, Risk and Compliance Committee. He is also a Visiting Fellow at the University of Reading and Henley Business School. Peter is co-author of "Essential Strategies for Financial Services Compliance", published by Wiley in 2015.

In January 2017, Peter became Global Head of GRC Training for CCL Academy, joining a team of experienced trainers committed to providing world class training in Europe and the Middle East.

# Interact with MLROs.com via Social Media

Don't forget that you can follow and interact with us via the following social media channels:

| | | |
|---|---|---|
|  | LinkedIn Group: MLROs.com Community | https://www.linkedin.com/groups/8590282 |
|  | LinkedIn (Company Page) | https://www.linkedin.com/company/5222499 |
|  | Twitter | http://www.twitter.com/MlrosCom |
|  | Facebook | https://www.facebook.com/mlroserviceslimited/ |

Our goal is to facilitate and provide the global Financial Crime community with impartial, practical content and analysis on the latest issues in the area of Financial Crime. Our members include representatives from a wide range of financial institutions, regulatory bodies, law enforcement agencies and industry sectors.

Membership to MLROs.com is free, if you have not already registered with us then please register here: http://www.mlros.com/register/

# Announcing MLROs.com Community on LinkedIn

In order to allow our community to share important stories, papers, reports, and intelligence we invite you to join our brand new LinkedIn Group: "MLROs.com Community". Simply search for our group on LinkedIn and join us, or find us directly here: https://www.linkedin.com/groups/8590282

This group will be moderated with a zero tolerance policy for sales pitches and "noise". We encourage you to use the group to as a convenient place to collaborate, share information or start discussions. We hope you will find this to be a useful addition to our presence on social media.

# Upcoming Events

The MLROs.com upcoming events schedule is a constantly evolving and growing entity in its own right.

We are currently trying to schedule events further ahead as a standard procedure to allow members to have better control of their diaries and ensure that they can maximise their involvement opportunities and reduce costs by using the early bird discount ticket system.

The next two events in 2017 are :-

**MLROs.com Conference One 2017 NORTH** – 11th October at the offices of Squire Patten Boggs in Birmingham.

This is the inaugural conference for MLROs.com outside of London, and we are expecting a high turnout as we are already taking ticket sales even though we have yet to finalise the agenda.

I can confirm, we have a great speaker line-up including Mark Rainsford QC as our keynote speaker.

It will be a busy few days for us at MLROs.com central as early the next morning we have our inaugural **Regulatory Roundup** meeting chaired by Emma Radmore at the offices of bond Dickinson in London on the 12th October.

This free to attend members briefing event has been sold out for quite some time. We will be announcing the date and venue for the next in the quarterly series shortly, and you can of course keep up to date via the members Regulatory Roundup section of the website. Remember, this like most of the content, is on the secure side of the site and requires you to have re-registered for free to obtain your username and password.

**Conference One 2018** will be hosted by Paul Hastings in London probably on the third or fourth Wednesday in January, dates are being finalised at the moment and will be announced shortly.

**Conference Two 2018** will be hosted by Squire Patten Boggs in London again probably third or fourth Wednesday in April, dates are being finalised at the moment and will be announced shortly.

In General we will be running the following full day conference schedule each year:

- Three or four MLROs.com full day conferences in London every year.
- Two or Three MLROs.com full day conferences in Midlands and the North every year.
- One MLROs.com full day conference in Scotland every year.

We will also be running a compliment of free to attend practitioner only briefing sessions in each area to compliment the conference schedule.

# PSD 2 Glossary

*As there are at least two sessions that deal heavily with payments and PSD 2 issues we thought it would be useful to provide delegates with a glossary of commonly used terms and concepts.*

*This material has kindly been donated by FICO*

# PSD2 Glossary

Payment Services Directive 2, or PSD2 as its better known, involves a lot of acronyms and new terminology. These terms can be both difficult to understand and easy to forget! To help you keep all the terms and their definitions to hand we've created this handy PSD2glossary.

| Term | Definition |
|---|---|
| AISP -Account Information Service Provider | An authorised entity that provides aggregation services related to payment accounts such as bank accounts. PSD2 allows AISPs authorised access to bank account data through an API. An example of a service an AISP could provide is personal financial management: a single platform where an account holder can login to view and manage multiple bank accounts from multiple providers. AISP's can be existing banking providers or third parties. |
| API- Application Programming Interface | A set of defined methods of communication between programmes so that information can be exchanged without a need to access the core of either programme. Under PSD2 APIs will define how third party providers (AISPs and PISPs) access customers' payment account information and initiate payments on their behalf. |
| ASPSP- Account Servicing Payment Service Provider | A Payment Service Provider (PSP) such as a bank or card issuer that provides authorised access to bank account information. For PSD2 they are allowing API access to bank account data for AISPs and PISPs. |
| Brexit (PSD2 context) | Brexit is the process by which the United Kingdom plans to end its current membership of the European Union. In the context of PSD2 Brexit is unlikely to have an effect on the implementation of the legislation in the UK. |
| CMA -Competition Markets Authority | The Competition Markets Authority is a UK body, they have been working to increase competition in UK banking; this has lead them to push for reforms in retail banking that are in line with PSD2. |
| CNP - Card Not Present | Sometimes referred to as cardholder not present, this refers to a transaction where the payer, payee and the method of payment (the card) are not in the same location, when the transaction takes place. Tackling fraud in the CNP process is a main objective of PSD2. |

| | |
|---|---|
| Competent Authorities (PSD2 Context) | A competent authority is any person or organization that has the legally delegated or invested authority, capacity, or power to perform a designated function. For PSD2 the competent authority in each EU member state will have primary responsibility for monitoring compliance and enforcement of PSD2. In the UK the competent authority for PSD2 is the Financial Conduct Authority (FCA). |
| EBA - Euro Banking Association | Not to be confused with the European Banking Authority, the Euro Banking Association is an industry forum for the European payments industry. Their role in PSD2 is to promote the interests of their members and help them to adapt to PSD2 in addition to sponsoring the Open Forum on Open Banking. Also known as ABE. |
| EBA - European Banking Authority | Not to be confused with the Euro Banking Association, the European Banking Authority is an independent EU body which works to ensure effective and consistent prudential regulation and supervision across the European banking sector. For PSD2 they have responsibility for developing the Regulatory Technical Standards and guidelines. |
| e-IDAS | A framework that provides a set of standards for electronic identification and trust services for electronic transactions in the European Single Market. For PSD2, the e-IDAS framework informs the developing standards for Strong Customer Authentication for remote payments. |
| European Commission (PSD2 context) | An institution of the European union, it is responsible for proposing legislation, implementing decisions and upholding EU treaties. In the context of PSD2 it is the force behind the proposition and adoption of the directive at a European wide level. In each country this responsibility will be managed in conjunction with the local governments and appointed Competent Authorities for example in the UK the FCA. |
| European Payments Council | Is a membership organisation created in 2002 by the major European banks. The main task of the EPC is the development of the Single Euro Payment Area. (SEPA) a key initiative of PSD1. They represent their members' interests in the development of PSD2, for example by preparing responses to the developing Regulatory Technical Standards. |
| EEA – European Economic Area (PSD2 context) | The European Economic Area (EEA) unites the EU member states and the three EFTA States (Iceland, Liechtenstein and Norway) 28 countries are members. PSD2 is in force for payments within the EEA, from the EEA to outside countries and from outside countries into the EEA, in all currencies. Where one of the PSPs is situated outsied the EEA these are known as One Leg Payment Transactions. |
| Exemptions (PSD2 context) | For PSD2 Exemptions are most widely talked about in the context of exemptions from using Strong Customer Authentication, for example for parking or ticketing payments or for payments where the threshold is met based on Reference Fraud Rates for the payment value; these permissible exemptions are detailed in the Regulatory Technical Standards. |
| Exemption Threshold Value | Related to the application of exemptions from Strong Customer Authentication ETV defines the payment value at which the Reference Fraud Rates must be adhered to, in order to secure a payment using Transaction Risk Analysis. |

| | |
|---|---|
| FCA -Financial Conduct Authority | The FCA is the UK regulatory body responsible for the adherence of regulated financial institutions to applicable legislation. They are the Competent Authority for PSD2 in the UK and will have primary responsibility for authorising service providers and monitoring compliance and enforcement ofPSD2. |
| Inherence (PSD2 context) | Along with Knowledge and Possession, Inherence is one of the factors required for Strong Customer Authentication for PSD2. Inherence refers to providing authentication via something you are, a biometric check is an example of inherence. |
| Instant Payments | A European initiative to process payments within 10 seconds between European accounts in euro and supported by the Euro Banking Association. In the context of PSD2, this will further facilitate the use of bank accounts for retail payments through Payment Initiation Services (PIS). |
| Interchange fees | Interchange is the fee paid by the retailer's merchant acquirer to the card issuer each time a card payment transaction occurs. Historically, the relative expense of fees for lower value transactions has led to merchants making surcharges to offset the cost to them of payments by debit or credit cards. PSD2 will severely limit surcharging on such transactions. |
| ISO 20022 | This is an international messaging standard for electronic data interchange between financial institutions. It is expected that ISO20022 will be the standard deployed to enable the use of the API's between the ASPSPs and the PISPs and AISPs. |
| Knowledge (PSD2 context) | Along with Possession and Inherence, Knowledge is one of the factors required for Strong Customer Authentication for PSD2. Knowledge for PSD2 refers to something an account holder knows that can be verified, for example a password or answer to a secret question. |
| KYC -Know Your Customer | In the context of PSD2 Know Your Customer refers to the authentication needed to secure payments. This is managed either through Strong Customer Authentication or Transaction Risk Analysis. Further requirements are documented in the Fourth Money Laundering Directive. |
| Merchant | A Merchant is an entity suppling either goods or services generally in return for payment, typically via payment cards. PSD2 is concerned with securing the payments from customers to merchants through the customers Payment Service Provider. |
| Merchant Acquirer | Merchant Acquirers enable Merchants to accept and process payments from card schemes and as such they are Payment Service Providers as defined by PSD2. |
| MIDAS Alliance | Membership organisation which defines and promotes of standards for digital identification and authentication of individuals and organisations to enable them to trust each other's digital identity, and to manage it in a secure manner. FICO is a participating member. MIDAS Alliance is engaged in developing the PAS 499 standard with the British Standards Institute with the intention of it becoming the standard used for PSD2 for Strong Customer Authentication. |

| | |
|---|---|
| Open Banking | Refers to the opening up of banking systems to third parties to allow them to provide services directly to their joint customers. Open Banking is one of the main drivers of PSD2 (and other global open banking initiatives) the objective is to improve consumer choice and increase competition in the banking sector. Open banking will be achieved through the development of APIs. Also known as Access to Accounts (XS2A). |
| PAS 499 | Managed by the British Standards Institute PAS 499 is a planned UK code of conduct for enhanced identity and authentication online. It is being developed by the MIDAS alliance, an industry body in which FICO participates. The aim is to provide an acknowledged identity verification standard that can be referred to when implementing legislation including PSD2. |
| Payment card surcharges | This is a practice where merchants look to offset costs associated with processing credit and debit card payments by making an additional charge to their customers. PSD2 will prohibit most surcharges. |
| Payment Initiation Service | An electronic service facilitating payment by a third party from a customer's payment account via APIs or Open Banking. |
| Payment Institution | The concept of a Payment Institution was created by the enactment of the first Payment Services Directive. They can offer customers a range of payment related services that are defined in the directive. Payment Institutions are regulated but not to the same degree as PSPs as there are limits on the services they can offer. |
| PISP - Payment Initiation Service Providers | A regulated entity which allows customers to initiate payments without the customer needing to directly access their bank account or use a debit or credit card. PSD2 allows authorised PISPs authorised access to bank accounts through an API. Payment Initiation Services can be provided by existing retail banks, payment service providers or by third parties. |
| Possession (PSD2 context) | Along with Knowledge and Inherence, possession is one of the factors required for Strong Customer Authentication for PSD2. Possession for PSD2 relates to securing payments through the possession of a verifiable item such as a token, bank card or device, for example a smartphone. |
| PSD2 - Payment Services Directive 2 | The second Payment Services Directive is an EU Directive that aims to regulate payment services and payment service providers throughout the European Union and European Economic Area. PSD2 updates and replaces the Payment Services Directive 2008. Two of the key aims of PSD2 are to reduce payments fraud and to deliver open banking to increase competition. PSD2 builds on PSD1 which delivered standardisation to payments through SEPA. |
| PSP - Payment Service Provider | In the context of PSD2 a Payment Service Provider relates to the entities that provide payment services through issuing credit or debit cards or offering payment mechanisms through accounts e.g. direct debit, direct credit or Instant/Faster Payments. In a wider context Payment Service Providers also include the providers of payments gateways and platforms. |

| | |
|---|---|
| PSR-Payment Systems Regulator | The Payment Systems Regulator Limited is the UK economic regulator for the payments systems industry. In the context of PSD2 the PSR is responsible for the provision on access to payment systems (XS2A) the PSR is part of the FCA, the Competent Authority responsible for monitoring compliance and enforcement of PSD2 in the UK. |
| Reference Fraud Rates | These are the fraud rates laid out in the PSD2 Regulatory Technical Standard, based on the percentage of value of fraudulent transaction to total transaction values over the previous 90 days, the reference fraud rates, together with the transaction value determine when it is permissible to use Transactional Risk Analysis to secure payments instead of Strong Customer Authentication. |
| Remote Payments | Payments that are made when the payer and the payee are not in the same location, an online payment or payment over the telephone are examples of remote payments. PSD2 is concerned with limiting fraud in remote payments. |
| RTS- Regulatory Technical Standard | The Regulatory Technical Standard provides the rules by which PSD2 will be implemented. The European Banking Authority is responsible for the development of the RTS to meet the objectives of PSD2 as defined by the European Commission. |
| SCA -Strong Customer Authentication | A methodology by which PSD2 looks to secure payments. Strong Customer Authentication aims to reduce payment fraud and is based on authenticating payment initiation using multiple factors that include inherence, possession and knowledge. |
| Screen scraping | A programmatic means of processing web content to extract data. In the context of PSD2 this was the pre-cursor to API access to accounts (XS2A) and relies on third parties holding some security credentials for their customers. Whether screen scraping is allowed by PSD2 in some specific cases is still under discussion. |
| Secure Execution Environments | Refers to a hardware element, such as a SIM Card, on a mobile device that is secure and can therefore be used to store sensitive data such as financial data and passwords. For PSD2 Secure Execution Environments are referenced in terms of providing independent environments to manage multiple factors for authentication separately even if on the same device. |
| SEPA - Single Euro Payments Area | Supported by PSD1 ad launching in 2008, SEPA is a payment integration initiative of the European Union to ensure the same terms regardless of where the payment starts and ends. It established common payment mechanisms such as SEPA Credit Transfer and SEPA Direct Debit which operate across EU borders. It also used/ implemented common ISO 20022 XML messaging standards for bank account information and the mandatory use of the IBAN (International Bank Account Number). |
| TPP - Third Party Providers | Provide services which are based on access to payment accounts provided by a PSP who is not the 'account servicing' PSP (ASPSP), in the form of payment initiation services and / or account information services. AISPs and PISPs are examples of TPPs for PSD2. |

| | |
|---|---|
| TRA -Transaction Risk Analysis | A methodology by which fraud is spotted due to behaviour observed in the transaction or by the counterparties to the transaction. Transaction Risk Analysis software relies on a number of underlying technologies including analytical models and Machine Learning. In PSD2 exemptions are made that means that those with low fraud rates can avoid using burdensome Strong Customer Authentication for payments using Transaction Risk Analysis. This is desirable as TRA will reduce friction for consumers and may be delivered at lower cost than SCA. |
| Transposition (PSD2 Context) | Transposition is the process by which the EU Directive becomes national law in each member state. Once transposition is complete then adherence to the law is mandatory. Currently Transposition to PSD2 is to be complete by January 2018 at the latest. Further requirements, such as Regulatory Technical Standards will have different deadlines after this date. |
| TMM -Transaction Monitoring Mechanisms | The RTS on Strong Customer Authentication states that Payment Service Providers must undertake transaction monitoring using a number of mechanisms including typical fraud patterns, identification of malware and location of Payment Service User and Payment Service Provider. |
| TRM -Transaction Risk Monitoring | Uses Transaction Risk Analysis as a tool to monitor and report fraud. Under PSD2 PSPs must provide a risk score based on detailed factors that are laid out in the Regulatory Technical Standard. Transaction Risk Monitoring can help them to deliver this. |
| XS2A - Access to Accounts | This is a term, coined before Open Banking, which refers to access to payment accounts by third parties acting on behalf of the Payment Service User. The basic requirements are set by the European Banking Authority which define how data from bank accounts is accessed for PSD2. It makes it mandatory for banks to set up access to bank account data via API, although there are multiple standards for APIs including those from the Berlin Group, due for consultation in Q4 2017 This will enable consumers to logon to their bank accounts on a third-party provider's platform without exposing their bank login data to them. |

# GDPR Checklist

*As we all know, there is not one simple standard solution to be GDPR compliant. GDPR compliance is a process and a journey that will be different for every organisation.*

*We hope that this useful checklist kindly supplied by Storm 7 Consulting helps supplement Adam Wiseman's informative session this morning.*


# GDPR Cyber Risk Checklist

Date: 8th September 2017

Prepared by: Neil Hare-Brown

# Distribution

| | Copy No. |
|---|---|
| STORM Guidance Ltd. | 1 |

# Approbation

| Approver | Position | Version | Date Approved | Notes |
|---|---|---|---|---|

# Copyright

# Introduction

The new General Data Protection Regulation (GDPR) will apply as UK law from 25th May 2018. There are many narratives as to how the regulation will be enforced and what organisations need to do to achieve and maintain compliance.

What makes GDPR different to the old Data Protection regime? There are many similarities and the UK Information Commissioners Office prefers to explain GDPR as an evolution; rather than a revolution, in law protecting the rights of data subjects. The enforcement regime though is significantly empowered and some recognise the GDPR as a major step in correcting the previous imbalance of rights of organisations to monetise personal data in favour of the rights data subjects as the originators and, some might say, the owners of their personal data.

Whatever the view, the mining of personal data is still seen by many in government or corporate executives as essential for business. Indeed, many organisations of all types and sizes would simply not exist if they could not process personal data. Ask yourself about this reliance in relation to your business and use the answer to encourage those whose responsibility it is to attribute value to business assets and who should assign a suitable budget in support of your actions towards achieving compliance with GDPR.

This document is a simple set of actions which should help organisations of all sizes achieve compliance with GDPR. It is not a panacea for compliance and there may well be other actions needed. However, this checklist style should assist it taking some of the complication out of the challenge. It should be noted that the key actions presented here are in no inferred order of importance.

Whilst there will be costs associated with some of the actions, the broad approach is one that does not infer high costs. We recommend careful assessment in the need for consultancy and technology solutions, as often these will not be needed. However, ownership of the GDPR compliance activities must be assigned. This must be at board level otherwise it is at extreme risk of failure.

The overwhelmingly positive result of these actions should be in the realisation of digital asset value which your organisation can achieve. Many companies are currently ignorant of the Personally Identifiable Information (PII) which they exchange, store and process. In my role as a risk advisor and Digital Investigator, I find very few organisations that have a clear view of the PII in their possession.

These 'silent assets' have associated risk in both directions; downside in that misuse of the PII may result in harm to data both data subjects and organisations alike and upside in more efficient, optimised use of PII and the reputational benefits flowing from responsible use.

# Measure-Manage-Manifest

You can't manage what you don't measure is an old adage that is still accurate today. Most organisations simply do not know what PII they exchange, store and process and so there is first a need to measure this by determining the types, forms, amount and storage/processing locations of PII. It will also be necessary to identify responsibility for controlling and processing the data.

Secondly there are the steps needed to efficiently manage the PII whilst the organisation is responsible for it.

Thirdly, there is a need to prove, through a manifest, that measurement and management processes are suitable and effective. This last step is vital when it comes to a reduction in risk for the organisation should a potential breach of PII occur as regulatory bodies will attribute a good deal of credence; and preferential consideration in enforcement actions, if your organisation can show evidence of responsible practice in the management of PII.

## *Discovering PII*

Discovering all sources of PII within your organisation is often not trivial. The best way to categorise PII is to align it to a 'purpose'. This is in keeping with data protection legislation incl. GDPR. Remember that you need to be able to align your purpose for each use of PII with specific legitimate need and this will be particularly important should regulators like the ICO ask you for such clarification so it is best to start as you mean to go on.

There are four key aspects of PII which should be recorded in an asset register. These are type, form, location and amount. It is vital that you document the methods you use to determine your results in these four areas as this documentation should become the benchmark by which your organisation continues to assess its use of PII.

Each entry line in your PII asset register should also record the purposes for each use of the PII.

### Types of PII

The generic definition of PII is not sufficient to be able to demonstrate compliance with the GDPR and other legal and regulatory obligations. You need a more granular assignment in PII sub-types as follows:

**SPI** – Sensitive Personal Information
**PFI** – Personal Financial Information
**PHI** – Personal Health Information (sometimes also called Protected Health Information)

All other personal information can be categorised as General Personal Information (**GPI**).

### Forms of PII

The generic definition of PII data is by record. Records are relatively simple to quantify if the PII is stored within a database or spreadsheet.

However, a record is just one digital format. Other common formats include documents e.g. typical office formats for word processing. Additional formats containing PII include images and emails. Many of these formats are harder to reconcile to a 'per record' model (see Grouping and Quantifying PII below).

Don't forget that PII which are stored/processed from structured physical files i.e. printed or written, is also a valid format.

### Locating PII

PII can be located both physically and logically. The pervasive nature of PII in business usually means that it is spread across many systems and stored and processed in many locations. This is especially the case with the increasing take up of cloud services.

It is important that you learn and record where the PII is located so that this information can help when you quantify the amount of PII for any given purpose and to quickly assimilate potential impact should an incident occur which may affect the confidentiality, integrity or availability of the PII.

## Grouping and Quantifying PII

### Creating and maintaining your Purposes for processing PII

In order to simplify your PII Asset Register you need to record your legitimate business purposes for processing PII. I would recommend using a simple dept./letter/number system which you can further refine with a text description. An example would be:

***FIN/S1*** *- This data will be used for administrative purposes so that the Finance department can manage its suppliers effectively.*

You can scale this method dependent on the type and size of your organisation. Remember, the aim is only to broadly categorise your PII assets but if you can do so with a suitable level of granularity this will really help the Management and the Manifest steps.

### Assigning a PII Type

The process of assigning a type is often a challenge for organisations. Unfortunately, this is often because the business wants to play down the sensitivity of certain PII so that it can justify the implementation of less secure technologies and processes. Whilst this has never been an approach endorsed by the ICO and security professionals, such a practice becomes significantly higher risk under GDPR because it exposes the data controller/processer to charges of negligence and the potential for heavy fines should this be proven. It is therefore very important to assign PII types carefully and to keep a record of such determination.

When looking at an instance of PII; either a record or within a document etc., ask yourself the question in the following order:

1. Does the PII contain any medical data pertaining to a person (by at least their name)? If yes, it has the **PHI** type designation as a minimum.
2. Does the PII contain any financial identification data pertaining to a person? This includes bank account number, credit card number. If yes, it has at least the **PFI** type designation.
3. Does the PII contain any data pertaining to a persons' ethnicity, racial or religious status? If yes, it has at least the **SPI** type designation.
4. If none of the above are assigned yet the PII still contains information such as physical address, email address, telephone number pertaining to a person then it should be assigned to the **GPI** designation.

**Note**: an instance of PII may be designated with PHI, PFI and SPI – a highly sensitive record. Additionally, you may have an instance of PII which is clearly only PHI or PFI or SPI. In these cases, it is not necessary to also designate the PII as GPI i.e. the GPI type is a catch-all designation.

### Aggregating PII - Creating PII 'Counts'.

As mentioned earlier, it is relatively easy to count records in a database or spreadsheet; of course, taking relational and duplication into account. However, it is not so easy for other forms of PII e.g. documents. My solution is to aggregate PII in 'counts'. Examples:

*A spreadsheet with 17,000 client records; de-duped results in 12,000 unique client names, addresses etc. PII Count = 12,000*

*A folder system with 8,000 case data subfolders each containing a number of documents referring to a client case. Each case containing client PII; de-duped results in 2,700 client PII details AND PII related to other parties in each case in the order of an average 2 parties per case (de-duped).*
*PII Count = 2,700 + 16,000 = 18,700*

*A folder used for KYC ID verification pertaining to 4,300 customers and including image scans of passports, driving licenses and utility bills. Each ID verification at least 3 document scans*
*PII Count = 4,300 x 3 = 12,900*

*A payment transactions database recording PII in the form of name, address and payment details containing 278,000 transactions. De-duped results 178,000 records.*
*PII Count = 178,000*

## De-duplicating and Aggregating under each Purpose

Removing duplicates of PII instances to obtain an accurate count where each instance relates to a single individual is often the hardest task of all and can lead to the most expense. However, there are a range of tools available to help with such an exercise and many are low cost or even free. Of course, there are still the costs associated with the time the de-duping exercise takes.

My advice is not to get too obsessed with precision but to focus on accuracy. If the methods you use are are 5% or even 10% out then it may not matter in the original assessment.

What is important is that the method you do use can be further refined with little additional effort; for instance, should you need to be more accurate if a breach were to occur. This ability to extend a process, as and when needed, is critical as the GDPR only gives a very short time window for organisations to determine PII records affected by a breach before mandatory notification and you would not want this number to be either over or understated.

Remember to include PII contained in structured physical formats in your PII aggregation counts. Also remember to factor an understanding of your data backups into your overall determination of aggregate PII counts.

A count of PII may contain any combination of any type – all types should be recorded e.g. a personal health record may incorporate data on medical history (PHI), details of ethnicity (SPI), financial details (PFI) as well as patients name and address (GPI) but still be only a single record.

However, depending on form and location of PII data sources, it may make sense to de-duplicate discrete collections before determining an aggregate count under a single purpose.

Ensure that the methods used are documented as your organisation benchmark.

# The Checklist

| Measure | | |
|---|---|---|
| **Ref.** | **Action** | **Done** |
| ME.1 | Identify all instances of PII that are exchanged, stored and processed by your organisation. Record the type, form and location and quantify the amount of PII in each distinct group in a PII Asset Register against given business purposes. | |
| ME.2 | Build flowcharts for each PII purpose within your organisation recording lifecycle of PII from receipt to secure destruction. | |
| ME.3 | Ensure that all methods used in the discovery, designation, de-duplication and aggregation to determine accurate PII counts are repeatable and documented. | |
| ME.4 | Create a process of Privacy Audits which will enable a more formal approach to the measurement of PII in your organisation going forward. | |
| ME.5 | Be confident that you can accurately answer key questions about the purposes, amounts, trends and expected developments in the use of PII within your organisation. | |
| | | |

| Manage | | |
|---|---|---|
| **Ref.** | **Action** | **Done** |
| MA.1 | Ensure that a single board member is responsible overall for compliance with the GDPR and that subordinate assignments are made to appropriately skilled specialists with a direct and independent reporting line to the board. | |
| MA.2 | Ensure that suitable security techniques are applied to protect PII at each location. Key techniques include strong, accountable access control and encryption. | |
| MA.3 | Use the process flowcharts to ensure PII is sourced reliably and responsibly. Ideally, the data subjects themselves should be responsible for the maintenance of PII relating to them. You may need to make system changes to accommodate this process. | |
| MA.4 | Ensure PII data retention processes are employed which securely destroy PII when the retention expiry date is reached. This may also apply to customer driven deletion of their PII. | |
| MA.5 | Ensure PII data backups are suitably segregated to enable optimal recovery time. Test the data restoration regularly and ensure that backups are encrypted and securely stored. | |
| MA.6 | Ensure secure collection of PII from customers and secure exchange of PII with all third parties. Regularly confirm third party assurance of security from data processors. | |
| MA.7 | Implement a monitoring system which records all access and changes made to PII in a tamper-proof and ideally centralised log management system. | |
| MA.8 | Undertake Privacy Audits on any new or significantly changed purposes (and supporting systems & processes) involved in the storage and processing of PII. | |
| MA.9 | Undertake an exercise to plan and test your response to a PII breach to ensure the forensic readiness and capability to determine PII affected and to fully satisfy notification requirements should an incident occur. | |
| MA.10 | Regularly review management techniques to ensure that all principles of GDPR are upheld and that your internal benchmarks are effective. | |

| | | |
|---|---|---|
| **Manifest** | | |
| **Ref.** | **Action** | **Done** |
| MF.1 | Ensure that each and every decision and action taken in the measurement and management of PII are recorded in a 'captain's log' of your PII management activities. | |
| MF.2 | Provide absolute clarity to data subjects on the purposes you use in processing and storing PII. Accept that GDPR swings the balance of ownership in their favour and so affords them due respect in trusting you to process their PII. | |
| MF.3 | Update your organisations board on a regular basis, helping them to clearly see the value of PII, how it is processed, stored and protected and how assurance is provided. | |
| MF.4 | Regularly update other stakeholders to demonstrate your organisations responsible handling of PII especially those with whom you transfer PII. | |
| | | |

# A special thank you to our sponsors, to all of our great speakers and you, our delegates!

**MLROs.com hope you have enjoyed a great day of fantastic content and networking opportunities!**

**Please share your thoughts with us via the email below.**

**We have an incredible line up planned for 2018 and we hope you can join us! Be sure to catch all of our great content and discounts first by heading over to [http://www.mlros.com](http://www.mlros.com)**

**Thanks again!**

**Conference Team**
**conferece@mlros.com**

GORDON DADDS