Financial Crime - the past, the present and the future
Tom Scampion, Partner, EMEA Financial Crime Leader
Agenda

<table>
<thead>
<tr>
<th>Topic</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where are we today? (20 mins)</td>
<td>3</td>
</tr>
<tr>
<td>The transformation journey (20 mins)</td>
<td>12</td>
</tr>
<tr>
<td>Looking ahead (20 mins)</td>
<td>20</td>
</tr>
</tbody>
</table>
Where are we today?
There has been a decade of enforcement actions across Europe

2009
Lloyds TSB given $217m fine for stripping SWIFT messages

2012
HSBC agree to pay $1.9bn U.S. fine in money-laundering case

2014
SCB fined $300m fine for deficiencies in Transaction Monitoring

2017
Deutsche Bank fined $630m over Russia money laundering claims

2018
Justice department inquiry into €200bn money laundering scandal at Danske
The global geo-political landscape remains troubled
Billions spent but not a lot to show for it

Illegal wildlife trade
Valued at $7 to $23 billion, illegal wildlife trafficking is among the largest and most lucrative criminal activities worldwide.

Human Trafficking
Human trafficking is thought to be one of the fastest-growing activities of transnational criminal organizations

North Korea
Tensions rise again as North Korea issues nuclear threat ahead of high-level talks with US

Financial Crime isn’t going anywhere – it needs to remain a key priority

Drugs Trade
Transnational crime remains a particularly serious problem in Latin America. Although a range of issues confront policymakers and decision makers, most are, in some way or another, connected with the drug trade.

Terrorism
Islamic State, formerly known as the Islamic State of Iraq and al-Sham (ISIS) has managed to position itself as the most significant threat to regional stability in the Middle East.
And financial crime issues continue to make headlines

We cannot fight cross-border money laundering with local tools

Crooks are exploiting the lack of transnational co-operation

HSBC brings in AI to help spot money laundering

Bank is latest to harness tech as a cheaper and better way of tackling crime

Rolling up the welcome mat

A crackdown on financial crime means global banks are de-risking

Charities and poor migrants are among the hardest hit

ING to pay €775m in money laundering case

Penalties are the largest ever imposed on a company by Dutch public prosecution service

Danske discloses criminal investigation by US prosecutors

Bank is co-operating with justice department inquiry into €200bn money laundering scandal

Britain, headquarters of fraud

The UK is at the centre of global corruption: shell companies that launder dirty money can be set up with ease.

Europol, UK banks’ Cyber Defence Alliance join forces

Washing whiter

Increasingly, hunting money-launderers is automated

The business of providing the software is booming

Awash

Britain’s war on dirty money lacks oomph

It is strong on transparency but weak on enforcement

Nordic banks in anti-money laundering tie-up

Five of region’s biggest banks join forces to develop know-your-customer infrastructure
New regulatory requirements continue apace

The 5th Money Laundering Directive must be implemented into national law by 10 January 2020

Then to be rapidly followed by the 6th Money Laundering Directive

Key Provisions of the 6th Money Laundering Directive

- A unified list of predicate crimes
- Extension of criminal liability to organisations
- Increased international co-operation for prosecution of money laundering
- Requirement for dual criminality
- Enhanced sanctions measures

Focus areas of the 5th Money Laundering Directive

- Customer Due Diligence
- Enhanced Due Diligence
- Beneficial Ownership Registers
- Information Sharing
- Obligated Entities
- Electronic Money
- Politically Exposed Persons

New regulatory requirements continue apace
And Financial Crime efforts are expensive

**Fines**
Since 2008, banks have paid US$321 billion in fines for regulatory failings

**Poorly configured systems**
>99% of FC alerts are typically false positives

**Resource hungry processes**
60% of effort investigating an FC case involves gathering the information

**Enforcements**
OFAC issued 16 civil penalties in 2017 to a total of $120M

**Intervention**
In 2016, 97% of global organisations reporting increased regulatory intervention

**Cost**
One global bank is spending $2bn p.a. on Financial Crime

Ineffective and inefficient processes and procedures lead to significant costs
Financial Crime maturity overview
Characteristics of leading institutions

Maturity evolution model

Key insights

Mature Function – Characteristics
- **Staffing**: Right number of people, balanced levels of seniority by location/region
- **Capabilities**: Invested in building own expertise across regions; low reliance on externals
- **Delineation**: Strong delineation between 1st and 2nd LoD activities
- **Synergies**: Strong focus on developing cross functional synergies with Risk/Compliance/Legal
- **Controls**: Functional processes/controls in place
- **Technology**: Cross-geographical, system-data-work-flow integration; reg-tech innovation enabled
- **Culture**: Pro-active and shared-accountability

Mature Function – Reasoning
- Many started investing in transformation of their FC function in 2010
- They completed the FC transformation in 2015-16 and they now focus on “next-gen.” value-add levers
- They have completed major parts of their DPA obligations; or they are not in a “DPA-status” any longer, which enables them to free-up capacities
# Financial Crime strategic priorities

Leading institutions are focusing their efforts on at least 10 strategic priorities

<table>
<thead>
<tr>
<th>1</th>
<th>Streamlining workflows with focus on <strong>AML investigations</strong>, alerts, etc.</th>
<th>![checkmark]</th>
<th>![checkmark]</th>
<th>![checkmark]</th>
<th>![checkmark]</th>
<th>![checkmark]</th>
<th>![checkmark]</th>
<th>p</th>
<th>![checkmark]</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Broadening and <strong>automating intel.</strong> capturing to improve client screening</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>3</td>
<td>Leveraging <strong>data analytics/tools</strong> to improve prioritisation of <strong>alerts</strong></td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>5</td>
<td>Improving <strong>triage</strong> effectiveness and efficiency</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>6</td>
<td>Establishing <strong>partnerships</strong> in the wider eco-system with Fin-/Reg-Tech.</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>7</td>
<td>Embedding a strong <strong>culture</strong> of ownership and pro-activeness</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>8</td>
<td>Moving roles to <strong>lower cost locations</strong> and altering seniority mix</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>9</td>
<td>Moving FC <strong>Ops out of FC sub-function</strong> allowing risk stewards to focus on advisory and oversight</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
<tr>
<td>10</td>
<td>Enhancing 1st/ 2nd line <strong>delineation in BAU</strong> empowering risk owners</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
<td>![checkmark]</td>
</tr>
</tbody>
</table>

* p - Partial focus
Live poll 1: Key financial crime risks
Please go to www.menti.com and enter code 57 56 84

Which of the threats below do you consider to be the most prevalent in today’s society? Please choose three.

i. Cyber and the dark web
ii. Terrorist financing
iii. Bribery and corruption
iv. Human trafficking
v. Illegal wildlife trade
vi. Tax evasion
vii. Russia
viii. North Korea
ix. Something else
The transformation journey
Enabling success
Transformation phases

**Stabilise**
Address known issues and regulatory findings to lay the foundations for strategic change. Largely reactive in nature

Example activities
- Conducting an Enterprise Wide Risk Assessment
- Establishing clear Programme governance
- Building an issues inventory and assigning to projects

Closing regulatory findings and internal audit issues e.g.

Laying the foundation for an effective and sustainable future e.g.
- Designing the strategic target state operating model
- Implementing common global processes e.g. KYC
- Moving to single or standardised systems e.g. a single KYC system

Improve the efficiency and effectiveness of existing capability e.g.
- Automating processes using “machine learning” and artificial intelligence i.e. e.g. discounting screening alerts
- Developing advanced analytics and intelligence capabilities

**Optimise**
Enhance existing capability through automation and intelligence-led processes

Following completion of TOM design

Following resolution of immediate priorities

Current status
Effective Sanctions Compliance transformation programs start with an in-depth and enterprise-wide risk assessment to evaluate the inherent risk facing the business, assesses the mitigating controls in place, and provide a view of the residual risk.

**Risk Assessment Spectrum of Activity**

- **Scope**
  - Define the scope and structure of business areas to assess, including business units, legal entities, divisions, countries and regions

- **Inherent Risk Assessment**
  - Select risk areas and factors for assessment
  - Determine the inherent risk present based on quantitative data analysis, other qualitative factors and analytical techniques

- **Controls Assessment**
  - Assess design and operating effectiveness of mitigating controls based on self-evaluation questionnaires that document evidence of controls

- **Residual Risk**
  - Highlight risk factors without sufficient mitigation and business areas posing the greatest risk
  - Evaluate results against institution’s risk statement

- **Action Plan and Reporting**
  - Develop action plan for underperforming controls based on identified gaps
  - Create reporting
  - Prepare documentation for audit/exam purposes
Addressing the issues identified from the EWRA provides a solid foundation for your compliance transformation.
Transform
Common implementation pitfalls and challenges

We have seen various implementation pitfalls and challenges faced by institutions, which can be classified into four key themes:

**Data**
- Poor historic quality of KYC
- Cost of remediation
- Information sharing challenges

**Talent and Resources**
- Lack of internal expertise / relevant experience
- Lack of resources

**Budgetary**
- Cost of transformation
- Implementing cost-effective BAU processes and operating models

**Collaboration Issues**
- FC <-> business collaboration
- Group / subsidiary governance
Optimise
Using technology to drive efficiency and compliance

Getting the basics right:
- Automation of manual processes, workflows and MI
- Consolidation of customer information
- Understanding and cleansing your data

Core systems: are they fit for purpose and “next generation”?
- Transaction monitoring
- Customer screening and alert management
- Customer onboarding

Using disruptive technologies to drive intelligence and efficiency:
- Robotics
- Big Data and Advanced Analytics
- Artificial Intelligence
- Distributed Ledger Technology

- Single view of customers across the organisation
- AI driven next-generation KYC and digital on boarding
- Robotic process automation to drive consistency and remove manual steps
- Consolidation of monitoring and screening solutions into strategic solution(s)
- AI used to drive efficiency and effectiveness in TM and Sanctions alert management
- Data enrichment
- Use of social network and behavioural analytics used to enable intelligence-led risk management.
Live poll 2: Key challenges to getting it right
Please go to www.menti.com and enter code 57 56 84

What do you consider to be the key challenges when implementing an effective anti-financial crime system?

i. Interpreting regulation (or conflicting regulation)

ii. Accessing investment

iii. Working with complex technology and organisational structures

iv. Sharing data and intelligence

v. Something else
Looking ahead
What does the future look like?
Financial Crime – Trends of Tomorrow
Trends that are likely to affect future requirements

Future Banking Environment

Changing customer expectations
- Demand for easy and fast access to services, across digital channels
- Greater transparency & data control
- Tailored services & greater choice
- Real-time banking/ payment channels

Regulatory environment
- EU Money Laundering Directives
- Criminal Finance Act
- Payment Services Directive 2
- CMA findings & Project Bulldog
- Open Banking APIs
- FCA Project Innovate & Innovation Hub

Emerging technology
- FinTech & RegTech
- Artificial intelligence (AI)
- Distributed ledger technology (DLT)
- Robotic process automation (RPA)
- Advanced/ predictive analytics
- Biometrics
- Cloud computing
Characteristics of the future

These trends are driving fundamental changes in how financial crime risk is managed in the short term and in the medium to long term.

**Financial crime risk management tomorrow**
- Cost focused
- Automated
- Regulation driven
- Managed Services/Utilities
- Analytics led
- Improved controls for current infrastructure

**Financial crime risk management in the future**
- Customer centric
- Collaborative
- Risk driven
- Eco-systems plays
- Intelligence led
- New controls for new infrastructure

These trends are driving fundamental changes in how financial crime risk is managed in the short term and in the medium to long term.
Evolution of role of technology in Financial Crime
Technology has great potential to improve efficiency and effectiveness.

The potential impact of technology on Compliance continues to grow.

- **2017**
  - Automation of high volume processes
  - Limited use of market utilities
  - Artificial Intelligence use-cases explored

- **2018**
  - Further automation of onboarding processes
  - Adoption of client self-service and digital interaction
  - Further expansion of AI
  - Optimisation of client file quality

- **2019**
  - Process highly automated
  - Mature Full-service KYC industry utilities
  - Digital identity based on distributed ledger technology
  - Advanced analytics leveraged

- **2020+**
  - Digital identity profile at the forefront of client interactions
  - Multi-factor biometric authentication
  - Intelligent insights derived through Artificial Intelligence and Advanced Analytics
  - Trigger event driven review replaces periodic reviews/refresh
  - Machine Learning unlocks enhanced ongoing risk management capabilities
Robotics and Cognitive in the FC lifecycle
Selected example use cases

- **Alert Risk Scoring**: Leverage historical alert and case information to more effectively triage alerts for investigation.
- **Alert Review Preprocessing**: Collection and aggregation of information for investigation purposes.
- **Enhanced Alert Triage, Stratification and Smart Case Routing**: Leverage disposition data for stratification, smart routing, specialized procedures.
- **Automated Narrative Drafts**: Automate drafting of initial case investigation summary narratives.
- **Check Image Recognition**: Extract check data from images for filtering and review.
- **SAR Form Packaging**: Automate population of SAR form and supporting material for review.
- **Anomaly Detection / Investigator Guidance**: Leverage cognitive to support and augment investigator judgement with anomaly detection.
Collaboration
JMLIT – A case study

September 2017 JMLIT paper ‘Sharing intelligence to tackle financial crime (v1.3)’

1. Developing the response template
   Based on input from the NCA and 8 JMLIT OWG members.

2. Requesting data and gathering the responses
   Live case used for POC data request (S7). Data returned in the response template and anonymized for the proof of concept.

3. Data processing and network analytics
   Modelling of data for automated loading, integration and visualization.
JMLIT

Data collation and modelling process

A pilot response template was developed by conducting a series of workshops held with JMLIT OWG members. Based on the responses received from banks, data was modelled into nodes and edges to enable the visualisation of relationships.
JMLIT
Data modelling approach

Structured data was modelled into the below nodes and edges (i.e. relationships). Pre-built queries were applied to visualise the network and demonstrate relationships across the datasets.

Data sources
- Bank data
- SAR Data
- Subjects of interest
- Public data

Node and edge types
- Node types
  - Individuals
  - Subjects of interest
  - Companies
  - Entities (where not company/individual is not specified)
  - Bank accounts
  - Banks

- Edge Types
  - Common address
  - Has bank account
  - Transactions
  - Possibly same company as
  - Similar name as
  - Very similar name as
  - Director/significant controller/UBO/shareholder/signatory of

Received from banks with the following data fields:
- Customer Personal
- Customer Business
- Customer Level Address
- Account Level Retail
- Transaction Level

Unstructured data including transactions, addresses, companies, individuals, additional company names, phone numbers and email addresses.

A list of the entities under investigation

This included entity information such as addresses and the directors/significant controllers of these entities.
Combining data from multiple institutions and other external sources can help build better intelligence and understanding of the wider network by revealing hidden connections.
JMLIT

Examples outputs with potential relevance to the JMLIT operating model

The outputs from Analyses 1 and 2 demonstrate how structured data and network analytics can be used to deliver Reactive Tactical, Pro-active Tactical and Proactive Strategic value to the JMLIT customer.

Examples:

- **Analysis 1** – Identify and investigate common controllers of different subjects of interest
- **Analysis 2** – Transaction flows assist with asset tracing, it also highlights and prioritises investigative leads

- **Analysis 1** – Common address between multiple subjects of interest that are otherwise unrelated could be relevant for identifying new potential leads
- **Analysis 2** – Visualising complex relationships and behaviours can be used to build better understanding of money laundering typologies and organised crime group structures. This in turn enables the development of valuable strategic insight that both LE and the industry can use for intelligence based detection and prevention.
- **Analysis 2** - Hidden connections that cannot be identified by looking at one dataset in isolation can be revealed, providing a broader view of customer activity and relationships. Where justifiable and proportionate and subject to obtaining necessary agreement(s) to sharing data, the NCA could provide banks with the un-sanitised network chart, this would show the parties and relationships identified in a case to assist banks with understanding customer and third party risks.
JMLIT
Key successes from Deloitte’s work on the proof of concept

- is based on a real case and real data from multiple banks
- developed the pilot approach to standardising bank data and considered other possible data sources
- successfully engaged the public and private sector stakeholders in the standardisation of data and the sharing of raw data as part of the proof of concept
- shows that relevant data can be provided in a structured format and transformed using automation and analytics to provide a more holistic view of the network. This is a key enabler for understanding and disrupting more complex money laundering cases.
Live poll 3: Our future priorities
Please go to www.menti.com and enter code 57 56 84

Which topic from the below should be the priority for the financial crime agenda in the medium to long term?

i. Addressing new financial crime risks and regulation
ii. Adopting new technologies
iii. Improving intelligence sharing between industry bodies
iv. Taking a more customer centric and holistic approach
v. Something else