



Review of banks' anti-money laundering systems and controls

Stewart McGlynn
Anti-Money Laundering
Banking Supervision Department
Hong Kong Monetary Authority

22 & 23 April 2013



HONG KONG MONETARY AUTHORITY
香港金融管理局



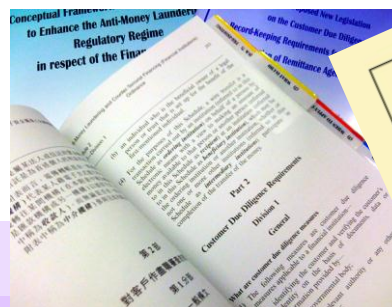
Disclaimer

- This presentation provides guidance to authorized institutions (“AIs”) on issues relating to the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (“AMLO”) and the AMLO Guideline. The presentation is provided for training purposes and does not form part of the formal legal and regulatory requirements of the HKMA. It should not be substituted for seeking detailed advice on any specific case from an AI’s own professional adviser.
- The HKMA is the owner of the copyright and any other rights in the PowerPoint materials of this presentation. These materials may be used for personal viewing purposes or for use within an AI. Such materials may not be reproduced for or distributed to third parties, or used for commercial purposes, without the HKMA’s prior written consent.



Regulatory Regime

- Mature Anti-Money Laundering (AML) Regime
 - HKMA Guideline since 1993, STR requirement since 1989/95
- Anti-Money Laundering and Counter-Terrorist Financing Ord. (AMLO) commenced on 1 April 2012
- 14 x AML Examinations after 1 April 2012
 - 5 x In-Depth 'Tier 2'
 - 9 x Thematic examination - Transaction Monitoring (TM) & Suspicious Transaction Reporting (STR)





ML/TF Risk Management

- Senior Management Oversight
- Policies and Procedures
- Management of AML/CFT Function
- Internal Audit and Compliance Reviews
- Correspondent Banking
- Transaction Screening
- Transaction Monitoring
- Suspicious Transaction Reporting



Senior Management Oversight

- Expectation is senior management should take clear responsibility for managing ML risks
 - There should be evidence of active engagement by senior management in the bank's approach to managing ML risks
- AMLO requires a FI to take all reasonable measures to ensure that proper safeguards are taken to prevent a contravention and to mitigate ML and TF risks (s.23)





Senior Management Oversight

- Participation by management at sufficiently high level is needed
- Senior management should receive informative and objective information sufficient to discharge AML obligations
- Must be strategy or evidence of self improvement
 - Coordination across the bank on AML required
 - AML issues must be dealt with on a proactive basis
- Senior Management should ensure AML department has sufficient resources



Policies and Procedures

Must have in place up-to-date P&P that are appropriate to its business. These P&P must be readily accessible, effective and understood by all relevant staff. We expect banks to check whether P&P are applied consistently and effectively





Money Laundering Reporting Officer

Money Laundering Reporting Officers (MLRO) are responsible for oversight of the banks compliance with its AML/CFT obligations and should act as a central reference point for reporting suspicious transactions. For example:

- the MLRO should have sufficient **resources**, **experience**, access and seniority to be effective
- the MLRO should fully understand the rationale of policies they were overseeing
- The MLRO should have sufficient awareness and oversight of the highest risk relationships



Money Laundering Reporting Officer

Our Requirements:

- MLRO should not simply be that of a passive recipient of ad hoc reports of suspicious transactions
- MLRO should play an active role in the identification and reporting of suspicious transactions
- This may also involve regular review of exception reports or large or irregular transaction reports as well as ad hoc reports made by staff



Internal Audit & Compliance Reviews

- Banks approach to reviews of effectiveness of AML systems must be comprehensive
- Scope of review must address Bank's risks
- Findings of recent IA and compliance reviews on AML controls must drive change
 - Reports must be of sufficient quality
 - Should ensure the information is discussed at sufficiently senior level
- Implementation of remedial measures must be consistent





Risks of Correspondent Banking

- The correspondent AI often has no direct relationship with the underlying parties to a transaction
- Banks often have limited information regarding the nature and purpose of the underlying transactions
- Correspondent banking is therefore regarded as high-risk from a ML/TF perspective
- Special due diligence requirements for correspondent banking relationships apply



Correspondent Banking

- Must consider the ML risk of Correspondent Bank
- Should have adequate P&P on how to deal with respondents
- Should not apply a one size fits all
- Reliance on assessments that exist elsewhere within a group, without local nexus, may not be sufficient
- Ensure robust monitoring of respondents identified as presenting higher risks



Transaction Screening

- Does the bank maintain a comprehensive and up-to-date watch list database for effective identification of names that may trigger suspicion?





Transaction Screening

- Should ensure the designated parties database and high-risk / sanctioned jurisdictions list are complete
- The algorithm used in the screening system should be able to identify names with minor alterations (e.g. reverse order or partial name)
- Screening system must support Chinese characters / commercial code OR written guidance must be provided to mitigate this risk
- Should have formal P&P for handling transactions connected with high-risk / sanctioned jurisdictions



Good Practices

- Clear P&P to ensure timely updating of the designation parties database and high-risk / sanctioned jurisdictions list
- Conduct testing on the names of newly added designated parties to ensure completeness and accuracy of database
- Establish internal P&P to provide guidance to staff handling transactions with sanctioned jurisdictions taking into account the restrictions imposed in sanction programmes, including the requirement for review, EDD etc



Transaction Monitoring

- Are the banks transaction monitoring systems adequate, given their business activities and size?
- How does the bank ensure systematic investigations into unusual transactions and potential STRs?





Transaction Monitoring

- Depending on nature and scale of the bank, automated TM systems may be important for effective AML controls
- Must ensure sufficiently detailed system review
 - Sufficient coverage of TM systems
 - Thresholds and parameters must be appropriate
- Should have a clear understanding of what the system could deliver / limitations
 - TM can only supplement, not replace human element
- Responsibilities for reviewing, investigating and reporting alerts must be clearly allocated



Good Practices

- Conduct detailed assessments prior to the launch of TM systems to ensure adequate coverage
- Give careful consideration to thresholds and parameters and consider validation by independent third parties
- No “one size fits all” - categorize thresholds and parameters according to customer’s business size and nature
- Conduct regular (e.g. annual) review and enhancements on TM system by internal department or use external consultants where the system is complex or internal experience is insufficient



Suspicious Transaction Reports

- To what extent does the bank understand and carry out, their detection and reporting obligations on the suspected proceeds of crime?





Suspicious Transaction Reports

- STR reporting is not only a legal necessity, rather it is a matter of real concern for banks
- All internal reports must be subject to meaningful analysis to determine whether disclosure is required
- Guidance should be provided on connected accounts to ensure understanding
- Should conduct an appropriate review of business relationship upon filing, to mitigate the risk
- Processes for dealing with repeat internal / external STRs must be sufficiently robust to protect the bank
- Consent System must be clearly understood



Good Practices

- Mandatory trigger event review & thorough process to determine applicability of risk classification etc
- Robust P&P underpinning these actions, including escalation, to mitigate risk
- Policy on repeat internal / external STRs
- Termination of relationships where unacceptable ML risks existed and indicate this in the initial disclosure to the JFIU
- Use of internal / external reporting experience to identify weaknesses in CDD, branch controls; evidence of active learning
- Clear P&P regarding timeframe for analysis; clear guidance for escalation where immediate risk existed
- Conduct regular reviews of resources allocated to these tasks, and ensure the Board act upon the findings of the review



Looking Forward



Alerts

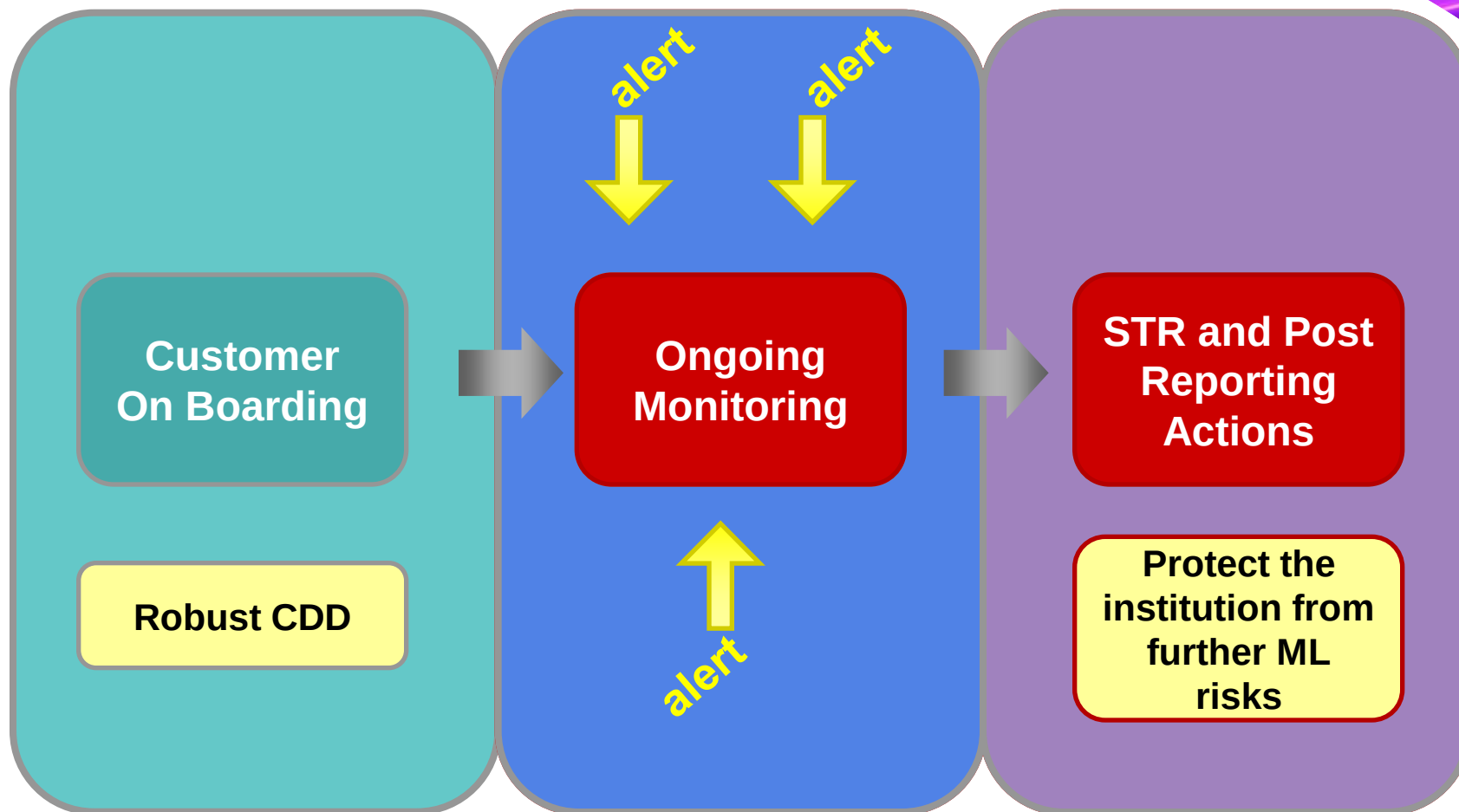


WARNING!

Handling of alerts must be effective
Actions performed must address
risk



Opportunity for Intervention





Key Takeaways

- Senior management must demonstrate leadership on AML
- Policy & procedure must reflect that leadership
- AML function needs experienced people and adequate resources – requirement to review
- AML responsibility lies with all staff but CO/MLRO play a central role
- Effectiveness of controls must be regularly reviewed – Transaction Monitoring and STR are pillars
- ML risks should be understood and mitigated
- Banks should demonstrate willingness to exit where there are unacceptable ML risks



Stewart McGlynn
Tel. 2878 1095
smcglynn@hkma.gov.hk



Suspicious Transaction Report Trends and Quality Improvement

Chief Inspector Bernard LAW
Joint Financial Intelligence Unit



Joint Financial
Intelligence Unit



Important Notice

All rights, including copyright, in this PowerPoint file are owned and reserved by the Hong Kong Police Force. Unless prior permission in writing is given by the Commissioner of Police, you may not use the materials other than for your personal learning and in the course of your official duty.

重要告示

香港警務處持有並保留本簡報檔案包括版權在內的所有權益。除預先獲得警務處處長書面許可外，本簡報檔案只可用作個人學習及處理公務上用途。

Agenda

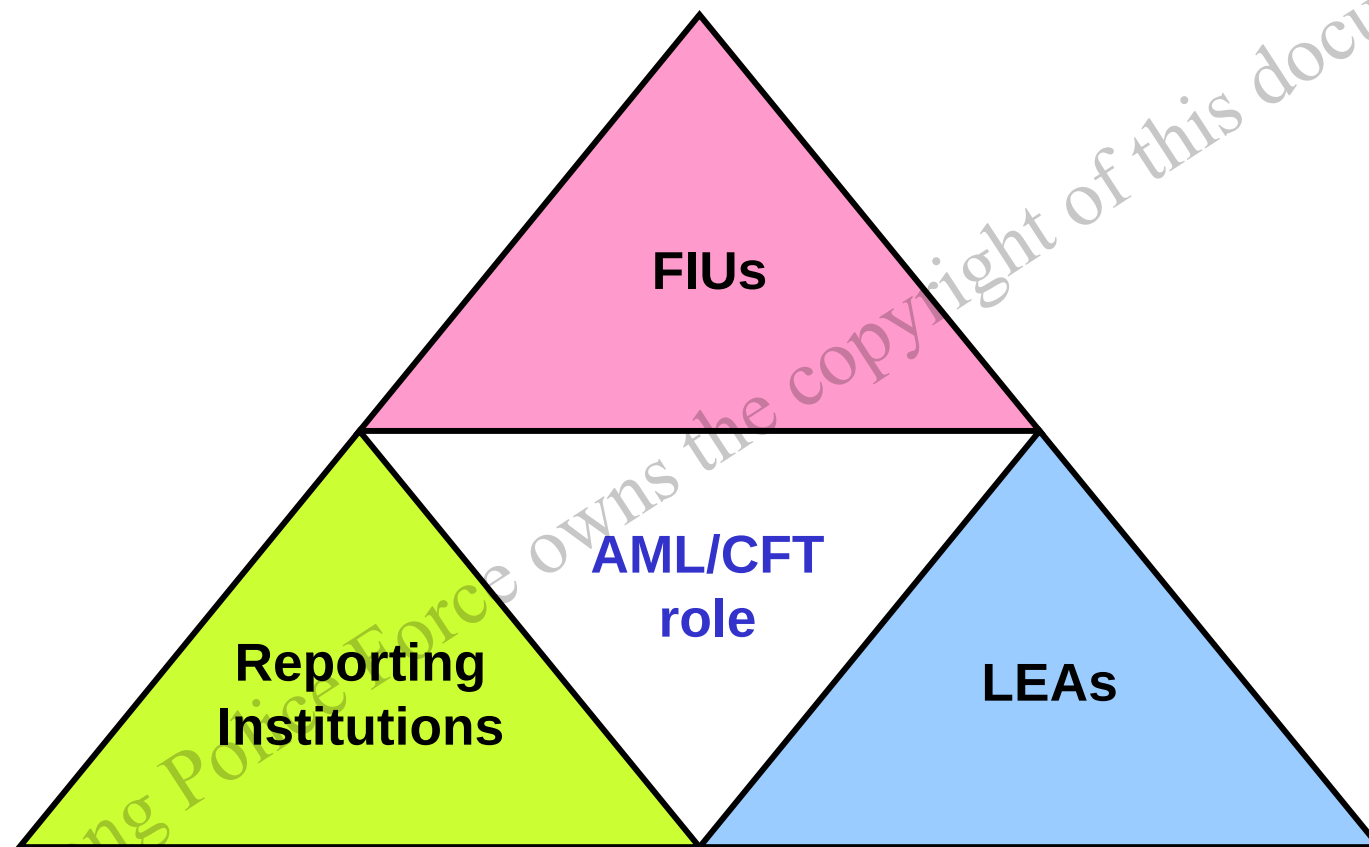
- Importance of Reporting Institutions
- Typologies
- Statistic of Suspicious Transaction Reports
- Quality Suspicious Transaction Reporting
- Conclusion



Joint Financial
Intelligence Unit



Importance of Reporting Institution



Joint Financial
Intelligence Unit



Different Players and Roles

Reporting Institutions

- Customer identification
- Record keeping
- Internal systems and controls
- Suspicious transactions

FIUs

- Handling STR
- Dissemination
- Information exchange
- Feedback
- Outreach program

LEAs

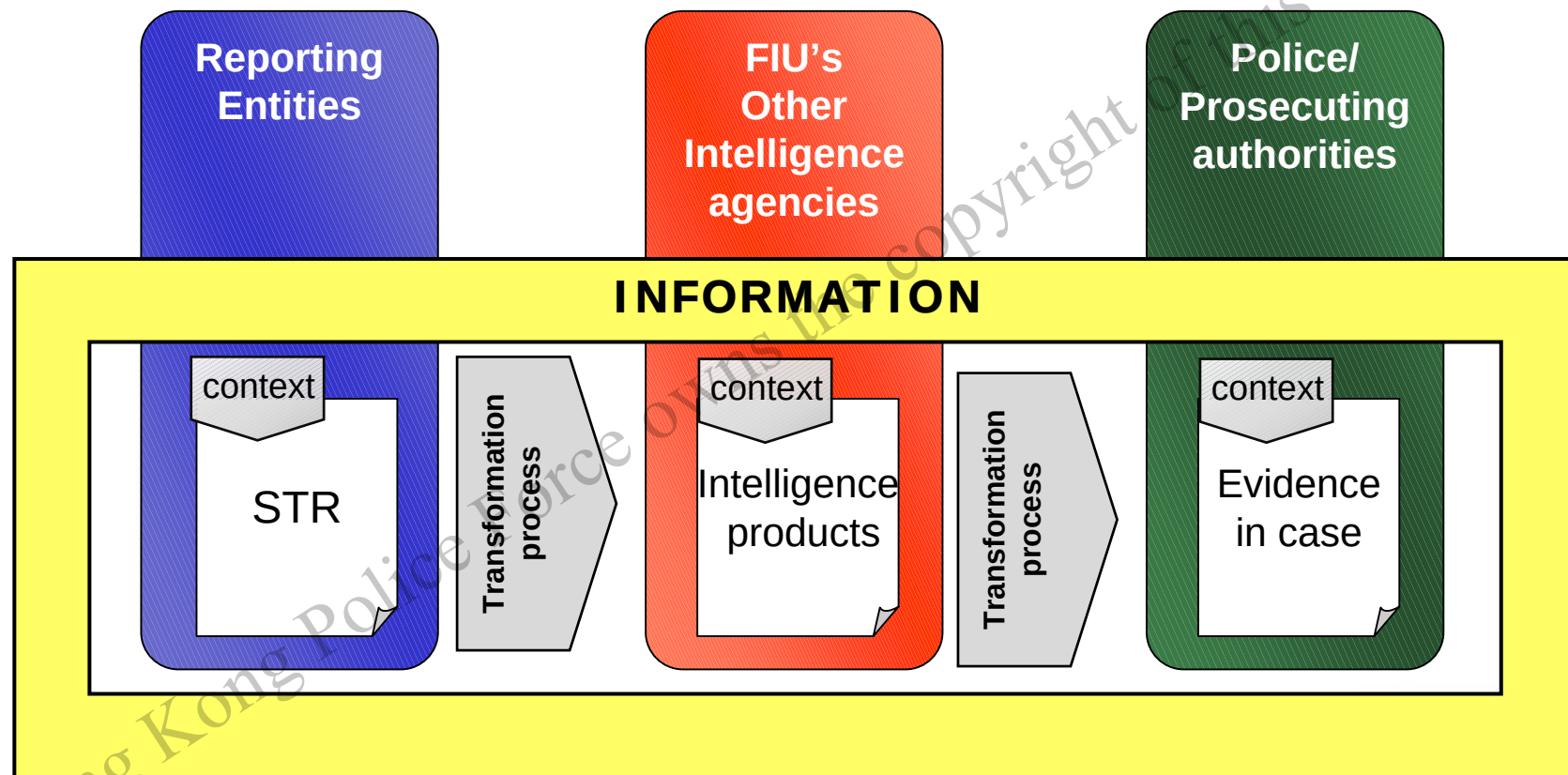
- ML investigation
- Asset tracing
- Asset recovery
- Information exchange
- MLA



**Joint Financial
Intelligence Unit**



Information Flow



Joint Financial
Intelligence Unit



Legislation

Reporting Obligation

Organized and Serious Crimes Ordinance “OSCO”

Section 25A(1)

A person knows or suspect that
any property (directly or indirectly) represents any
person's proceeds of an indictable offence

should disclose that knowledge or suspicion to an
authorized officer within a reasonable time



**Suspicious Transaction Report
(STR)**

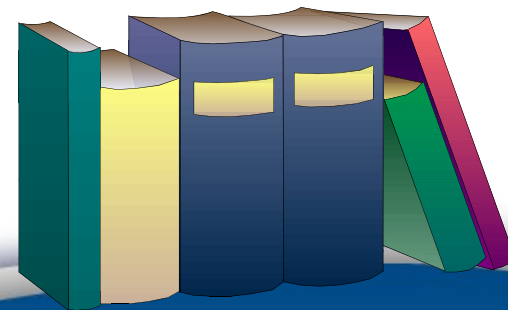


Joint Financial
Intelligence Unit



Legislation

- Offence if failing to report: s. 25A(1)
- Disclosure protection of ML offence: s.25A(2)
- Protection against suit: s.25A (3)
- Offence to disclose the disclosure: s.25A (5)
tipping off “any matter likely to prejudice an investigation”



Joint Financial
Intelligence Unit





Typologies



Joint Financial
Intelligence Unit



Typologies

- A series of ML or TF arrangements which are conducted in similar manner or using the same methods.
- In general term, the study of methods, techniques and trends used by money launderer and terrorist financier.



Typologies

To help the reporting institutions in understanding the trend and identifying the vulnerable areas used by the Money Launderer and Terrorist Financier



**Joint Financial
Intelligence Unit**



Typologies



Corporate Vehicle

- easy to set up
- beneficial ownership
- shell company



Use of TCSP

- non-resident holding several companies
- registered / corresponding address
- secretarial services



Bank Account

- opened company accounts with different banks
- 3rd party as authorized signatories

Typologies



Trade-based Transaction

- over & under invoicing
- counter balance
- multiple business



Money Transfer

- e-Banking
- via Money Services Operator
- multiple transfers between accounts



Other issues

- unlicensed Money Services Operator
- front man
- theft of identity

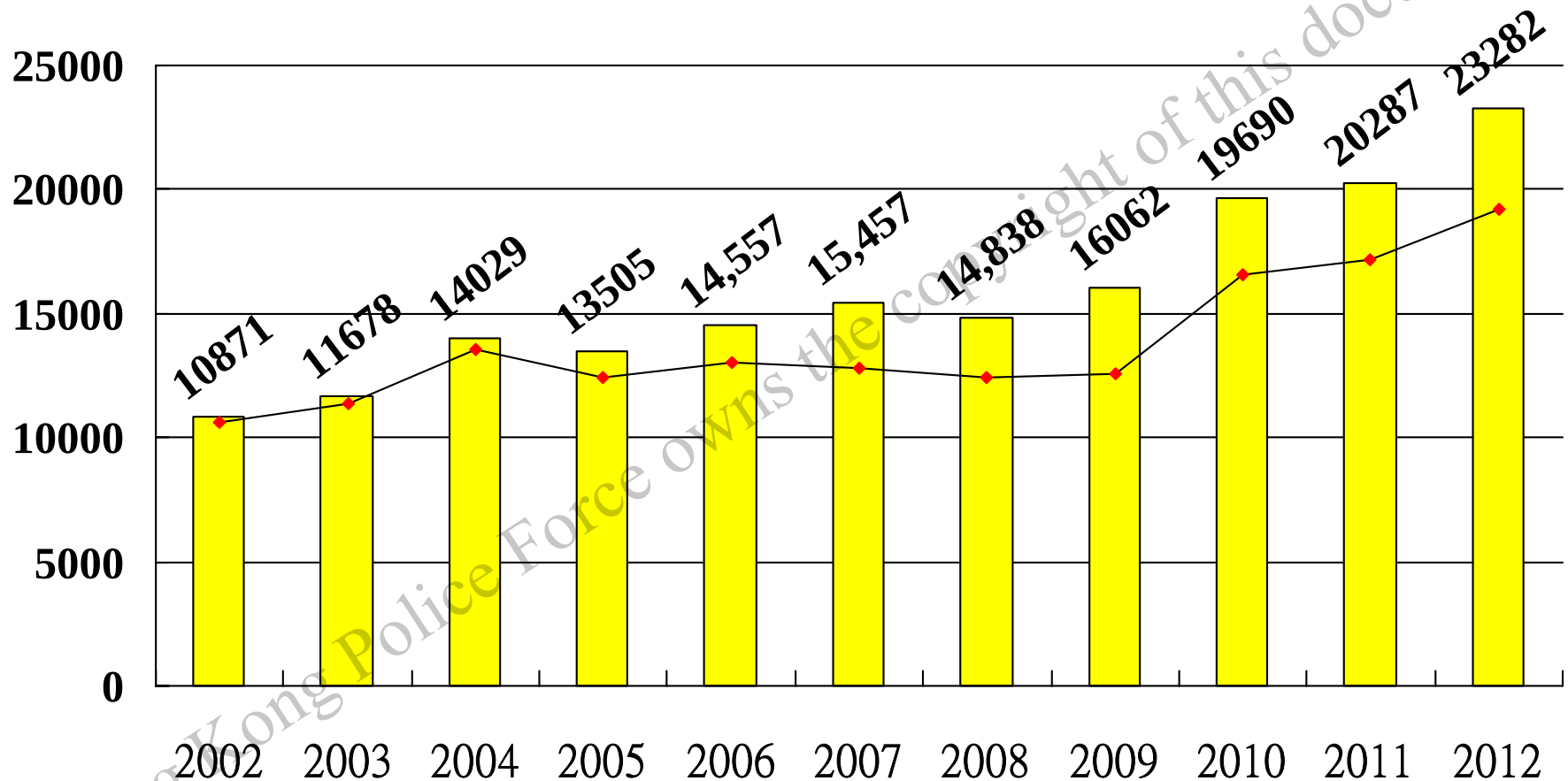
Typologies

Indicators

- Multiple inward remittances from different senders
- Multiple outward remittances to overseas accounts
- Temporary repository of fund
- Destination of transfer not commensurate with customer profile
- Payment of “consultancy fees” or “loan”
- Accounts only operated for a few months



STR received in the past 10 years



- Represents no. of STR made by Banks

Quality Reporting

Sufficient
information?

Suspicion
identified?

CDD and KYC
process?

Precise and
Concise?

Evaluation?



Joint Financial
Intelligence Unit



Quality Reporting

Sufficient Information

- **Client / BO information**
 - company details
 - ID information
- **Transaction information**
 - fund flow
 - counterparties information



Joint Financial
Intelligence Unit



Quality Reporting

Suspicion identified



- Background of customer/BO
- Quote source of suspicion
- Transaction patterns
- Avoid incoherent information



Joint Financial
Intelligence Unit



Quality Reporting

KYC and CDD Process

- Update Personal and Company information
- Enquire customers for suspicious transactions
- On-going transaction monitoring



Joint Financial
Intelligence Unit



Quality Reporting

Precise and Concise

- 23,282 STRs received in 2012
- Quality reporting is essential
- Precise and concise without redundant and duplicated information



Joint Financial
Intelligence Unit



Quality Reporting

Evaluation

- Not every STR is to be reported if risk can be mitigated
- Detailed the conclusion reached on the necessity of STR reporting
- Report STR once suspicion arose



Conclusion

“Compliance is not a ‘check-the-box’ exercise, but rather requires financial institutions to exercise their judgement, as informed by our guidance and assistance.”



Bill Fox, ex-FinCEN Director



**Joint Financial
Intelligence Unit**





Thank You



**Joint Financial
Intelligence Unit**





Supervisory Response of the HKMA

**Stewart McGlynn
Banking Supervision Department
Hong Kong Monetary Authority**

22 & 23 April 2013

Well-focused Supervision



- Our programme of in-depth AML examinations will continue and at the same time be strengthened
- Thematic AML examinations will remain a key part of our supervisory approach
- A thematic review of the private banking sector has just commenced
- AML examinations will also test banks' controls and vigilance to combat the risks of tax evasion

What to expect?



- We intend to be more proactive, adopting a more forward looking approach
- We will review the frequency, intensity and scope of our on-site and off-site examinations
- We are significantly strengthening the resources dedicated to AML supervision and are reviewing our follow-up processes
- We will be prepared to take early intervention to tackle root cause rather than waiting for risks to accumulate

Key Questions



- Is the tone from the top clear in your bank?
- What steps have you taken to foster a strong risk culture?
- How do you ensure that the AML function is equipped with sufficient resources to perform effectively?
- Do you oversee measures to ensure that your AML programme is systematic?
- Is your AML programme subject to regular review?
- Do you play a central and proactive role?

Key Takeaways



- International standards and obligations on AML must be met
- Effective AML measures in the banking sector are essential as it acts as a gatekeeper
- Resources afforded to AML work must be adequate
- The obligation to implement the AML rules fully and in good faith must always come before business interests
- HKMA will be ready to take tougher actions, including the use of our powers under AMLO.



~ Thank You ~