OLIVER WYMAN

Financial Services

ASIA PACIFIC RISK CENTER: FINANCE AND RISK SERIES

FINANCIAL CRIME RISK MANAGEMENT IN ASIA PACIFIC

A RISING COST, AND URGENT IMPERATIVE

MARSH GUY CARPENTER MERCER OLIVER WYMAN

MARSH & McLENNAN COMPANIES

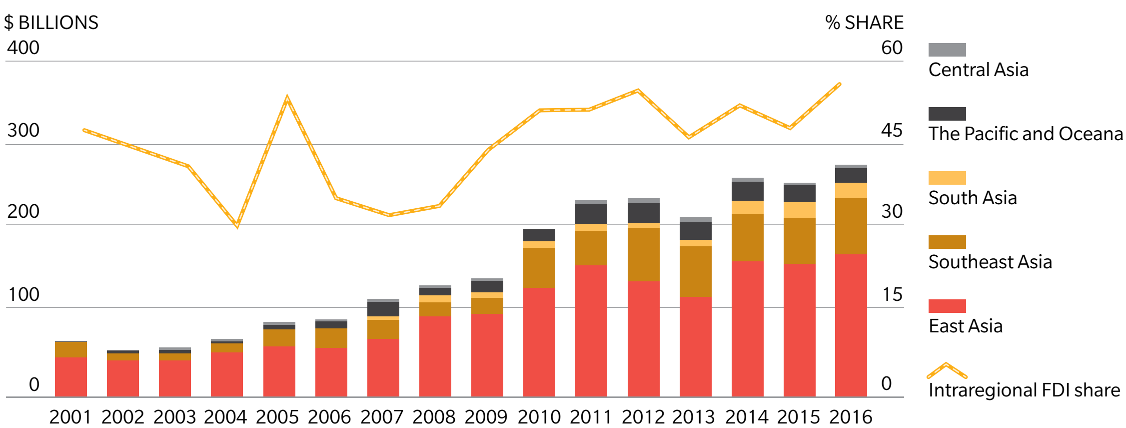
Costs for Financial Crime are rising and financial institutions in Asia are having to bear them. In February 2018, a large state owned Indian bank was involved in fraudulent transactions of total value exceeding USD 2 BN. As a direct cause of the market's reaction to the news, the bank's shares dropped by almost 40% of its market value in three weeks. This happened due to the lack of adequate controls in the bank, which allowed criminals to work through the loopholes of the system and bribe internal employees to help them implement the fraud. While this has been dubbed as the biggest fraud in India's banking history, it is by no means an isolated incident in the region. This is an issue that FS institutions all over Asia Pacific should deal with urgently, or the costs may become unwieldy for the industry and society at large.

BANKS HAVE FAILED TO RECOGNIZE THE LEGITIMACY OF MONEY

Asia has long been a key market of interest, with consistent financial flows from the West. Foreign Direct Investment (FDI) is generally desirable for growing economies, not only in terms of immediate available cashflow for the local economy, but also in terms of impact on local employment indices and socio-economic progress due to inundation of new ideas. However, countries often relax trade laws, foreign ownership rules and government processes in order to make their country business- or investment- "friendly". This may affect the country's ability to effectively assess and manage the legitimacy of incoming cashflows. Recent trends in Asia[1] indicate that intraregional FDI has been on the rise in the region (see Exhibit 1).

With over 50% of FDI in Asia coming from other Asian countries, the overall development in the region is strongly dependent on the financial health and stability of the Asian market as a whole. This underscores the need to ensure that incoming capital is robust and reliable.

Exhibit 1: Intraregional FDI Inflows—Asia



Source: Asian Economic Integration Report 2017, ADB

1 Based on study by ADB, "Asian Economic Integration Report 2017", https://aric.adb.org/pdf/aeir/AEIR2017_3_cross-border-investment.pdf

ADB calculations using data from Association of Southeast Nations Secretariat; CEIC; Eurostat. Balance of Payments. http://ec.europa.eu/eurostat/web/ balance-of-payments/data/database (accessed July 2017); Korean Statistical Information Service. Balance of Payments. http://kosis.kr/statHtml/statHtml.do?orgId= 301&tblId=DT_022Y016&language=en&conn_path=I3 (accessed August 2017); Rep. of Korea Ministry of Trade, Industry, and Energy. http://www.motie.go.kr/www/ main.do (accessed August 2017); United Nations Conference on Trade and Development. Bilateral FDI Statistics. http://unctad.org/en/Pages/DIAE/FDI%20Statistics/ FDI-Statistics-Bilateral.aspx (accessed July 2017); Financial Times. fDi Markets (accessed May 2017); and Bureau van Dijk. Zephyr M&A Database (accessed May 2017).

Yet, the incoming cashflows are by no means all legitimate. Apart from carrying cash into a country, banks serve as the only "on and off ramp" for the payments system, and are the nexus through which all foreign money flows. However, banks have had a history of spectacular failures in risk management; most notably failure to identify payments and transfers that cause a breach in sanctions, and accusations of being complicit in money-laundering schemes. The latter issue has specifically plagued a multi-national British bank, which was accused of being complicit in sovereign money laundering of a staggering GBP 191.8 BN (approximately USD 254.7 BN) over 10 years. Perhaps the magnitude of the amount involved is best fathomed in relative terms – a single transaction of this order would likely wipe out quarterly profit for all but the largest 50 banks in the world.

Considering the extensive inflow of foreign funds, it is especially imperative for Asian banks to actively manage and mitigate risks associated with Financial Crime. This will not only help limit freedom for criminals and rogue states to operate, but also serve as a simple protection against financial distress and build trust in society.

A FOCUS FOR GOVERNMENT

Nearly all developing economies have substantial trade in the "black" market. This is a broad term used to refer to the untaxed, cash and foremost illegal transactions, which is frequently associated with serious crime, occasionally including terrorism funding. All the associated financial flows ultimately touch the banking sector, and governments all over the region have been steadily ramping up its resources and regulations in order to crack down on Financial Crime and its actors:

- The Monetary Authority of Singapore (MAS) is known for its zero tolerance approach to Financial Crime, and has historically taken strict action against any breaches or violations. In 2016-17, the Singaporean branches of two Swiss-based banks were shut down and senior executives prosecuted for failing to control money-laundering activities connected with an Asian sovereign wealth fund. Other local and foreign banks that were considered in violation of Singapore's anti-money laundering laws were slapped with sizeable fines of over SGD 1MN each. Following this major breach, the MAS set up dedicated units to monitor money-laundering risks and boost enforcement action.
- The Hong Kong Monetary Authority (HKMA) also launched a Fraud and Money Laundering Intelligence Taskforce (FMLIT [2]) in May 2017. The taskforce was launched as a 12-month pilot, and is a collaborative effort between the HKMA, Hong Kong Association of Banks, and 10 retail banks, with a single aim of enhancing detection, prevention and disruption mechanisms to combat Financial Crime.
- An extreme case of government action was documented[3] in Vietnam in Dec 2017, where the former board chairman of a large privately owned bank was handed a life sentence over charges of embezzlement and money laundering.

Other governments have directly enhanced funding to programs that track suspicious activity: The annual budget of the Australian Transaction Reports and Analysis Centre (AUSTRAC) has been increasing in line with the increased proliferation in Financial Crime. In 2010, AUSTRAC's annual budget was AUD 79.9MN. The estimated actual budget for 2016-17 was upped to AUD 88.6MN by the government, with additional funds made available for recruiting appropriately skilled staff. On December 2017, the Australian minister for Justice Michael Keenan announced a new funding package to inject an *extra AUD 43.3MN* (~50% of the announced budget) " to allow AUSTRAC to recruit more staff to ensure our financial

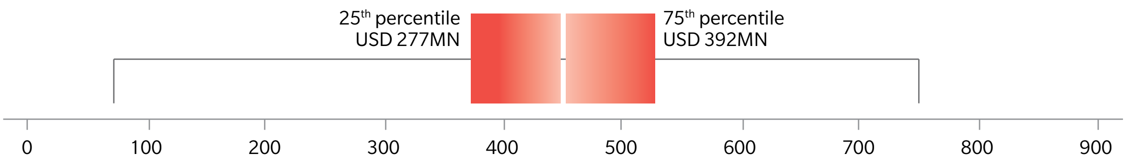
40%

INCREASE IN SUSPICIOUS ACTIVITY REPORTS FILED WITH THE JOINT FINANCIAL INTELLIGENCE UNIT, HONG KONG, 2015-17

2 Source: http://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml

3 Source: https://www.forbes.com/sites/ralphjennings/2017/12/19/corruption-is-threatening-vietnams-economic-miracle/#4cd147874767

Exhibit 2: Large scale financial crime control transformation programs, typical spend (USD MN; *excluding remediation* cost, total spend over 3-5 years)



institutions comply with the AML/CTF law and AML/CTF Rules."[4] This injection is a significant statement of intent by the Australian Government and AUSTRAC to Reporting Entities to ensure they have in place appropriate responses to their AML/CTF obligations.

THE IMPERATIVE FOR REGULATED FINANCIAL INSTITUTIONS

Regulators in the Asia-Pacific region will expect much more of the banks in terms of monitoring, controls and reporting, and banks will have to move closer to international norms in terms of investment in preventing Financial Crime. In terms of cost, we expect most banks to at least double their annual spend on Financial Crime Risk Management in business-as-usual state. Additionally, many banks which are coming from a lower base will need to significantly upscale their Financial Crime control environment to meet international norms. Estimates for large-scale Financial Crime control transformation programs range from USD 52MN to over USD 111MN annually, (average spending by industry leaders and large banks, excluding remediation cost) of which 10-20% will continue to accrue annually in business-as-usual state (see Exhibit 2).

At the lower end of the spectrum are typically domestic banks, with a limited international footprint. Such banks are characterized by:

- Less stringent local regulations and/or low regulatory intervention
- Institutions with historically higher levels of investment in Financial Crime control
- Greater use of internal resources, only leveraging external advisors in key SME roles

At the higher end of the spectrum are large global universal banks, with the following characteristics:

- Significant regulatory intervention/findings
- Historical underinvestment in Financial Crime control programmes
- Higher global minimum standards, e.g. global application of US standards
- High dependency on external advisors, e.g. advisory, legal and specialist SMEs

Asian banks should align themselves to where they want to be in future, instead of where they map at present. Banks can take a cue from peer jurisdictions here:

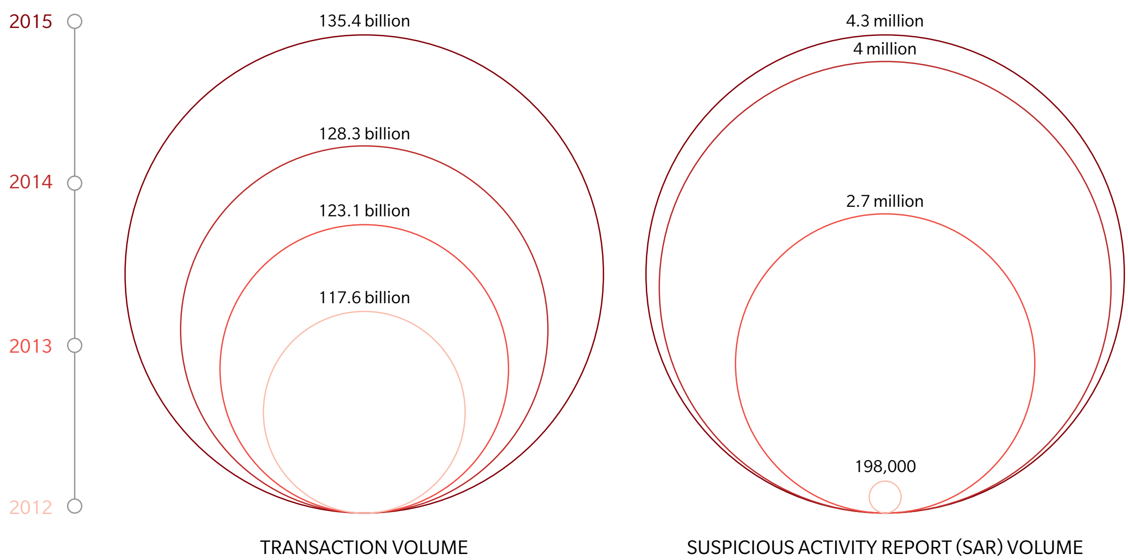
- The US saw a shocking 20x increase in Suspicious Activity Reports (SARs) filings in just 3 years (between 2012-2015) while growth in transactions increased moderately by approximately 3% between 2013 and 2015 (see Exhibit 3).
- Closer to home, a similar increase in reporting of suspicious activities is noted[5] by the Joint Financial Intelligence Unit (JFIU[6]) in Hong Kong (see Exhibit 3 on the next page). The JFIU received more suspicious activity reports from banks in 2017 than in any single year since their inception in 1989. This increase has been linked with the HKMA's requirement for banks to focus resources on the identification, assessment and filing on suspicious activity reports.

4 Source: https://www.linkedin.com/pulse/austrac-given-50-budget-increase-ensure-amlctf-compliance-neil-jeans/

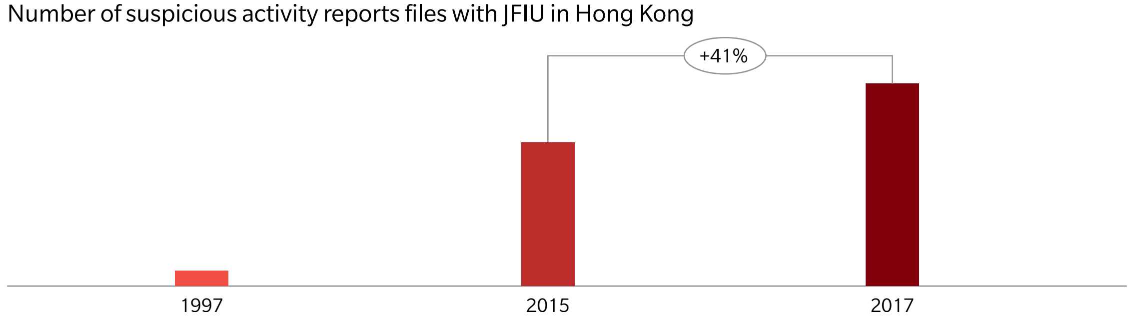
5 Source: South China Morning Post, Hong Kong money laundering and terrorism financing reports hit record high, Wed 2nd Nov 2017, "http://www.scmp.com/news/hong-kong/law-crime/article/2042029/hong-kong-money-laundering-and-terrorism-financing-reports"

6 JFIU is a 50-member outfit comprising police and customs officials

Exhibit 3: Recent trends in transaction volumes and suspicious activity report filings in the USA*



Number of suspicious activity reports files with JFIU in Hong Kong



***Sources:** BIS Committee on Payments and Market Infrastructure. Statistics on payment, clearing and settlement systems in the CPMI countries. Figures for 2015. December 2016; FinCEN SAR Stats. Technical Bulletin. March 2017; Data includes reports for money laundering, fraud, mortgage fraud, casinos, identification documentation, insurance, secruities/futures/options, structuring, terrorist financing, and other suspicious activities.

Source: *South China Morning Post*, Wednesday 2nd, November, 2017

While SAR filings have also been increasing in other major financial centres around the world with annual growth rates of 11% between 2012 and 2016[7], those rates have been far lower than the ones experienced in the US or Hong Kong market while increases in transaction volumes have been similar across the major financial centres such as US, Singapore, Hong Kong or Australia [8]. The differences observed in SAR filings growth rates can generally be attributed to three factors:

1. Either there is indeed more suspicious activity in the US and Hong Kong market compared to other financial centres, or
2. Regulators in other jurisdictions are less stringent on reporting activities, or
3. The US and Hong Kong regulators are much more sensitive with what constitutes suspicious activity and the reporting requirements it imposes on the entities operating within their jurisdiction.

In any case, the numbers show that even in sophisticated markets, Financial Crime operations are not yet fully effective – especially given that regulators have observed that only 10-20% of reported SAR filings actually add value to active law-enforcement investigations [9].

7 Source: Royal United Services Institute, "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime", October 2017

8 Source: Bank for International Settlements, Statistics on payment, clearing and settlement systems

9 Source: Royal United Services Institute, "The Role of Financial Information-Sharing Partnerships in the Disruption of Crime", October 2017

We therefore expect that regulators in many affected markets will keep raising demands on their reporting entities and that the pressure and need to raise awareness and investment will not go away. In order to remain relevant to their international competitors, Asian banks need to invest heavily in non-financial risk management in general, and specifically, to manage Financial Crime. Inaction may result in extensive regulatory and supervisory implications in the future, including fines, stricter capital, compliance rules and severe reputational damage and loss of trust with customers.

SIX THINGS TO DO NOW

Many firms that find themselves early in the journey of investing in Financial Crime Risk Management may struggle to know where to start and how to get a grip on the issues and their priorities. The first step is getting a handle on the issues and establishing a good relationship with the regulator. Most supervising bodies appreciate the complexities with which the bank is dealing. They are aware that controls sometimes represent a trade-off with customer experience; that systems may themselves prevent the creation of perfect

COMMUNICATION

- Top-down communication on importance of controls
- Active involvement from senior officials in educating the organization

CULTURE

- Risk awareness should be embedded in the culture of the bank
- Bankers are expected to be well-versed with details of each transaction

COMPLIANCE

- Compliance and reporting should be at expected levels
- Staff at all levels should be aware of relevant requirements

COVERAGE

- All customer segments, product classes, geographies etc. should be included for monitoring

COMPUTATION

- Banks should effectively leverage analytics and robotic process automation to monitor transactions and identify likely criminal activity
- Results in highest gains without excessive manpower deployment

COOPERATION

- Cooperation between banks on “best practices” in risk management
- Sharing critical information such as KYC utilities

controls environments; and that cultures and behaviours are slow to change. Nevertheless, their expectations have moved and we suggest an action plan targeting six areas for gains to get started:

COMMUNICATION

Senior leadership need to cascade communication of the importance of Financial Crime controls. Cultural gaps will begin with expectations from leadership; Board and Executive Committees need to be well-versed in specific examples of failures of Financial Crime controls and their implications. These can then be used to educate their leadership teams in the importance of world-class risk management in this area.

CULTURE

Uncertainty about the purpose of a transaction and identity of a customer must be unacceptable in the culture of the organization. This will be critical not just for management of Financial Crime, but also for good conduct and to satisfy community expectations. The playing field of expertise in finance is not level between provider and customer; bankers will be expected to have a solid grasp of transaction logic. Unusual requests should be met with questions, not executed regardless. This can be turned into a competitive advantage if done well and seamlessly.

COMPLIANCE

All staff need to understand the organization's obligations for clear and transparent reporting to regulatory and supervisory bodies. Staff should be aware of their role within that overall obligation. Compliance must be a 'gate' for performance measurement and a basic requirement at all levels.

COVERAGE

Technical aspects of managing Financial Crime are equally important – all transactions need to be screened, and all customers need to go through Know Your Customer (KYC) procedures to the desired quality. Risk assessments need to be thorough and scenarios tested need to be comprehensive to cover all products and segments. All geographies, branches and subsidiaries need to meet minimum standards, which are well-articulated and understood.

COMPUTATION

While Financial Crime is a major issue for all banks, armies of people conducting transaction checks and monitoring is not the answer. The most advanced institutions are finding radical increases in productivity from analytics. To this end, Citigroup president and chief executive of the bank's institutional clients group Jamie Forese, believes that the bank could replace up to half of its 20,000 technology and operations staff with machines over the next five years[10]. According to Mr Forese, operational positions at the bank were "most fertile for machine processing." It is an increasingly common sentiment. Transaction monitoring is moving from merely screening to use of advanced analytics and machine learning. This, by prioritizing the files for manual review, skews focus of expensive expert time to cases where it is most needed. Large complex organizations such as HSBC[11] have realized double digit gains in productivity, and helped set the goal-post for the industry.

COOPERATION

There are areas where cooperation in the industry is possible and to everyone's benefit, such as in the creation of utilities for processes that meet KYC requirements. Well-targeted cooperation makes regulators more rather than less comfortable, customers more satisfied (assuming privacy can be handled appropriately), and banks more efficient (where incentives are aligned).

The cost of poor Financial Crime Risk Management falls heavily on society as a whole – but especially heavily on the pockets of shareholders in firms judged to have materially missed expected standards. The response needs to be broad and deep, raising seniority of issue ownership, capabilities, and engagement at all levels of the industry. Leaders have already made substantive moves; where is your firm?

10 Source: Financial Times, "Citi issues stark warning on automation of bank jobs", June 2018
11 Source: AYASDI, "Anti-Money Laundering and AI at HSBC", June 2017

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

ASIA PACIFIC
+65 6510 9700

EMEA
+44 20 7333 8333

AMERICAS
+1 212 541 8100

AUTHORS

Jayant Raman
Principal, Finance & Risk
jayant.raman@oliverwyman.com

David Howard-Jones
Partner, Finance & Risk
david.howardjones@oliverwyman.co

Marie Stohldreier
Associate
Marie.Stohldreier@oliverwyman.com

CONTRIBUTORS

Ashwini Karandikar
Associate
ashwini.karandikar@oliverwyman.com

Kevin Zhang
Consultant
kevin.zhang@oliverwyman.com

www.oliverwyman.com

ABOUT THE ASIA PACIFIC RISK CENTER

Marsh & McLennan Companies' Asia Pacific Risk Center addresses the major threats facing industries, governments, and societies in the Asia Pacific Region and serves as the regional hub for our Global Risk Center. Our research staff in Singapore draws on the resources of Marsh, Guy Carpenter, Mercer, Oliver Wyman, and leading independent research partners around the world. We gather leaders from different sectors around critical challenges to stimulate new thinking and solutions vital to Asian markets. Our digital news service, BRINK Asia, keeps decision makers current on developing risk issues in the region.

For more information, please email the team at contactaprc@mmc.com.

OLIVER WYMAN