AFB COMPLIANCE PLATFORM

FINANCIAL CRIME EXPERT PANEL – OUTPUT PAPER

**AFB Expert Panels meet regularly and produce Output Papers on behalf of the whole membership (see Note).*

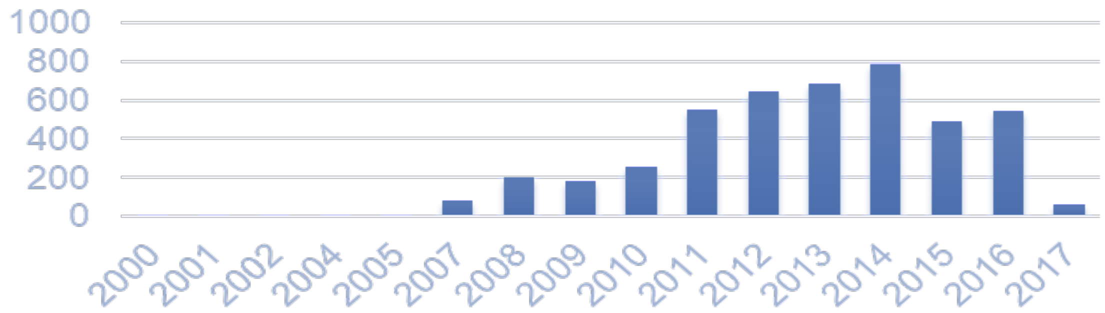
ANTI-MONEY LAUNDERING: WHAT DO THE 2020 FINCEN LEAKS TELL US ABOUT REGULATORY COLLABORATION AND THE FUTURE OF SARS?

A. THE US FINCEN LEAKS

In September 2020 BuzzFeed and the International Consortium of Investigative Journalists (ICIJ) published information on over 2,100 leaked documents from the US Financial Crimes Enforcement Network (FinCEN).[1] The detailed information from the leaks was never made public and we can only speculate on the content of the materials based on the press articles that were published.

The ICIJ published a 'transaction map' which set out the originator and beneficiary banks, and their jurisdictions; the number of transactions and suspicious activity reports (SARs); as well as the values of the suspicious transactions reported.[2] Our analysis of the transaction map shows that most of the data on the SARs and transactions reported relates to years between 2011 and 2016 (Fig. 1).

Fig 1. Number of transactions reported per year in the FinCEN leaks



[1] Buzzfeed News, 2020, https://www.buzzfeednews.com/article/jasonleopold/fincen-files-financial-scandal-criminal-networks

[2] ICIJ, 2020, https://www.icij.org/investigations/fincen-files/explore-the-fincen-files-data/ or https://www.icij.org/investigations/fincen-files/

While this data was often mistaken for evidence of widespread money laundering through the banks involved, it is not known what proportion of these SARs were as a result of genuine suspicions, and which were merely 'defensive' SAR filings.

A perhaps more generous interpretation of the leaked data is that, by filing these reports, the banks were behaving cautiously and working hard to fulfil their regulatory obligations, which would be a positive outcome which showed that the banks' systems and controls were able to detect the illicit funds. This process, however, did not seem to yield the best results in all cases.

B. WHAT WE CAN LEARN FROM THE FINCEN LEAKS

The historic nature of the leaked data does allow it to be compared to the fines issued by the various regulators for anti-money laundering (AML) deficiencies. This comparison reveals that banks reporting the largest volumes of suspicious transactions or with the largest values, were among those fined by the regulators for AML violations.

The investigations published in the press also revealed little in the way of new typologies. In many ways these latest leaks only confirmed what has already come to light from previous reporting on the Russian Laundromat, Azerbaijani Laundromat, Panama Papers, Paradise Papers and Formation House leak. These typologies related to the use of corporate structures to obfuscate the ownership and origin of the funds, by using UK Ltd companies, Scottish LPs and corporate structures in secrecy jurisdictions.

Analysis of the originator and beneficiary banks' jurisdictions also only confirmed what was already known from previous scandals. It still holds true that the majority of large money laundering activity occurs between Russia and Latvia, and from there, flows between financial centres in The Netherlands, Switzerland, UK, Singapore, Hong Kong, and the US.

It is not practical or realistic, however, to argue that banks should simply stop dealing with these 'higher-risk' countries. So, if last year's leaks demonstrate that the current system of defensive SARs filing may not be producing optimal outcomes, then it is perhaps time for a different approach, which involves more collaboration between banks and regulators.

C. RISK APPETITE AND RISK MITIGATION

Faced with these leaks, the temptation may be for banks to lower their risk appetite, especially when dealing with transactions from certain markets. Trying to approach the problem in this manner will, however, inevitably come at a cost.

The data set out in the FinCEN leaks shows that there is a clear profile for a risky transaction. Despite this, banks should not simply limit their risk appetite or slip into making blanket prohibitions. Refusing to deal with any transactions from Russia or Azerbaijan, for example, is simply not a realistic solution. Furthermore, any bank that does so will miss out on legitimate business which its competitors will benefit from.

Rather than focusing on limiting all exposure to risk – a difficult and sometimes damaging task – banks should be finding better ways to mitigate risks and operate safely and comfortably in high-risk environments. Focusing on developing strong controls and infrastructure, rather than denying business, however, requires a much more active engagement with AML procedures, senior management commitment and likely an increased spending on resources.

D. IDENTIFYING THE PROBLEMS

The first step towards better risk mitigation is identifying the current problems. Duff & Phelps' 2020 Global Enforcement Review showed that there are common failures identified by regulators among banks which have received AML fines.

These failures are often related to customer due diligence and the ongoing monitoring of relationships, the firm's overall management and understanding of AML risks, and the reporting of suspicious transactions.[3] While these areas do not appear to be immediately related, there are a number of common weaknesses which prevent banks reporting suspicious transactions:

- **Inadequate governance of the transaction monitoring processes** means that often the process itself is fragmented and lacks a senior manager who carries overall responsibility, which means it does not provide adequate coverage of transactional risks.
- **Weaknesses in customer risk assessment and due diligence** may also mean that banks do not collect sufficient customer information to allow for an adequate investigation of any unusual transactions or behaviours and therefore do not apply the adequate level of scrutiny to transactions.
- In some cases, **inadequate resources** (financial and staff) are allocated to the monitoring and reporting of transactions, which may lead to either delays in reporting or to ineffective investigations.
- On the other hand, **over-resourcing** by throwing several employees, contractors or spending on transaction monitoring systems, without the appropriate understanding of transactional risks, may also face failures. This can become a significant issue when banks do not retain the knowledge brought in by experienced contractors and external advisors.
- **Transaction monitoring systems** offered by specialised vendors can often prove helpful in identifying unusual transactions, by using advanced analytical technologies. However, without adjusting these solutions to the risks relevant to the bank, the outputs are often of no use.
- **Data and legacy systems:** over time, implementation of new systems and technologies may result in differences in the bank's data structure, which makes compiling this data into a single, readable format is often nearly impossible. At the same time, a lack of controls over the integrity of the data may also result in poor outcomes from advanced monitoring systems – after all, the output will only be as good as the input.
- **Banks tend to deploy these systems working entirely in silos.** Payment screening, transaction monitoring, E-ID verification, fraud detection, PEP and adverse media screening systems, are all often utilised independently and there is rarely a complete integration of all these systems.
- Banks operating as a part of larger group often place **reliance on centrally developed and implemented solutions.** Whilst these solutions tend to work well in the head office, they may not always be appropriate and adequate to the types of transactions or customers in a subsidiary or branch operating outside of the home country.

There is clearly a lot that banks can do to improve existing processes. For example, during the panel discussion, 48% of attendees declared that their bank is in the process of enhancing the transaction monitoring arrangements. Similarly, 48% declared that their transaction monitoring systems use a combination of both monetary thresholds and behavioural factors to increase the systems' effectiveness. It is important to recognise that money laundering is not something that the banks alone can prevent. No bank will have control over the weak verification of companies registered in certain jurisdictions, or over secrecy laws or lax regulations.

Banks can and do play an important part in the prevention of money laundering. They are not, however, solely responsible, and greater collaboration between all involved parties is essential to mitigate the money laundering risk and reduce the burdens on all involved.

E. EXISTING BEST PRACTICE MODELS

The UK currently has the leading best practice model for how regulators, financial intelligence units (FIUs) and the private sector can collaborate successfully. In 2015 the UK launched its Joint Money Laundering Intelligence Taskforce (JMLIT), which created a safe, legally sanctioned, environment where the public

[3] Duff & Phelps, 2020, https://www.duffandphelps.com/insights/publications/compliance-and-regulatory-consulting/global-enforcement-review-2020

and private sector can share information on crime typologies, discuss particular cases, and develop new methods of detection.

This was a vital step in the right direction and is currently considered international best practice. However, currently only the largest financial institutions in the UK can join the JMLIT, leaving smaller banks outside of its benefits. During the panel discussions 73% of participants considered that smaller and foreign banks should also have a seat at the table. However, some, quite rightly raised a concern regarding resources that would be required in order to be able to equally contribute and bring something useful to the table.

The National Economic Crime Centre (NECC) has also been created to promote broader cooperation between the UK's FIUs and other agencies, including outside of the UK. However, NECC efforts could be put into jeopardy by Brexit. Data sharing and collaboration with European regulators and agencies have both been impacted by the UK's exit from the EU. Additionally, it seems likely that Brexit will hinder the UK's ability to conduct cross-border investigations that affect both the UK and EU, at least temporarily.[4]

Given that so much information is exchanged on social media, perhaps the UK model needs to do more to engage with social media companies and bring them into the discussions. The same is true for the property and legal sector, particularly in London. There has been a wealth of reporting that has set out evidence that there are millions of pounds hidden in the London property market that were laundered out of Russia.[5] Despite this, nothing major has been done to address the problem, and the current system seems inadequate to address it.

There are still further problems with the UK approach, but for now it remains the best practice model for AML efforts. The key trend to observe is that the more collaborative and holistic AML measures are, the more effective their outcomes.

F. KEY TAKEAWAYS

The ideal goal then for banks is to move away from a process defined by defensively filing SARs to a more proactive stance which allows them to operate more comfortably in a high-risk environment. They cannot achieve this alone, however, and the support of regulators and enforcement agencies is vital. While these collaborative systems are built and improved, banks can use the lessons learned from the FinCEN leaks to re-think their approach to AML.

Fundamentally, hiring resources to deal with the volume of SARs is not a permanent solution. Banks need to hire quality resources that will be better able to analyse and detect potential wrongdoing by an ordinary customer. To do this, they must build a sound understanding of what risks the business may be exposed to, through thorough risk assessments and training programmes. This will allow businesses to develop an understanding of what a high-risk transaction may look like and subsequently what behaviour or transaction should be viewed as suspicious.

Identifying these suspicious transactions starts with obtaining and maintaining strong customer information, in line with KYC (know your customer) and KYB (know your business) procedures. Just because a customer has made an unusual payment, it doesn't mean that a report needs to be filed. It is when a payment does not make any logical sense in the context of the customer's profile, occupation, income and past behavioural patterns, that an analysis needs to be undertaken to establish why transaction took place, where the criminal funds may have come from and where they are going. During the panel discussion, we considered what should happen where MLROs detect "repeat offenders" or where multiple suspicions have been raised but the senior management is not prepared to exit a client.

[4] Sky News, 2020, https://news.sky.com/story/brexit-britain-will-be-less-secure-without-access-to-shared-data-12172399

[5] The Guardian, 2020, https://www.theguardian.com/money/2020/dec/21/luxury-london-homes-still-used-to-launder-illicit-funds-says-report

If it is not possible to raise concerns internally in the safe environment, the MLRO must consider his/her own position and where appropriate make a report to the FCA's Whistleblowing team. However, one needs to remember about the legal protections given to whistle-blowers through the Public Interest Disclosure Act as the FCA may in some circumstances share the information with relevant organisations.

Finally, banks should remember that filing a SAR is not an evidence of wrongdoing, but instead an opportunity to provide information that may help the authorities in their investigations. SARs should set out the reasons for suspicion, outline the suspected wrongdoing and have their investigations completed in a reasonable timeframe. During the panel we asked attendees how long a SAR investigation takes on average from identification of suspicious behaviour to filing a SAR and found that 28% were able to submit a SAR within 5 business days, 16% took between 1-2 weeks to file with only 8% taking over 2 weeks to investigate a potentially suspicious transaction.

One must remember that whilst ensuring that SARs are filed as soon as reasonably possible in line with their obligations, it is equally important to place the emphasis on the quality of the information and on providing all the relevant details to the authorities, so that a new and stronger working pattern can be built.

NOTE

Meetings of AFB Expert Panels are held in compliance with AFB's Competition Law Guidance. All issues discussed are included in the relevant Output Paper. AFB holds a central record of all attendees at Expert Panel Meetings. AFB Expert Panel Output Papers are intended as general guidance and no action should be taken in reliance on them without specific legal advice.

QUERIES AND FOLLOW-UP

If you wish to speak to one of the AFB team, please feel free to contact

Ilza Javed, Associate, Practice and Events

Tel: 020 7283 8300

Email: ilza.javed@foreignbanks.org.uk

Alternatively, if you would like any further information about any of these matters, please feel free to contact the following individuals at Duff & Phelps below:

Maria Evstropova, Director, Regulatory Consulting

Tel: +44 2070890861 / +44 7921396527

Email: Maria.Evstropova@DuffandPhelps.com

Julius Kania, Vice President, Regulatory Consulting

Email: Julius.Kania@duffandphelps.com

Tel: +44 2070890803 /+44 7776470294

Issued March 2020

In Partnership with

DUFF & PHELPS
A KROLL BUSINESS

REPRESENTATIVE MEMBER BANKS
Rabobank (Chair)
BACB plc
Bank of China
Bank of India
Bank of Ireland UK Plc
Bank of New York Mellon
Bank Sepah International Plc
Commonwealth Bank of Australia
Daiwa Capital Markets Europe Ltd
DBS Bank Ltd
Deutsche Pfandbriefbank AG
DZ Bank
Emirates NBD
ICICI Bank UK PLC
IKANO Bank
KfW IPEX-Bank
Landesbank Baden-W¸rttemberg
LHV Bank
Mizuho Bank, Ltd
National Australia Bank Limited
NBG Bank, London Branch
Norddeutsche Landesbank
OCBC Bank
PNC Business Credit
Riyad Bank London Branch
Sberbank CIB (UK) Ltd
Silicon Valley Bank
Standard Advisory London Ltd
Turkish Bank (UK) Ltd
UniCredit Bank AG
UOB London Branch