Stop. Collaborate and Listen

March 2020

FINTRAIL

rdc
Smarter Screening

Introduction

Collaboration is key to fighting financial crime. By sharing information and exploring concerted approaches and solutions, with a balance between data sharing and data protection, we all stand to gain a broader perception of the various factors that envelop us and develop the capability to identify repeat offenders. In these rapidly changing times, it is imperative that we reassess our current strategies and check that they are fit for purpose. Disrupting financial criminals needs a new approach, and companies must be ready to challenge the norm. With 1.7 billion unbanked adults worldwide, FinTech is set to be a powerhouse, particularly with the help of government initiatives such as digital IDs[1]. This means the attitude FinTech takes to tackling financial crime is of key importance. The public and private sectors need to converge to attempt to share data to track and understand financial crime.

Criminals collaborate too

Throughout history, criminals have mastered the art of collaboration. It is well-established that criminal actors share their tactics, techniques, and procedures, including the processes by which they launder their ill-gotten gains. They have advantages over legitimate actors as they can be agile and responsive, have no data sharing concerns, and don't need regulations, laws, or frameworks to allow them to collaborate. Whilst there are unsophisticated actors in this space, there are also those who are extremely sophisticated in how they generate and launder the proceeds of their crimes, sharing tips and tricks amongst each other. In order to combat these actors, a similar stance should be taken by the banks, FinTechs, and law enforcement: a dynamic, collaborative effort.

To take one example, during the 1980s the Bank of Credit and Commerce International (BCCI) and its customers 'committ[ed] fraud and money laundering across the world, for an estimated value of £17.6 billion'[2]. News of the BCCI laundering scheme spread much faster through the underground networks than it did through the private or public sectors, and BCCI gained a reputation for being the go-to bank for arms smugglers, drug cartels, and dictators. Whilst the law did eventually catch up with BCCI[3], many criminals had already profited from their shortcomings, and the damage had already been done.

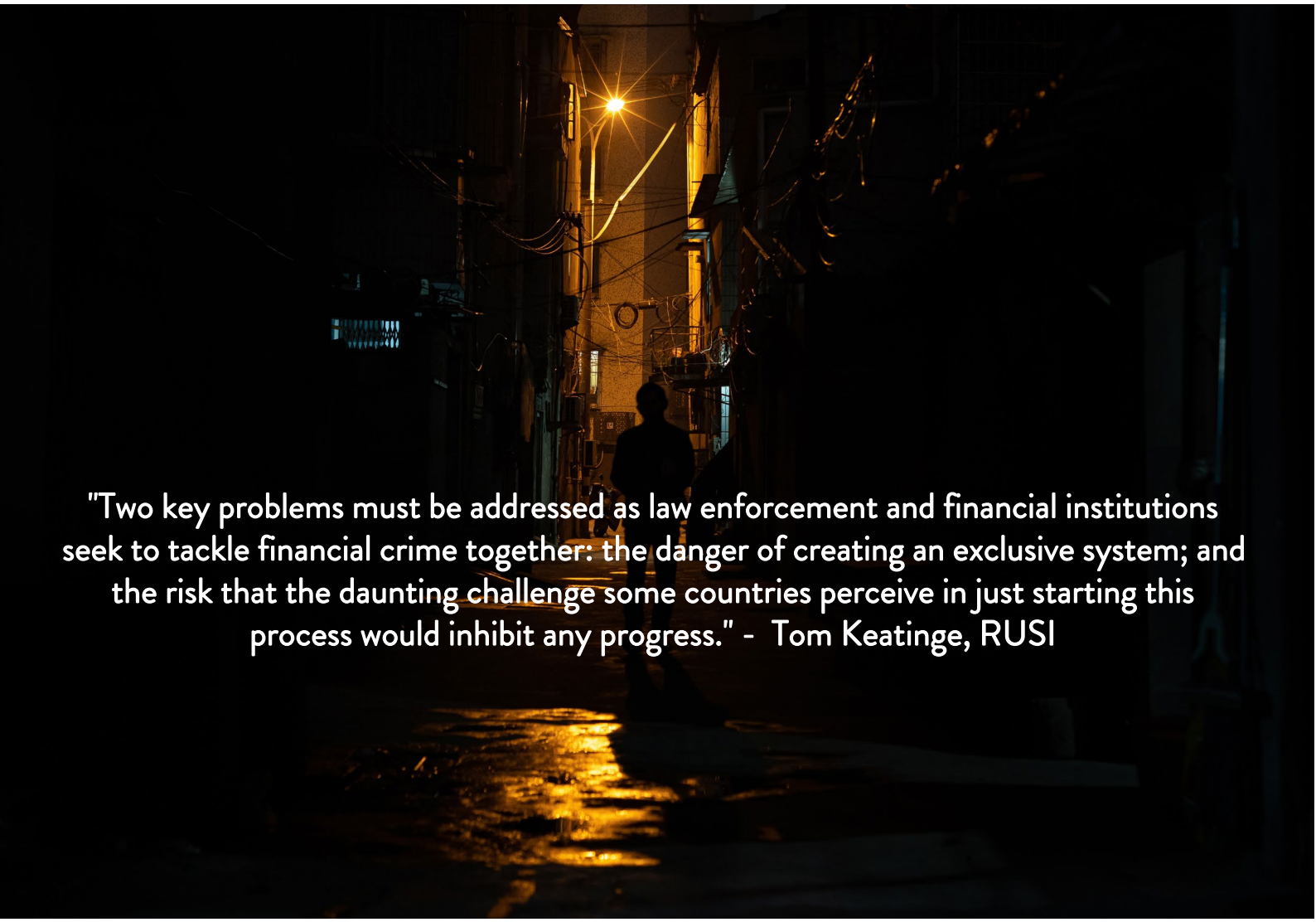
In today's world, everything is presented as an instant service - requesting taxis from your phone, ordering restaurant food to your door, and even recruiting money mules through social media. Whilst the traditional model of one ringmaster managing a money laundering scheme may still exist, an increasing trend is that of 'laundering-as-a-service' whereby a community of willing launderers, often money mules, are used on a demand-led basis. As noted in FINTRAIL's previous blog post, the criminals behind these activities keep track of the latest challenger banks, who have the easiest controls to circumvent, and actively seek out the demographic that tend to use these FinTechs.

1. Money-Laundering and Globalization

2. Top 5 Money Laundering Cases of the Last 30 Years

3. Business | Britain's biggest banking scandal

The use of messaging services is constantly on the rise, with popular favourites including Skype, WhatsApp, WeChat and Telegram[4]. Criminals have the advantage here; they can make use of the (often encrypted) technology available to any user, and re-purpose these services as a forum where they can create a network of like-minded people, sharing useful information and ideas - all with the aim of staying out of sight.



Collaboration can come in many shapes and sizes

Cross-sector collaboration

Credit Industry Fraud Avoidance System (Cifas)
Cifas is the UK's largest cross-sector fraud sharing platform, providing actionable insights into fraud, regardless of sector. As a collective, Cifas provides fraud databases, training, and tools to help with identity protection. The databases specifically include internal fraud and account takeover intelligence. This intelligence is provided by the community members, to be used by the community members. Its structure provides a framework and external mechanism through which different sectors and organisations can share information, whilst also remaining anonymous and ensuring they are not breaching any customer data restrictions.

4. Cyber-criminals reap the benefits of cross-community collaboration

Public sector led collaborations

Joint Money Laundering Intelligence Taskforce (JMLIT)
Launched in 2014, JMLIT is a partnership between law enforcement, over 40 financial institutions and the Financial Conduct Authority (FCA). The idea behind the taskforce is for members to exchange and analyse information relating to money laundering, alongside other wider economic threats.

Europol/Interpol Working Groups
A good example of successful joint effort is the 'European Money Mule Action' or EMMA. In December 2019, the 5th EMMA took place, resulting in the identification of 3,833 money mules alongside 386 money mule recruiters, of which 228 were arrested. 1,025 criminal investigations were opened, many of them are still ongoing. More than 650 banks, 17 bank associations and other financial institutions helped to report 7520 fraudulent money mule transactions, preventing a total loss of €12.9 million[5].

FCA TechSprint 2019[6]
This was an event led by the FCA hosting over 140 active participants from a variety of different institutions to tackle how privacy enhancing technologies can help increase the data sharing around money laundering and financial crime concerns, whilst still remaining compliant. A number of conceptual ideas were presented at the event, and the FCA continues to support those actionable outputs from the session.

Darkweb Takedowns
Following on from the successful takedown of Alphabay and Hansa in 2017 after a multi-jurisdiction investigation[7], the latest financial crime crackdown targeted Sweden's largest drug-related darknet platform. The Swedish police received collaborative support from more than 79 locations, 25 countries and at least 14 different server providers[8]. They drew on help from international law enforcement agencies, FinTechs and technological partners. As a result, the suspect is now in custody. This in itself is a testament to the fact that active collaboration, whether big or small, can always make a difference.

Private sector led collaborations

Dutch Banks Joint Transaction Monitoring[9]
In late 2019, five of the largest Dutch banks announced they were exploring the idea of joint transaction monitoring. Whilst the feasibility is still being ironed out, the banks note that not only will it allow them to share transactional information, but also join forces in terms of technical resources, to hopefully allow the banks to build algorithms together to identify illicit activity.

Nordic Banks' KYC efforts[10]
Six Nordic banks announced in July 2019 that they were starting a joint venture to develop a platform for handing KYC data, known as 'Nordic KYC Utility'. The idea behind this is to allow for standard processes for handling such data, and creating a smoother experience for the customer.

RDC and Liberty Shared Partnership[1]
Liberty Shared is a company whose aim is to reduce human trafficking through legal advocacy, technological advancements, and strategic partnerships. The nature of this partnership allows for Liberty Shared to channel intelligence through RDC's screening technology, creating an effective way of surfacing suspects and criminals convicted of human trafficking. The technology underpinning RDC's product provides a value-added information to Liberty Shared intel, as well as having the capability to share this information effectively amongst its customers.

The Wolfsberg Group
The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for managing financial crime risks. Its recent Statement on Effectiveness[12] outlines how determined the Group is to implement effective collaboration, notwithstanding its overriding purpose of regulatory compliance. The basis of this shift hinges on the review of an FI/AFC framework with a focus on collaboration.

Global Alliance FinTech Link[13]
In 2019, Bank Leumi of Israel, CIBC and National Australia Bank introduced Global Alliance Fintech Link, an online portal developed to help drive client-focused innovation by facilitating collaboration between the banks and financial technology firms (fintechs)[14]. The aim is to make it easier to collaborate on technology, simplify global cooperation, and also provide a potential partners to FinTechs that could help their business scale.

5. 228 arrests and over 3800 money mules identified in global action against money laundering
6. 2019 Global AML and Financial Crime TechSprint
7. Massive blow to criminal Dark Web activities after globally coordinated operation
8. Financial Ecosystem Provides Support In Massive Swedish Darkmarket Bust
9. In Fight Against Dirty Money, Dutch Banks Team Up on Algorithms
10. The collaboration of six Nordic banks results in a joint KYC company
11. RDC and Liberty Shared Partnership Now Identifying More than 30 Human Traffickers Per Day
12. The Wolfsberg Group - Statement on Effectiveness
13. Global Alliance Fintech Link | Discover. Pitch. Partner.
14. Bank Leumi, CIBC and National Australia Bank launch online portal to drive collaboration with fintechs

The future of collaboration

We live in a digital age where information can be shared instantaneously. Consequently, within organisations there should be no barriers and silos. The next step is to provide a suitable platform to share between external partners - public or private - so that we might be able to remain in step with the criminals as they innovate and deploy new schemes, rather than playing catch up from far behind.

Data sharing is a key future aspect of collaboration and advances still need to be made with regards to the sharing of actual data and typologies to promote a safer environment. Further diversification within the types of collaboration are also imperative to increasing interconnectivity within the community ie; not just involving big banks in a collaborative effort. Whilst efforts have been made in these areas, there is still room for improvement, and the landscape will no doubt change over the coming months and years.

Company-led collaboration

Companies should ensure that their anti-financial crime teams are communicating regularly with other departments within the company. Fraud, cyber security, and compliance teams should be well connected, as each team can provide valuable intelligence to the others when it comes to combating financial crime. This communication across departments can help to educate the business about wider threats to the company outside of their specific area.

Equally, the fight against financial crime doesn't just lie with FinCrime compliance teams. Awareness of financial crime should be baked into all financial institutions' products. From the initial conversations brainstorming a new product, through to launch day, FinCrime considerations should be borne in mind, and compliance teams should be kept involved at every step. For example, supplier onboarding, HR teams conducting background checks, and product and marketing departments should all be involved with the compliance teams. This allows for two things; designing products to be as robust as possible in terms of minimising or mitigating any financial crime risk, and the encouragement of a good compliance culture. By including the relevant compliance teams within the product development stages, FinCrime becomes an integral part of the company, not just a tick-box exercise at the end of the product development lifecycle.

FFE

The FinTech FinCrime Exchange (FFE) was established in January 2017 as a joint partnership between FINTRAIL and the Royal United Services Institute (RUSI). The FFE is a free forum that brings together a global network of FinTechs to discuss financial crime and the shared threats faced by all major FinTech hubs, collaborate on best practices, and share information and insight on an ongoing basis. The global FFE community gives its members not only a trusted place to exchange information, but also access to an increasingly far-reaching network of resources and perspectives. By sharing information on criminal typologies and controls, members help to strengthen the sector's ability to detect and counter the global threat of financial crime.

The FFE hosts monthly meet-ups in the UK and bi-monthly meet-ups in Singapore, New York and San Francisco. During these global meetings, RUSI gives an update on their own research, selected FFE members give a short presentation based on the theme of the month, and to round off there is a typologies discussion led by the FFE members. During the typologies discussion, members can share any new findings since the previous meet-up, present new financial crime trends they are seeing and what they look like in practise, and discuss new regulatory developments. These meet-ups also provide the chance for FFE members to ask the community any questions they might have. Members are granted access to an instant messaging platform connecting them globally to other FFE members, where they can post enquiries, best practices, articles, job opportunities and anything else of interest. This space gives members who weren't able to attend a meeting another channel to contribute with the ongoing collaboration efforts. Further, catering to the needs of the members, the FFE and FINTRAIL have already built strong relationships with partners such as the Metropolitan Police, City of London Police, HMRC, National Crime Agency, and Europol. This is evidenced very clearly by the FFE acting as a bridge between law enforcement and the wider FFE community sending

out Data Protection Act (DPA) requests to be distributed between members.

As an established group of FinTechs, the FFE are privy to certain government initiatives. One such initiative is the Economic Crime Plan whereby the government is reaching out to different stakeholders to establish an Innovation Working Group. The FFE community has a unique opportunity to contribute to this initiative and help to decide where best to focus the initial efforts of this group and to determine common barriers to innovation in the AML space. This is a direct demonstration of collaboration in motion with the potential for future improvement of controls.

The FFE network is growing rapidly, with members continuing to engage in effective collaboration towards the fight against financial crime. In 2020 FINTRAIL and the FFE aim to keep the momentum going, with plans in the next year to increase and improve collaboration across the community. Some of the areas of focus are:

- Increased sharing of typologies amongst the growing member group
- Hosting over 20 meet-ups across the three regions, as well as a conference to bring together the global community
- The launch of a podcast to dive into topics that are not covered during the meet-ups
- Establishing an Expert Working Group which will involve quarterly meet-ups of senior financial crime leaders across the FinTech and financial services industry to delve into key topics affecting their institutions and map out a common way forward

RDC

RDC was founded as a screening utility in 2002 by 20 of the world's largest financial institutions. These organisations came together following the enactment of the USA PATRIOT Act to develop a solution that could help tackle evolving anti-money laundering rules and provide more effective financial crime controls. Over the past two decades, close collaboration with banks and FinTech companies has remained central to RDC in shaping its customer screening solution.

RDC has also established relationships with several NGOs and trusted industry bodies in order to gather unique sources of financial crime risk information that augment its risk database. These sources help identify individuals and businesses linked to various crimes that may have otherwise gone undetected, and through RDC's screening engine can be flagged to financial institutions around the world.

Today, RDC's risk database draws relevant information from over 120,000 sources including global adverse media. As well as providing comprehensive financial crime risk coverage, this information is also being used to extract unique insights into financial crime trends and emerging risks, which is shared with financial institutions through partnerships such as the FFE. These insights help shine a light on topics relevant to anyone who is part of the global fight against financial crime and can help raise awareness and improve understanding of underlying crimes such as modern slavery.

Key takeaways

- **Although the industry is playing catch-up, it is better late than never.** Whilst there have been some past efforts, there is still a lot of work to do to ensure effective and efficient collaboration. The private sector has a critical role to play in supporting law enforcement efforts against criminality in all its forms, and the public sector has an equally critical role to play in involving the different segments. However, many efforts so far have generated good discussions and talking points, but have had little practical impact. But it's never too late: to avoid this pattern as a collective community we need to think outside the box and try out new concepts to ensure actions are generated from our efforts.

- **Engage in the communities that work for you and your company**. Some of you may already have found a community or collaboration forum that works for you - if so stick with it, engage, and help to improve that ecosystem. A great example of this is the FFE. If you are already a member, or want to become one, reach out, remain an active member of the community, engage in discussions, suggest new members, lead talking points at meet-ups or on the Slack channels, and continue to help in the fight against financial crime.

- **Financial crime cannot be solved in a siloed FinCrime department.** Neither should all of the responsibility to communicate cross-department be put onto the FinCrime team. Vital intelligence can be shared within the same company across departments, which is something that must be encouraged and continued. The wider fight against crime - whether it's fraud, cybercrime, or money laundering - will be impossible if each department acts independently.

Thank You

www.fintrail.co.uk
www.rdc.com

FINTRAIL

rdc
Smarter Screening