The Banker
GLOBAL FINANCIAL INTELLIGENCE SINCE 1926
13 AUGUST 2021

Transactions & Technology

Teaming up to fight financial crime

Tackling money laundering, terrorist financing and other financial crime is a difficult chore for banks. However, public–private partnerships, technology solutions and new approaches are beginning to make a difference.

Anita Hawser

In June, one of the most significant operations in the Australian Federal Police's (AFP) 40-year history, called Operation Ironside, resulted in more than 500 charges being laid against the Australian mafia and Asian criminal syndicates involved in industrial-scale illicit drug trafficking. The three-year covert operation, which arrested kingmakers and seized more than $45m in cash and assets, saw unprecedented levels of co-operation between the AFP, the US Federal Bureau of Investigation, Australia's financial intelligence unit (FIU) — the Australian Transaction Reports and Analysis Centre (Austrac) — and major domestic banks.

During the operation, Austrac worked alongside the banks to share information between AFP investigators and the banks in almost real time, a spokesperson told *The Banker*. Since setting up the Fintel Alliance in 2017, a public-private partnership bringing together government, law enforcement and the financial sector to combat and disrupt money laundering and terrorism financing, Austrac says it has contributed financial intelligence to a significant number of taskforces and law enforcement outcomes against crimes involving money laundering, child sexual exploitation, tax evasion and fraud.

> BANKS HAVE ALL THESE FANCY TRANSACTION MONITORING SYSTEMS, BUT THEY'RE NOT PICKING UP THE GUY SAT IN MALAYSIA MOVING MONEY TO NIGERIA THROUGH A UAE BANK ACCOUNT

Zoe Newman, Kroll

For the banks, the alliance is an opportunity to see the results of the work their financial crime teams do day in, day out, and to rewrite the narrative, which often casts them — not the criminals — in the spotlight. While everyone wants to catch the bad guys, or at least prevent the money laundering that fuels their activities, financial institutions, law enforcement and regulators are not always in step with another.

Mounting fines

In 2020, Australia's second largest bank, Westpac, agreed to pay a $1.3bn civil penalty — the largest fine in Australian corporate history — for more than 23 million breaches of anti-money laundering (AML) laws, including the failure to properly report more than 19 million international funds transfer instructions (worth more than $11bn) to Austrac. In June this year, National Australia Bank revealed it is under investigation for "suspected serious and ongoing breaches of AML and counter-terrorism laws". But how can banks work alongside regulators and law enforcement one minute, helping them crack transnational crimes such as drug, human and wildlife trafficking, only to be hauled over the coals the next for not having adequate AML and counter-terrorism financing (CTF) programmes or sanctions screening controls?

"One of the biggest shortcomings of AML programmes is the lack of a strong compliance culture in financial institutions," says Fatih Coşkun, chief executive and founder at Sanction Scanner, an AML compliance software company. "A strong culture of compliance has to start at the top and permeate the organisation until it reaches every staff member, but this is not usually the case. Senior managers often focus on compliance and AML to avoid regulatory penalties without creating an AML culture. In addition, an incompetent or uninformed compliance manager can harm a financial institution."

Despite the hefty fines levied against banks for non-compliance with AML/CTF and sanctions screening requirements, most banks end up reaching non-prosecution agreements with regulators. "The regulators don't take a bank's license away, which is a fatal error," says former money launderer and now financial crime consultant Kenneth Rijock. "Every five to 10 years, the banks get hit with a penalty and move on."

Austrac, which oversees compliance of

banks, credit unions, non-bank financial institutions, remittance, gambling services providers and digital currency exchanges with Australia's 2006 AML and CFT Act, say sit does not hesitate to take appropriate and proportionate action where non-compliance is identified. "The type of action taken needs to reflect the nature of the breaches, any harm resulting from them and actions required to make entities compliant," an Austrac spokesperson told *The Banker*.

One of the remedial actions banks have taken after being hit with a hefty fine is to employ ex-law enforcement officers to bring a different skillset to bear in their financial crime teams. "Banks really want to challenge the way they are seen and be good corporate citizens, so they've started reaching out to people with my background," says Nick Lewis, group head, financial crime intelligence and investigations and government relations at Standard Chartered Bank. Mr Lewis leads a team of almost 100 financial crime investigators at the bank, working on cases across more than 50 countries.

Despite past AML and sanctions failings, which saw Standard Chartered agree to pay a combined $1.1bn fine to the US and UK regulators in 2019, Mr Lewis says the chief executive and board were upfront about their desire to fight financial crime when he joined the bank in 2016. "If I didn't think they were serious, I wouldn't stay," he says. "We have a robust relationship with regulators around the world, who will tell us if we are doing something inappropriate. We often get a chance to fix things, but sometimes stuff comes completely out of the blue and you have to take it on the chin."

Striking a balance

With the movement of money, and the speed with which that happens, there is a tolerance by lawmakers that things will go wrong, says Mitch Trehan, UK head of compliance and money laundering reporting officer at Banking Circle, a financial infrastructure provider. "In practice, fighting financial crime is about striking a balance between identifying illegal behaviour and not slowing e-commerce and payments down, which would be detrimental for society at large," he says.

Having been in the fighting financial crime game for 20 years, Mr Trehan says that conduct, culture and awareness have improved, but that does not mean there are no outliers. "Fines will still happen, but I'm hopeful that things can get even better by using technology." One of the challenges, he says, is that smaller firms are not implementing the control environments found in larger firms. LexisNexis Risk Solutions estimates financial institutions spent a staggering $213.9bn on financial crime compliance in 2020, with most of that coming from the coffers of mid-to-large-sized institutions in the US and western Europe.

John Tobon, special agent in charge for Homeland Security Investigations in Honolulu, whose 20-year career spans numerous high-profile money laundering investigations targeting transnational criminal organisations, says compliance officers within banks have the toughest job. "They have to go and tell the business side, 'You can't do that'. But the business side says, 'Wait a minute, this is going to bring us a lot of profit'."

Banks are in the business of making money, says Mr Tobon. So too are the criminals, and when it comes to figuring out how to launder their money or make it look legitimate, he says they spend zero dollars on research and development.

"Tax avoidance and asset protection schemes — these methods have been created by legitimate accountants, bankers and attorneys, but have been adapted by criminal organisations to move and launder their funds, often without the knowledge of the legitimate professionals. Now with the internet, distances are shortened and money launderers can leverage technology to create a wider customer base. They don't need a fancy office. They can stay at home and do it," he explains.

The innovation race

Money launderers are constantly innovating, says Mr Rijock. If there is a problem with a bank, they move on to non-bank financial institutions. If that is too time consuming, they target Fortune 500 companies. "They are much more dynamic than people in compliance," he says. "They stay up nights and weekends coming up with new schemes."

Zoe Newman, co-head of the global financial investigations practice at Kroll, a provider of governance, risk and transparency services, says fraudsters or money launderers behave more like large international corporations, opening corporate entities and accounts around the world to manage international movements of cash. To catch them, she says banks need to look not just at the transaction, but at how illicit monies are moving across different jurisdictions. "Banks have all these fancy transaction monitoring systems (TMSs), but they're not picking up the guy sat in Malaysia moving money to Nigeria through a UAE bank account," she says. "They only see a small piece of the jigsaw. One of the biggest issues is that people can only launder money if they can open accounts. The red flag needs to be raised at the point of account opening and considered once the account starts operating."

> LEGACY TRANSACTION MONITORING SYSTEMS DO A TERRIBLE JOB OF IDENTIFYING CRIMES

Phil McLaughlin, QuantaVerse

Stuart Davis, executive vice-president and global head of financial crime and risk management at Scotiabank, says most banks have pretty good know-your-customer (KYC) solutions. "But KYC only goes so far. We're not really going to know whether a customer is likely to launder money until they start transacting, so we have to see who they're transacting with and the amounts of money involved." He says fighting financial crime is like looking for a needle in a haystack of needles. There are a multitude of ways to launder money, and identifying the patterns indicative of crimes fuelled by money laundering is challenging.

While the bulk of money laundering still occurs in cross-border transactions that are disguised as legitimate, the systems banks use to detect suspicious transactions are unreliable. On average, across most banks, Mr Davis estimates that 97-99% of alerts in TMSs are false positives. Every alert must be thoroughly reviewed, however. Banks are constantly innovating to reduce the rate of false positives. When it comes to matching customers to names on government sanction lists, Scotiabank says it has reduced its rate of false positives by 90% using a combination of innovation and technology.

"Legacy TMSs do a terrible job of identifying crimes," says Phil

John Tobon, Homeland Security

McLaughlin, chief information officer at QuantaVerse, a financial crime software vendor that uses artificial intelligence (AI) and machine learning to identify financial crimes that have gone undetected by these systems. "TMSs look at a small amount of transactional data and have simple rules that detect potential financial crimes. My motivation is to deliver new and better technologies that solve the problem in the most effective way," he says. "If we help a bank catch more bad guys, that's a win. That could be a human trafficker or a terrorist financier that's been thwarted."

'Fight financial crime with AI' is the latest mantra in the financial services industry. But Ms Newman says it is no substitute for good old-fashioned investigative legwork. "Money laundering can create an explosion of transactions. The hard bit is identifying the money laundering ring. Is it one, two or three that are controlling these accounts? That is where the human element comes in, looking at what emails are used, IP addresses and what jurisdiction they're based in."

The reporting issue

An increasing number of people with a law enforcement background have joined banks' financial crime teams over the past six years, Mr Lewis says. "But no single strand on its own can be successful," he says. "Banks are trying to provide the best possible service they can to help law enforcement catch the bad guys, which at the end of the day is what financial crime compliance is about."

To some extent, however, financial institutions are hampered by the very system designed to help catch the criminals: the suspicious activity reporting (SAR) regime that exists in most countries. Financial institutions must report suspicious transactions, even if they cannot reach 100% certainty that something is suspicious. "Reporting transactions that we think are suspicious often results in defensive reporting," says Mr Lewis. "Very often we don't have enough information, but we still have to report it anyway. Yet, from what we know, about 90% of everything reported to law enforcement has limited value."

In Canada, Mr Davis says financial institutions must have reasonable grounds to suspect a transaction is suspicious before filing a suspicious transaction report (STR), known as SARs in other jurisdictions. But an organisation can file a "defensive STR", he adds, when they are close but cannot make a final determination. While transaction thresholds exist in most jurisdictions for suspicious transactions, Canadian financial insti-tutions are obliged to report any transaction, regardless of its value, if they have reasonable grounds to suspect it is something nefarious. "The question is what do FIUs do with all that information?" asks Mr Davis.

Ms Newman says FIUs are facing a deluge of SARs, but don't have the resources to investigate every one of them. The UK's National Crime Agency says its FIU receives more than 460,000 SARs a year. In 2019 alone, Financial Crimes Enforcement Network received more than two million SARs from financial institutions. "The regulated financial institutions need to be cleverer at leveraging data and querying it," she says, "and FIUs need to take a more proactive approach to identifying suspicious activity and to share this analysis back with the financial institutions."

A SAR, or STR, does not prove a crime has been committed. The onus is on FIUs and law enforcement to investigate it and build a case if one has. Mr Tobon says almost every investigation he is involved in uses Bank Secrecy Act (BSA) data reported by financial institutions, which includes information about potentially suspicious transactions and cash transactions over $10,000. "It is information we find in BSA reporting that leads us to open a financial investigation to parallel an existing investigation into some other type of criminal activity," he explains.

Working together

Instead of reporting everything, Mr Lewis says bank's FIUs would be more useful to law enforcement if they were able to focus more on discretionary financial crime activity, in areas that are a priority for law enforcement. That means determining the problems law enforcement are trying to solve and helping them understand the information banks have at their disposal. For example, in child sexual exploitation, banks can help law enforcement understand how people pay online for images of children and what type of entities are involved, he explains.

"We're all trying to achieve the same objective to identify bad actors, which brings financial crime risk to a particular institution," he says. With that in mind, Standard Chartered has a dozen or so public-private partnerships with third parties from industry, law-enforcement, non-governmental organisations and other entities, helping to combat the money laundering that fuels high-risk crimes, such as the illegal wildlife trade and human trafficking. Bank branch tellers are being trained to spot potentially suspicious transactions relating to the illegal wildlife trade.

"The game-changer is not tech-nology, but public-private partner-ships: governments, banks and law enforcement working together," says Mr Davis. One such initiative, Project Shadow, which was formed by the Financial Transactions and Reports Analysis Centre of Canada and the Canadian Centre to End Child Exploitation, aims to address the rise in online child sexual exploitation — something that increased by more than 50% during the pandemic.

Compared to tax evasion and drug trafficking, where large amounts are laundered, child sexual exploitation typically involves small amounts of money — $10 or $20 in the typical transaction. "But the impact we can make is dramatic," he explains. "We share typologies looking at how this small dollar transaction differs from this one, and from there you can start seeing patterns. We want to be known for our innovation and cutting-edge efforts to make sure AML keeps pace with the ever-changing pace of financial crime, especially in the world of pandemic-motivated criminal activity."

But when considering the scale of the problem — the UN estimates that $1.6tn, or 2.7% of global gross domestic product is laundered every year — the transnational fight against financial crime can seem overwhelming. "It takes an optimistic personality to do this job," says Mr Davis. "We're looking to do the best for people and make a difference. That's what motivates me to get out of bed every morning."

"It's like an old fashioned 15-round boxing match," says Mr Tobon. "You can lose a round, but that doesn't mean you're going to lose the fight. We're going back and forth here. Are criminal organisations laundering money every day? Absolutely — hundreds of millions [of dollars] at a time. But law enforcement has come a long way. If you look at what is being done at the global level with the UN, the creation of the Financial Action Task Force and stuff at the G7 level, these are all wins. The tide certainly seems to be moving in the direction of the good guys, as we raise awareness of the problem and the tools for fighting financial crime catch up with criminal activities."