ARTICLE

Battling Financial Crime & Terror Financing

Ideologically inspired violence will always be with us, but the threat can be reduced by better intelligence, enhanced security and disrupting the terrorist's money supply.

Despite the killing of Abu Bakr al-Baghdadi, the leader of the militant Islamic group ISIS, in a US special forces raid in Syria in October 2019, the organisation remains intact and a major threat. It is under serious pressure and losing territory across Syria and Iraq, but it is regrouping and re-planning its next steps in the region and further afield. It was ISIS that claimed responsibility for the London Bridge stabbings in November that killed two people, though it did not provide any evidence.

Terrorist groups are spawned by a broad range of ideologies, not just those based on religion. Proponents of terror come from many sectors of society – the extreme left, the extreme right, nationalists and, on a less violent scale, even animal rights activists.

Despite their differences the more dangerous groups have several key things in common – extreme viewpoints, violence and illegal methods of financing such as theft, kidnapping for ransom, fraud and money laundering. Combatting the financing of terrorism is therefore a major priority for governments around the world, a priority that is coordinated by the Financial Action Task Force (FATF), based in Paris.

FATF is an inter-governmental body set up 30 years ago. It has 39 members: 37 countries and two regional organisations (the European Commission and the Gulf Cooperation Council). Its sets standards and promotes legal, regulatory and operational measures to prevent money laundering, combat the financing of terrorism (CFT) and counter the financing of weapons of mass destruction, all of which are contained in its 40 "Recommendations". FATF monitors how closely its members follow these recommendations, which were first written in 1990 and have been updated several times since, the last in 2012.

Recommendation 1, for example, requires countries to assess the risks and apply a risk-based approach to AML and CFT. "Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively," it states.

Recommendation 2 is that countries should cooperate with each other on their AML and CFT policies, through their financial intelligence units (FIUs), law enforcement authorities, financial supervisors and other relevant bodies.

Recommendation 3 sets out how countries should criminalise money laundering; recommendation 4 requires countries to seize assets gained from money laundering or intended to be used to finance terrorism; and recommendation 5 sets out the basis on which countries should criminalise terrorist financing.

Some are specifically aimed at banks and other financial institutions. For example, recommendation 9 says countries should ensure financial institution secrecy laws "do not inhibit the implementation of the FATF recommendations". Recommendation 10 places customer due diligence (CDD) requirements on financial institutions which should be "prohibited from keeping anonymous accounts or accounts in obviously fictitious names"; and they should carry out CDD checks for any transaction over €15,000 or if "there is a suspicion of money laundering or terrorist financing".

Other recommendations require financial firms, among other things, to keep records of customers' transactions for at least five years, comply with additional measures for "politically exposed persons", and be especially vigilant in their correspondent banking relationships around the world.

Terrorist Financing Methods – Traditional and Emerging

FATF provides details on the traditional and emerging financing methods used by terrorists. Traditional techniques include individual donations, including from wealthy people; diverting funds from non-profit organisations such as charities; committing fraud, robbery and other crimes, with the proceeds usually laundered through the banking system to legitimise them; extortion; kidnapping for ransom; revenues from legitimate commercial enterprises; and state sponsorship.

An emerging method of financing is the use of self-funded foreign terrorist fighters (FTFs) who are join local militant groups, as happened recently in Syria and Iraq. If they come from wealthy Western countries they may have a regular source of cash from employment income, social security benefits and bank loans.

Other new techniques include fund raising through social media, including crowdfunding; online payments to transfer funds quickly and globally; cryptocurrencies to disguise the origin and destination of payments; prepaid cards to move money offshore with little risk of detection; and the exploitation of natural resources, such as oil and gas, in captured territories, to generate huge revenues, a method used by ISIS in the Middle East.

The EU Raises Its Game

FATF members have incorporated its 40 recommendations and related guidance into national legislation and regulations, In the European Union, for example, they have been introduced through legislation such as a series of anti-money laundering (AML) and terrorist directives. The 5th AML Directive is due to come into effect in January 2020.

The European Commission took a further step in July 2019 when it adopted a Communication and four reports to help member states and EU institutions combat money laundering and terrorist financing. The Communication, Towards a better implementation of the EU's anti-money laundering and countering the financing of terrorism framework, summarises the four reports.

The first report assesses the risks associated with money laundering and terrorist financing. The second assesses the recent high-profile money cases in the financial sector, the shortcomings in supervision and how to address them. The third stresses the need for reinforced cooperation between national financial intelligence units (FIUs), while the fourth looks at how central bank account registries within the EU could be interconnected to allow efficient data sharing and retrieval.

Banks Must Play Their Part

But what the authorities say and do is not enough on its own. The banks and other financial institutions through which terrorist finance is channelled must be able to interpret and implement the laws and rules in an operational environment. They must also be genuinely committed to fighting financial crime in all its forms, starting with the board of directors at the top, down to frontline staff dealing with customers.

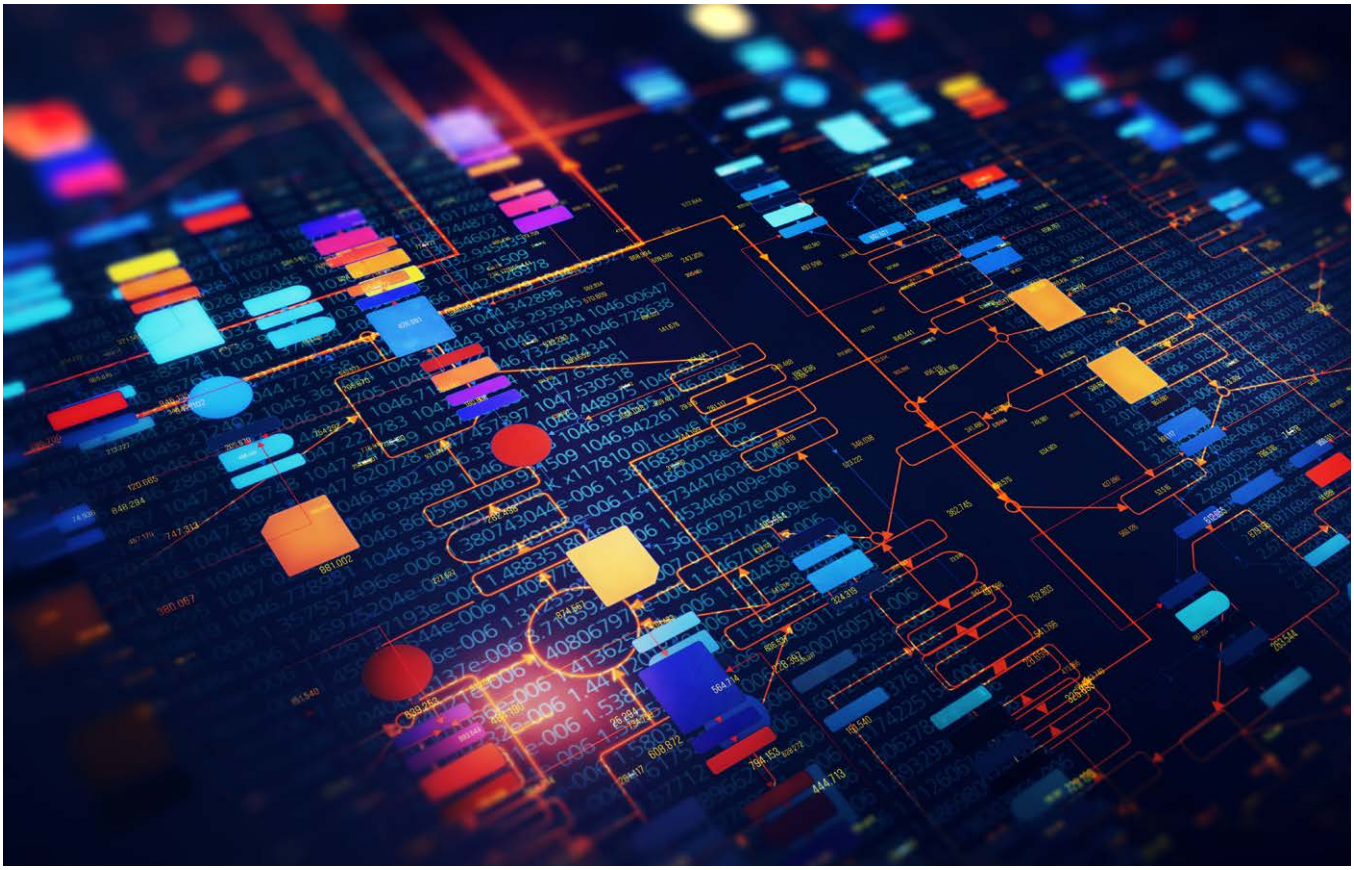
That is why the Wolfsberg Group was formed in 2000, an association of 13 global banks – including Bank of America, Barclays, Goldman Sachs and MUFG – to develop guidance for managing financial crime risks. The principles outlined in its Statement on the Suppression of the Financing of Terrorism have been closely observed by the banking industry since it was first published in 2002. Its most recent Country Risk Frequently Asked Questions document advises what data sources banks should use when assessing financial crime country risk (FCCR), including terrorist financing, when conducting their international business.

Industry associations like UK Finance, the American Bankers Association and the European Banking Federation are doing their bit to inform bankers of the risks and their obligations in combatting the financing of terrorist groups. UK Finance, for instance, runs courses on financial crime compliance, telling bankers what they must do to meet their responsibilities in this respect, including the prevention of money laundering and terrorist financing.

When the European Commission issued its Communication on AML and CFT in July 2019, the European Banking Federation responded by saying its members were "fully committed" in the fight against these crimes. It added that "for this fight to be effective we need to reduce fragmentation between national approaches while increasing cross-border cooperation in-and-outside the European Union", and there needs to be better information sharing between government bodies and banks.

Clearly there is no shortage of commitment from supranational bodies, national governments and financial firms to cut off the supply of money to violent groups. Yet these groups continue to find funds, continue to operate and continue to kill. Why is this?

It is because terrorists can be extremely clever and find ways round AML and CFT controls. Corrupt staff in banks might assist them or turn a blind eye. Negligent but otherwise honest staff may not follow correct procedures. Many banks have been slow to deploy the latest technology to detect and prevent suspicious transactions. Other banks' procedures and processes fail to comply with AML and CFT regulations.



Information Sharing is Key – Without Infringing Data Privacy Rights

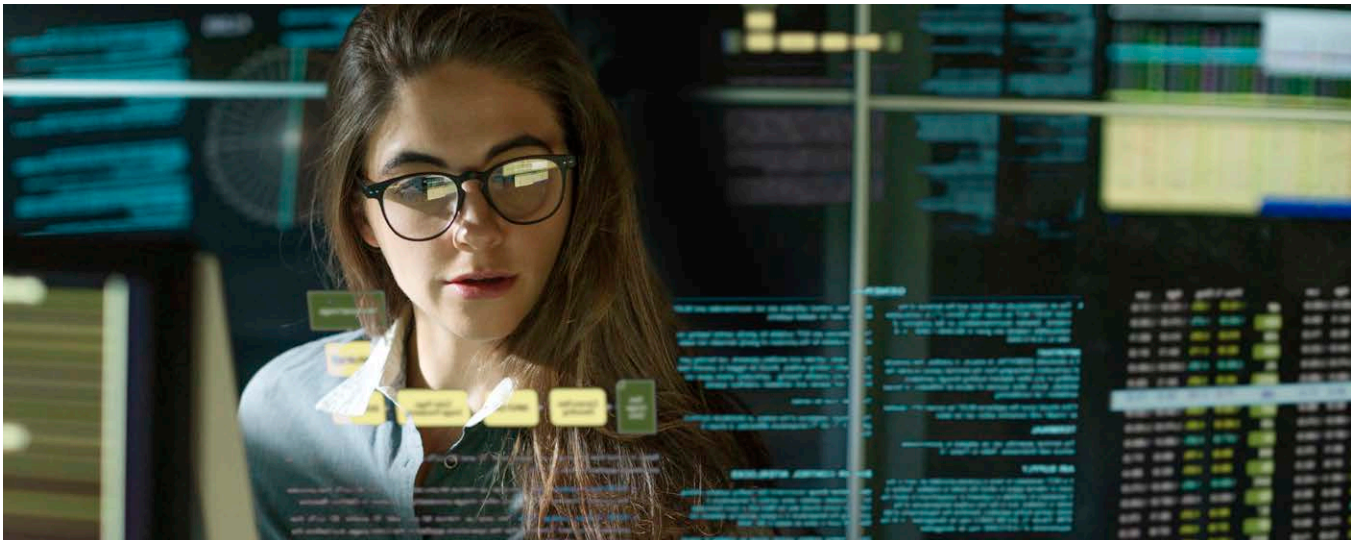
So what more can financial institutions do? A combination of measures is needed: better technological and procedural controls; more staff training; tighter regulatory compliance; engaging external help from forensic and litigation consultants like FTI Consulting to assist with compliance, risk management and investigations; and improved information sharing between banks and the authorities.

It is this last point that is perhaps receiving the biggest focus right now. The UK's Financial Conduct Authority organised a "TechSprint Demo Day" on global anti-money laundering and financial crime in August 2019. A TechSprint is a hackathon-style event, lasting several days, where technologists and subject matter experts collaborate intensively to solve specific problems using technology prototypes.

The Demo Day explored what could be done to encourage more and better sharing between financial firms, regulators and law enforcers. It showcased several possible technology solutions developed by teams of experts to allow data sharing to happen without breaking strict data privacy rules. Such rules are a serious impediment to organisations sharing information about someone's financial activities, but the prototype solutions demonstrated how "privacy enhancing technologies (PETs)" can be used to allow sharing in a legally compliant way and help detect financial crime. These technologies include homomorphic encryption, secure multi-party computation, zero knowledge proofs and trusted execution environments.

One solution uses PETs in conjunction with data analytics to allow a bank to view financial transactions stored in another bank's database and identify credible suspicions and stay within privacy laws. Another solution based on PETS allows a bank to check that a company or individual it is performing due diligence on has not raised concerns in another bank, again respecting privacy rules. A third solution allows a bank to process data in real-time to codify different crime topologies, and then share those topologies with other firms.

David Lewis, FATF's Executive Secretary, who was a judge at TechSprint, tells me that some people wonder why there is any point tracking terrorists' financial affairs when it is so easy for them to go out and kill someone. His response is two-fold. First, there is an expensively developed ideology behind every cheaply financed attack, so it is important to disrupt the funding of such ideologies.



Second, monitoring terrorists' bank accounts, even for small purchases like knives, or chemicals to make explosives, provides financial intelligence on what they are buying, who they are getting money from, and who they are providing money to. "Monitoring financial transactions to detect possible crimes but also gather information about what terrorists are doing and spending their money on is useful," he says.

The experience of attacks, like the Bataclan has been that financial transactions such as to hire cars and pay for overnight accommodation, including via pre-paid cards, has been useful in tracking the movements of terrorists and connecting them to other potential cells and terrorists.

Working Collaboratively

Whenever a terrorist attack takes place, whatever form it takes, the post-event investigation must include inquiries into all aspects of the perpetrators' financial affairs, with financial institutions working hand-in-hand and sharing data with law enforcement, financial intelligence units, regulators, forensic accountants and others.

Terrorism will never be eradicated. But the threat can be greatly reduced if public and private sector entities work collaboratively to cut off the terrorist's money supply.

Research Methodology

This research was conducted by FTI Consulting's Strategy Consulting & Research team in London via a CATI (Computer Assisted Telephone Interviewing) research methodology. Fieldwork was conducted from 29th October to 11th November 2014 involving n=50 organisations who supply retailers in the United Kingdom, representing a sum total of £11.8 billion in annual sales.

Please note that the standard convention for rounding has been applied and consequently some totals do not add up to 100%.
For more information on the research methodology, please email market.research@fticonsulting.com

ANDREW PIMLOTT
Senior Managing Director
+44 (0)20 3727 1285
andrew.pimlott@fticonsulting.com