# Cryptoassets, Social Media Platforms and Defence against Terrorism Financing Suspicious Activity Reports: A Step into the Regulatory Unknown

**Nicholas Ryder***

keywords to be inserted by the indexer

## Introduction

Almost two decades on from the al Qaeda terrorist attacks in September 2001 (9/11), the Financial War on Terrorism continues to gather pace. The international community led by the United Nations (UN), the Financial Action Task Force (FATF) and the European Union (EU) responded to these terrorist attacks by introducing a series of international counter-terrorism financing (CTF) legislative provisions. Collectively, these measures are referred to as the Financial War on Terrorism, which consists of five mechanisms: criminalisation, confiscation or forfeiture, asset freezing, a designated terrorism sanctions regime and the use of Defence Against Terrorism Financing Suspicious Activity Reports (DATF SARs).[1] These mechanisms, especially the sanctions regime, have been able to limit the funding avenues of some terrorist groups, such as al Qaeda.[2] Therefore, as terrorist fighters have been increasingly unable to secure enough funding via their traditional methods, they have had to turn towards other alternative sources. It has been argued by the FATF, that in order to continue its activities and to counter the five instruments of the Financial War on Terrorism and the Global Coalition Against Daesh,[3] the Islamic State of Iraq and the Levant (ISIL) has trained returning foreign terrorist fighters to use a wider range of funding streams.[4] Returning foreign terrorist fighters have been able to secure funding via the internet and social media platforms.[5] In particular, ISIL has posted numerous videos on You Tube [6] requesting

* Professor in Financial Crime, Bristol Law School, Faculty of Business and Law, University of the West of England, Bristol. I would like to thank Dr Noelle Quenivet, Processor Umut Turksen, Dr Alison Lui, Dr Colin King and the external reviewers for their helpful comments on early drafts of this paper. I would also like to thank Connor Bayley (Cardiff University) for his invaluable work as a research assistant on this project.

[1] See N. Ryder, *The Financial War on Terror: A Review of Counter-Terrorist Financing Strategies since 2001* (Abingdon: Routledge, 2015), pp.30–62.

[2] See C. Michaelsen, "The Security Council's Al Qaeda and Taliban Sanctions Regime: 'Essential Tool' or Increasing Liability for the UN's Counterterrorism Efforts?" (2010) 33 *Studies in Conflict & Terrorism* 448; and J. Gurule, *Unfunding Terror: The Legal Response to the Financing of Terror* (Cheltenham: Edward Elgar, 2008).

[3] See The Global Coalition Against Daesh 'Mission' (n/d), *https://theglobalcoalition.org/en/mission/#tackling-daeshs-financing-and-funding* [Accessed 17 September 2020].

[4] Financial Action Task Force, *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* ( 2015), pp.4, 7 and 10.

[5] Financial Action Task Force, 2015), *Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)* (2015), pp.4, 7 and 10; and United Nations Office on Drugs and Crime, *The use of the Internet for Terrorist Purposes* (2012).

[6] See generally A. Atwan, *Islamic State: The Digital Caliphate* (California: University of California Press, 2015).

advice on the production of cryptoassets.[7] The FATF stated that the funding requirements of foreign terrorist fighters presents an unprecedented threat because they only require modest amounts of funding.[8] Online sources of finance have become a growing funding avenue of choice for terrorism financiers, and this article presents evidence to support this contention.[9] The unprecedented expansion of cryptoassets and social media platforms as a terrorism-funding model has resulted in several states suffering from an unprecedented and concentrated wave of international terrorism. Thus, the importance of an in-depth understanding of the working of this new model cannot be stressed enough. As little has been written on the subject. Therefore, the first aim of this article is to offer an enhanced understanding of this new model of terrorism financing. More importantly, it seems that the measures stemming from the five aforementioned mechanisms appear ineffective in limiting the ability of terrorism financiers to accrue funding via cryptoassets and social media platforms.[10] A worrying fact is that the Financial War on Terrorism mechanisms seem unable to counteract some of the developing funding models. In order to tackle the threat posed by returning foreign terrorist fighters, the UN Security Council adopted Resolution 2178,[11] in which the UN

> "expresses its strong determination to consider listing pursuant to resolution 2161 (2014) individuals, groups, undertakings and entities associated with Al-Qaida who are financing, arming, planning, or recruiting for them, or otherwise supporting their acts or activities, including through information and communications technologies, such as the internet, social media, or any other means".[12]

Among the mechanisms used to tackle terrorism financing, one has proven efficient against money laundering and some traditional methods of terrorism financing: DATF SARs.[13] As they have so far been considered as one of the most appropriate mechanisms to deal with terrorism financing, it is argued that they are likely to be the most effective in the fight against these new funding models. The second aim of this article is thus to verify this hypothesis, using DATF SARs in the United

[7] Financial Action Task Force, *Financing of the Terrorist Organisation Islamic State* (2015), p.25. There is no universally agreed definition of a cryptoasset, and they have been referred as virtual currencies and cryptocurrencies. Virtual currencies are defined by the Fifth Anti-Money Laundering Directive (5MLD) as "a digital representation of value that is … not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically". See Directive (EU) 2018/843 of the European Parliament and of the European Council, art.1(3)(d).

[8] Financial Action Task Force, *Emerging Terrorist Financing Risks* (2015), pp.22–24.

[9] Financial Action Task Force, *Emerging Terrorist Financing Risks* (2015), pp.22–24.

[10] See M. Campbell-Verduyn, "Bitcoin, crypto-coins, and global anti-money laundering governance" (2018) 69 *Crime, Law and Social Change* 283, 305 and K. Choo, "Cryptocurrency and virtual currency: corruption and money laundering/terrorism financing risks?" n D. Cheun, *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data* (Amsterdam/Boston: Academic Press, 2015), pp.283–307.

[11] United Nations, "Resolution 2178 Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters" (24 September 2014), *https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29* [Accessed 17 September 2020].

[12] United Nations, "Resolution 2178 Condemning Violent Extremism, Underscoring Need to Prevent Travel, Support for Foreign Terrorist Fighters" (24 September 2014), para.7, *https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/2178%20%282014%29* [Accessed 17 September 2020]. For a more detailed discussion see The United Nations, "Foreign Terrorist Fighters implementation plan" (n/d), *https://www.un.org/counterterrorism/ctitf/en/foreign-terrorist-fighters-implementation-plan* [Accessed 28 February 2020].

[13] See generally National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2018* (2018).

Kingdom (UK).[14] Unfortunately, this article clearly demonstrates that while the current DATF SARs framework is indeed suitable for traditional methods of terrorism financing, it is unable in its current shape to tackle this new funding model. The article thus contends that reforming it by notably extending it to payments made via cryptoassets and social media platforms would greatly enhance its strength against new methods of terrorism financing, though it is not a panacea and a new approach is warranted. The article suggests further legal avenues to stave off such terrorism funding. In particular, it advocates that the voluntary exchange of information model, as developed by the Joint Money Laundering Intelligence Task Force (JMLIT), should be extended to cryptoasset providers and social media platforms. Therefore, the article is divided into four parts. The first part of the article identifies a new and emerging terrorism funding model via cryptoassets and social media platforms—the Social Networking Funding Model. The second part provides an overview of the scope of DATF Sand discusses their operation under the Terrorism Act 2000. The third part highlights how the Social Networking Funding Model exploits the loopholes in the DATF SARs regime as identified in the second part of the article. This part exposes the weaknesses in the application of DATF SARs to cryptoassets and social media platforms, and criticises the efforts by HM Government (HMG) to regulate cryptoassets. The final part of the article critically appraises the potential extension of DATF SARs to both cryptoassets and social media platforms and advocates the extension of the voluntary exchange of information model.

## Terrorism financing the Social Networking Funding Model

The first part of the article identifies a new terrorism financing model that involves a combination of cryptoassets and social media platforms—the Social Networking Funding Model. Traditionally, terrorists have relied on two sources of funding: state and private sponsors.[15] State-sponsored terrorism involves governments providing logistical and financial support to terrorists, or governments even conducting acts of terrorism against their own citizens.[16] As of November 2019, the United States (US) Department of State has identified four state sponsors of terrorism—the Democratic People's Republic of Korea, Iran, Sudan and Syria.[17] However, since the instigation of the Financial War on Terrorism, there has been a decline in state-sponsored terrorism, and terrorists have been forced to modify and adapt their funding models, and it is more likely that terrorists will receive

[14] This article adopts a case study approach that is "particularly well suited to new research areas or research areas for which existing theory seems inadequate". See K.M. Eisenhardt, "Building theories from case study research" (1989) 14 *Academy of Management Review* 532, 548–549. A case study has been defined as "an intensive study of a single unit with an aim to generalise across a larger set of units". See J. Gerring, "What is a case study and what is it good for?" (2004) 98 *American Political Science Review* 341, 342.

[15] See, generally, Financial Action Task Force, *Terrorist Financing* (2008).

[16] For a more detailed discussion, see US Department of State, *County Reports on Terrorism 2017* (2018). For a more detailed discussion on efforts to tackle state-sponsored terrorism, see D. Byman and and S. Kreps, "Agents of Destruction? Applying Principal-agent Analysis of State Sponsored Terrorism" (2010) 11 *International Studies Perspectives* 1.

[17] The United States Secretary of State is permitted to designate a country as a state sponsor of terrorism by virtue of powers provided by s.6(j) of the Export Administration Act (1979), s.40 of the Arms Export and Control Act (1976), and s.620A of the Foreign Assistance Act (1948). For an early discussion of state-sponsored terrorism, see G. Roberts, "Self-help in Combating State Sponsored Terrorism: Self-Defence and Peacetime Reprisals" (1987) 19 *Case Western Reserve Journal of International Law* 243.

funding from private sponsors or donors.[18] The demise of state-sponsored terrorism was acknowledged by Hardouin, who stated that

> "state sponsorship [terrorism] has been decreasing (not disappearing) as terrorist groups find it harder to obtain state support, and states that are not respecting international standards are less willing to risk exposure to severe international sanctions".[19]

It has been suggested that there are two factors that have contributed towards the decline in state-sponsored terrorism. First, "there are fewer states engaged in supporting terrorists".[20] Second,

> "the new global terrorist networks have arisen that no longer rely on states for support. Instead, terrorist groups rely more and more on networks of private donors and supporters and direct engagement with criminal activities to raise funds".[21]

Further evidence of the shift away from state-sponsored terrorism towards private donors was highlighted by The National Commission on the Terrorist Attacks upon the United States, which concluded that al-Qaeda relied on finances raised by private benefactors and not from state sponsors.[22] Additionally, the Inter-governmental Action Group Against Money Laundering in West Africa noted that Boko Harem has been partly financed through private donors and misapplied charitable donations.[23] The increased use of private financial benefactors was also highlighted by the US Department of Treasury, which conducted an analysis of terrorism financing cases and prosecutions between 2001 and 2014 and determined that approximately one-third of the cases involved financial support from private donors.[24] The FATF stated that,

> "wealthy private donors can be an important source of income for some terrorist groups. For example, the FATFISIL report acknowledges that ISIL has received some funding from wealthy private donors in the region".[25]

Terrorists are able to access funds through a spectrum of mechanisms including, inter alia, kidnap for ransom, robbery, drug trafficking, fraud, the control of oil reserves, the sale of ivory, abuse of natural resources, misapplied charitable donations and the internet.[26] More recently, terrorists have obtained finances from a wide range of emerging sources, including cryptoassets and social media platforms. The extent to which cryptoassets are exploited for money laundering

[18] A. Acharya, *Targeting Terrorist Financing: International Cooperation and New Regimes* (London: Routledge Cavendish, 2009), p.7.

[19] P. Hardouin, "Banks governance and public-private partnership in preventing and confronting organized crime, corruption and terrorism financing" (2009) 16 *Journal of Financial Crime* 199, 205.

[20] See A. Richard, *Fighting Terrorist Financing: Transatlantic Co-operation and International Institutions* (Baltimore, MD: Centre for Transatlantic Relations: John Hopkins University, 2005), p.6.

[21] Richard, *Fighting Terrorist Financing* (2005), p.6.

[22] See National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report* (New York: Norton and Co. 2004), p.172. For a more detailed discussion on how al-Qaeda is funded see V. Comras, "Al Qaeda and funding to affiliated groups" (2005) 4 *Centre for Contemporary Conflict* 1.

[23] Inter-governmental Action Group Against Money Laundering in West Africa, *Threat Assessment of Money Laundering and Terrorist Financing in West Africa* (2010), p.94.

[24] United States Department of Treasury, *National Terrorist Financing Risk Assessment 2015* (2015).

[25] Financial Action Task Force, *Emerging Terrorist Financing Risks* (2015), p.13.

[26] Financial Action Task Force, *Emerging Terrorist Financing Risks* (2015), p,13.

and/or terrorism financing is impossible to determine.[27] Yet, it has been estimated that between £3 and 4 billion is annually laundered via cryptoassets within the EU,[28] and that "cryptocurrencies have become the favoured detergent for criminals to launder money".[29] However, even if this figure is accurate, it only represents a small percentage of the money laundered within the EU.[30]

The association between cryptoassets and financial crime has been illustrated by several investigations and subsequent criminal convictions obtained by Law Enforcement Agencies (LEAs) in the US and UK. One of the first cases surrounding the illegal use of cryptoassets was "Silk Road", an online black market platform that was used by organised criminals and terrorists via the dark web.[31] Silk Road was able to

> "generate total sales revenue of approximately $1.2 billion and approximately $80 million in commissions … and hundreds of millions of dollars were laundered from these illegal transactions".[32]

The users of Silk Road were able to protect their anonymity by using "The Onion Router" and virtual private networks.[33] However, these platforms prevented anonymous payment methods. Ross Ulbriant was able to solve this problem by using Bitcoin, which, via Blockchain, provided a mechanism that was able to confirm if the payments had been made and received.[34] The website was launched in February 2011 and eventually closed by the Federal Bureau of Investigation (FBI) in 2013 following the arrest of its founder, Ross Ulbricht, who was convicted of money laundering and computer hacking in February 2015.[35]

The second example that illustrates the association between cryptoassets and financial crime is "Liberty Reserve", a Costa-Rican digital currency service that attracted over one million users. Liberty Reserve advertised itself as the internet's "oldest, safest and most popular payment processor… serving millions all around [the] world".[36] The users of Liberty Reserve were required to provide personal details, including their names, date of birth and e-mail addresses, but in most cases, the information provided was false. The account holders would "convert" their cash into Liberty Dollars following an instantaneous transfer, and the cash would

[27] For a detailed discussion on the calculation of money laundering, see B. Unger, *The Scale and Impacts of Money Laundering* (Cheltenham: Edward Elgar, 2007).

[28] Financial Conduct Authority, "Cryptoassets Taskforce: final report" ( 2018), p.34.

[29] V. Marria, "How Cryptocurrencies Are Empowering Cyber Criminals" (4 February 2019, *https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals/#690a4eb237c5* [Accessed 18 September 2020].

[30] HM Treasury Select Committee, "Oral Evidence: Economic Crime, HC 940 Donal Toon National Crime Agency" (4 July 2018, *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/economic-crime/oral/86570.pdf* [Accessed 18 September 2020].

[31] For a more detailed discussion of the "Dark Web", see M. Shillitto, "Untangling the 'Dark Web': An Emerging Technological Challenge for the Criminal Law" (2019) 28 *Information & Communications Technology Law* 186.

[32] Financial Action Task Force, *Virtual Currencies: Key Definitions and Potential AML/CFT Risks* (2014), p.10.

[33] TOR is a free and open source software that enables its user to conduct anonymous communication and other internet usage from any surveillance or online analysis.

[34] Blockchain is a system in which a record of financial transactions made by Bitcoin and other cryptoassets are maintained across several computers that are linked in a peer-to-peer network.

[35] United States Department of Justice, "Ross Ulbricht, A/K/A 'Dread Pirate Roberts',Sentenced In Manhattan Federal Court To Life In Prison'" (29) May 2015), *https://www.justice.gov/usao-sdny/pr/ross-ulbricht-aka-dread-pirate-roberts-sentenced-manhattan-federal-court-life-prison* [Accessed 18 September 2020]. Ulbricht was sentenced to two life sentences, which were upheld by the Court of Appeals for the Second Circuit in May 2017. In June 2018, the US Supreme Court declined to consider Ulbricht's appeal. See *Ulbricht v United States* (28 June 2018).

[36] *BBC*, "Liberty Reserve Digital Cash Chief Jailed for 20 Years" (9 May 2016), BBC, *https://www.bbc.co.uk/news/technology-36247289* [Accessed 18 September 2020].

be converted back into useable currencies. Liberty Reserve would charge its users approximately $3 per transaction, and operated on an unprecedented scale: it included over 200,000 users in the US and conducted over 55 million online transactions, "almost all of which were illegal. It [Liberty Reserve] had its own virtual currency, Liberty Dollars, but at each end, transfers were denominated and stored in fiat currency".[37] The Liberty Dollar was a private currency produced in the US that was issued as "electronic money" or "e-money".[38] Liberty Reserve has been described as the largest online money laundering cases in US history and it was eventually closed by the US Department of Justice (DoJ) after its co-founder, Arthur Budovsky, was convicted of laundering between $250 million and £550 million and sentenced to 20 years imprisonment in May 2016.[39]

The connection between cryptoassets and financial crime is illustrated by the third example—Western Express International, a virtual currency exchanger and unregistered money transmitter. Here, 16 members of the Western Express International Cybercrime Group were convicted for their role in numerous fraudulent schemes. Gang members stole over 100,000 credit card numbers and personal identities, which were sold and paid for with e-Gold and Webmoney.[40] Egor Shevelev used multiple internet forums to claim that he had millions of stolen credit cards and account numbers that were for sale. Douglas Latta and Anna Ciano agreed to purchase 1,000 of the credit cards and account numbers from Egor Shevelev by an online currency, that was difficult to trace. In February 2013, Egor Shevelev pleaded guilty to money laundering, fraud and conspiracy charges and was sentenced to 14 years' imprisonment.[41] One of the most recent examples relates to the alleged misconduct of Danske Bank, which is under investigation by authorities in the EU and the US for suspected money laundering (exceeding $230 billion between 2007 and 2015) via cryptoassets.[42] This has been referred to as the largest alleged money laundering scandal involving a bank and cryptoassets. As a result, Danske Bank's CEO, Thomas Borger, resigned and stated that "it is clear that Danske Bank has failed to live up to its responsibility in the case of possible money laundering".[43] Furthermore, regulators in Estonia have compelled Danske Bank to close its offices and the bank has agreed to end most of its business in Latvia, Lithuania and Russia.[44]

[37] Financial Action Task Force, *Terrorist Financing* (2008), p.10.

[38] E-money has been defined by the European Central Bank as "an electronic store of money value on a technical device that may be widely used for making payments to entitles other than the e-money issuer". See European Central Bank, "Electronic Money" (n/d), *https://www.ecb.europa.eu/stats/money_credit_banking/electronic_money/html/index.en.html* [Accessed 18 September 2020].

[39] United States Department of Justice, "Liberty Reserve Founder Arthur Budovsky Sentenced In Manhattan Federal Court To 20 Years For Laundering Hundreds Of Millions Of Dollars Through His Global Digital Currency Business" (6 May 2016, *https://www.justice.gov/usao-sdny/pr/liberty-reserve-founder-arthur-budovsky-sentenced-manhattan-federal-court-20-years* [Accessed 22 September 2020].

[40] Financial Action Task Force, Financial Action Task Force, *Terrorist Financing* (2008), p.10.

[41] *United States v Shevelev* 2014 WL 495393.

[42] News BCT, "The $234 Billion Money Laundering Case at Danske Bank's Impossible in Bitcoin Ecosystem" (20 September 2018), *https://www.newsbtc.com/2018/09/20/danske-bank-money-laundering/* [Accessed 18 September 2020].

[43] Danske Bank, "Findings of the Investigations Relating to Danske Bank's Branch in Estonia" (19 September 2018), *https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018* [Accessed 18 September 2020]. For a more detailed review of this incident, see BRUNN & HJEJLE, *Report on the Non-resident Portfolio at Danske Bank's Estonian Branch* (2018), pp.11–14, 27, 34; and Economic Governance Support Unit, *European Parliament Money Laundering: Recent Cases from a EU Banking Supervisory Perspective* (2019), pp.4–6.

[44] Finantsinspektsioon, "Finantsinspektsioon Has Issued a Precept Requiring Danske Bank to Terminate its Activities in Estonia" (19 February 2019), *https://www.fi.ee/en/news/finantsinspektsioon-has-issued-precept-requiring-danske-bank-terminate-its-activities-estonia* [Accessed 18 September 2020]. The association between cryptocurrencies and

There are also several examples illustrating the association between cryptoassets and financial crime within the UK. For example, Thomas White, who took over the administration of Silk Road after it was closed by the FBI in 2013, continued to use the technology that had previously permitted its users to illegally purchase drugs, computing hacking software and other illegal products by using cryptoassets. White was convicted and sentenced to five years imprisonment for drug trafficking offences, money laundering and making a number of indecent images of children.[45] Furthermore, in August 2019, Grant West was convicted of fraud after he carried out numerous cyber-attacks on over 100 UK based companies. West attempted to defraud the companies by installing ransomware software on their computer systems and then demanding a ransom payment via Bitcoin to uninstall the illegal software.

As these examples illustrate, there is a clear link between technological innovation and financial crime. Now that the association between cryptoassets and financial crime has been illustrated, this should be taken seriously, even more so when cryptoassets and social media platforms are used to accumulate funding for terrorist purposes. For example, the Indonesian Financial Transaction Reports and Analysis Centre reported that ISIL had used Bitcoin for terrorism financing purposes.[46] In August 2015, a computer hacker demanded a ransom of two Bitcoins from a retailer in exchange for removing bugs from their computer system. The hacker was able to use the extracted data from the server to create a "kill list" of over 1,300 names of US government and military personnel that was provided to ISIL.[47] Another example of ISIL attempting to acquire funding via cryptoassets was Ali Shukri Amin, who was convicted and sentenced to 11 years and four months imprisonment for using the "internet to provide material support and resources" to ISIL.[48] Amin pleaded guilty and admitted to using his Twitter handle "@Amreekiwitness" to "provide instruction [to ISIL] on how to use Bitcoin … to mask the provision of funds to ISIL".[49] This case demonstrates that terrorism financiers are using both social media platforms and cryptoassets to provide support and resources to ISIL.[50] Another example of terrorism financiers exploiting cryptoassets was Zoobia Shahnaz, who was arrested by the FBI after attempting to transfer $62,000 worth of Bitcoin to ISIL. The DoJ alleged that Shahnaz had

> "engaged in a bank fraud scheme, purchased Bitcoin and other cryptocurrencies and laundered money overseas, intending to put thousands

money laundering has also been referred to by the Bank of International Settlements, the International Monetary Fund and the Federal Bureau of Investigation. See Bank of International Settlements Committee on Payments and Market Infrastructure, *CPMI Report on Digital Currencies* (2015), and the Federal Bureau of Investigation, "Bitcoin virtual currency: unique features present distinct challenges for deterring illicit activity" (2012).

[45] Crown Prosecution Service, "Dark web drug dealer jailed after rebooting world's biggest online drug marketplace" (12 April 2019), *https://www.cps.gov.uk/cps/news/dark-web-drug-dealer-jailed-after-rebooting-worlds-biggest-online-drug-marketplace* [Accessed 18 September 2020].

[46] Indonesian Financial Transaction Reports and Analysis Centre, *Indonesia National Risk Assessment* (2015), pp.70–72.

[47] Centre for New American Security, *Terrorist Use of Virtual Currencies — Containing the Potential Threat* (2017), p.12.

[48] United States Department of Justice, "Virgina man sentenced to more than 11 years for providing material support to ISIL" (28 August 2015), *https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil* [Accessed 18 September 2020]

[49] United States Department of Justice, "Virgina man sentenced to more than 11 years for providing material support to ISIL" (28 August 2015), *https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil* [Accessed 18 September 2020].

[50] United States Department of Justice, "Virgina man sentenced to more than 11 years for providing material support to ISIL" (28 August 2015), *https://www.justice.gov/opa/pr/virginia-man-sentenced-more-11-years-providing-material-support-isil* [Accessed 18 September 2020].

> of dollars into the coffers of terrorists … allegedly tried to launder virtual currency to bolster terrorists' dwindling financial support".[51]

The DoJ stated that Shahnaz had entered into a number of financial transactions designed to circumvent the transaction reporting obligations imposed by the Currency and Foreign Transactions Reporting Act.[52] Therefore, terrorists are "creating safe havens to raise funds hiding in the shadows of the dark net … using cryptocurrencies such as Bitcoin to generate funds".[53] The Jackson Society noted that an al-Qaeda-linked entity, al-Sadaqah, used a public channel on Telegram to campaign for Bitcoin funding.[54] Clearly, then, modern forms of technology, especially social media platforms, are used by terrorism financiers. More often than not, the payments made over the internet, the Dark Web or social media platforms involve small amounts of funding which do not raise suspicion. This section of the article has illustrated that terrorists have continued to develop new funding mechanisms by exploiting the anonymity provided by the dark web and cryptoassets. The article now moves on to illustrate how terrorism financiers have used cryptoassets with social media platforms.

The anonymity and speed provided by the internet is an appealing tool for terrorists to solicit financial donors. In evidence presented to the House Foreign Affairs Committee (Subcommittee on Terrorism, Non-proliferation, and Trade Subcommittee on the Middle East and North Africa) the Washington Institute for Near East Policy stated that some of terrorism fundraising was carried out in plain sight on online social media platforms.[55] The evidence referred to a video uploaded to YouTube in October 2016 by Abd Allah al-Muhaysini who "thanked Gulf donors for supporting jihadists in Syria":

> "As for the businessmen, and I will mention some of them, the ones who prepared these hundred rockets, may Allah reward them … I tell all the businessmen of the Muslims, this is your money now, fighting in the path of Allah".[56]

Further evidence of the association between social media platforms and terrorism financing is illustrated by the US Department of the Treasury, which in 2014

[51] United States Department of Justice, "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists" (14 December 2017), *https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists* [Accessed 18 September 2020].

[52] United States Department of Justice, "Long Island Woman Indicted for Bank Fraud and Money Laundering to Support Terrorists" (14 December 2017), *https://www.justice.gov/usao-edny/pr/long-island-woman-indicted-bank-fraud-and-money-laundering-support-terrorists* [Accessed 18 September 2020]. . In November 2018, Shahnaz pleaded guilty to providing material support to ISIL and faces up to 20 years' imprisonment. See United States Department of Justice, "New York woman pleads guilty to providing material support to ISIS" (26 November 2018), *https://www.justice.gov/opa/pr/new-york-woman-pleads-guilty-providing-material-support-isis* [Accessed 18 September 2020].

[53] M. Townsend, "Terrorists 'plot in shadows of the dark net', report warns" ( 8 April 2018), *The Guardian*, *https://www.theguardian.com/uk-news/2018/apr/08/terrorists-plot-shadows-dark-net-report* [Accessed 18 September 2020].

[54] The Jackson Society, *Terror in the Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies* (2018), p.42.

[55] K. Blumenstein-Katz, "The Washington Institute for Near East Policy 'Grading counterterrorism Co-operation with GCC states' — Testimony submitted to the House Foreign Affairs Committee Subcommittee on Terrorism, Nonproliferation, and Trade Subcommittee on the Middle East and North Africa" (26 April 2018), *http://www.washingtoninstitute.org/uploads/Documents/testimony/BauerTestimony20180426.pdf* [Accessed 18 September 2020].

[56] Blumenstein-Katz, "The Washington Institute for Near East Policy 'Grading counterterrorism Co-operation with GCC states'" (26 April 2018), *http://www.washingtoninstitute.org/uploads/Documents/testimony/BauerTestimony20180426.pdf* [Accessed 18 September 2020].

imposed sanctions on three terrorism financiers for "fundraising appeals on social media".[57] Here, the US Department of the Treasury stated that:

> "Al-Ajmi operates regular social media campaigns seeking donations for Syrian fighters and is one of the most active Kuwaiti fundraisers for Al-Nusra Front (ANF). In July 2014, Al-Ajmi publicly admitted that he collected money under the auspices of charity and delivered the funds in person."[58]

Further sanctions were imposed on Abdul Mohsen Abdullah Ibrahim al-Sharikh, who

> "is a senior ANF leader and al-Qaida facilitator based in Syria … in this role, al-Sharikh has used social media posts to demonstrate his aspiration to target Americans and U.S. interests".[59]

Furthermore, in 2015 Mohamed Elshinawy was convicted for

> "conspiracy to provide material support to ISIS, providing and attempting to provide material support to ISIS; terrorism financing; and making false statements in connection with a terrorism matter".[60]

Elshinawy admitted his role in a conspiracy to provide funding for ISIL via a variety of mechanisms including PayPal and Western Union, totalling $8,700.[61] In March 2019, Gregory Lepsky was sentenced to 16 years' imprisonment after pleading guilty to attempting to provide material support to a designated foreign terrorist organisation. Here, law enforcement authorities were able to determine that Lepsky had used several social media platforms to plan his terrorist attack.[62] In September 2019, the US Department of Treasury stated that

> "HAMAS solicit[ed] Bitcoin donations via social media, using two Bitcoin addressed. As of late March 2019, those two known addressed had received at least $5,000 worth of Bitcoin".[63]

[57] United States Department of the Treasury, "Treasury Designates Three Key Supporters of Terrorists in Syria and Iraq" (6 August 2014),*https://www.treasury.gov/press-center/press-releases/Pages/jl2605.aspx* [Accessed 18 September 2020].

[58] United States Department of the Treasury, "Treasury Designates Three Key Supporters of Terrorists in Syria and Iraq" (6 August 2014), United States Department of the Treasury, "Treasury Designates Three Key Supporters of Terrorists in Syria and Iraq" (6 August 2014).

[59] US Department of the Treasury, "Treasury Designates Additional Supporters of the Al-Nusrah Front and Al-Qaida" (22 August 2014), *https://www.treasury.gov/press-center/press-releases/Pages/jl2613.aspx* [Accessed 18 September 2020]. Abd Allah al-Muhaysini was designated a terrorist by the US Department of Treasury in 2016. See US Department of State, "Treasury designates key Al-Nusrah front leaders" (10 November 2016), *https://www.treasury.gov/press-center/press-releases/Pages/jl0605.aspx* [Accessed 18 September 2020]. ANF has been described as representing al Qaeda in Syria and it has been designated a foreign terrorist organisation by virtue of the Immigration and Nationality Act 1965, Pub.L. 89–236, 79 Stat. 911, enacted 30 June 1968.

[60] United States Department of Justice, "Maryland man sentenced to 20 years in prison for providing material support to ISIS and terrorism financing" (30 March 2018), *https://www.justice.gov/opa/pr/maryland-man-sentenced-20-years-prison-providing-material-support-isis-and-terrorism* [Accessed 18 September 2020].

[61] *https://www.justice.gov/opa/pr/maryland-man-sentenced-20-years-prison-providing-material-support-isis-and-terrorism* [Accessed 18 September 2020].

[62] United States Department of Justice, "New Jersey man sentenced to 16 years in prison for attempting to provide material support to ISIS" (1 March 2019), *https://www.justice.gov/opa/pr/new-jersey-man-sentenced-16-years-prison-attempting-provide-material-support-isis* [Accessed 18 September 2020].

[63] United States Department of Treasury, "Under Secretary Mandelker remarks at the 19th Annual International Conference on Counterterrorism" (11 September 2019), *https://home.treasury.gov/news/press-releases/sm773* [Accessed 18 September 2020].

These instances illustrate that terrorism financiers are using several social media platforms in an attempt either to solicit donations or to transfer funds to proscribed terrorist groups. The evidence presented in this part of the article highlights that terrorism financing continues to evolve at an unprecedented level. The use of both cryptoassets and social media platforms to obtain financing represents a new funding model that is able to thrive owing to the anonymity provided by the Dark Web. The second part of the article provides a detailed overview of the operation of DATF SARs under the Terrorism Act 2000 to ascertain whether they apply to payments made via cryptoassets and social media platforms.

## Defence against Terrorist Financing Suspicious Activity Reports

DATF SARs are synonymous with the international efforts to tackle terrorism financing and have become an integral part of the Financial War on Terrorism.[64] The use of SARs to tackle drug money laundering in the UK was introduced via the Drug Trafficking Offences Act 1986,[65] following the decision of the House of Lords in *R. v Cuthbertson*.[66] The Drug Trafficking Offences Act 1986 was part of a comprehensive attempt by HMG to tackle the laundering of the proceeds of drug trafficking offences.[67] However, it was not until the enactment of the Prevention of Terrorism (Temporary Provisions) Act 1989 that mandatory reporting obligations applied to terrorism financing.[68] The scope of the reporting obligations were further extended by the Criminal Justice Act 1993[69] and the Money Laundering Regulations 1993,[70] following the introduction of the first Money Laundering Directive by the EU.[71] These legislative instruments introduced the concept of compulsory reporting for money laundering. Further legislative amendments were introduced by the Proceeds of Crime Act 2002,[72] following the recommendations of the Performance and Innovation Unit Report in 2000.[73] The introduction of the Second Money Laundering Directive[74] and Third Money Laundering Directive[75] resulted in the implementation of the 2003[76] and the 2007 Money Laundering Regulations.[77] More

[64] Europol, *From Suspicion to Action: Converting Financial Intelligence into Greater Operational Impact* (2017), p.4. Also see National Crime Agency, *Suspicious Activity Reports Annual Report* (National 2017), p.5. For a critical commentary on the use of DATF SARs to tackle terrorism financing, see N. Ryder, "Is it Time to Reform the Counter-terrorist Financing Reporting Obligations? A Critical and Comparative Assessment of the Counter-terrorist Financing Reporting Obligations in the European Union and the United Kingdom" (2018) 19 *German Law Review* 1169.

[65] Drug Trafficking Offences Act 1986 s.24(1).

[66] *R. v Cuthbertson* [1981] A.C. 470 HL. Here, the House of Lords determined that the forfeiture powers under the Misuse of Drugs Act 1971 Act could not be used against the defendants, who had accrued £750,000 from the manufacture and distribution of narcotic substances.

[67] The Drug Trafficking Offences Act 1986 implemented the recommendations of the Hodgson Committee following the decision of the House of Lords in *R. v Cuthbertson*. See D. Hodgson, *Profits of Crime and their Recovery: The Report of a Committee Chaired by Sir Derek Hodgson* (London: Cambridge Studies in Criminology, 1984).

[68] Prevention of Terrorism (Temporary Provisions) Act 1989 s12.

[69] Criminal Justice Act 1993 ss.29–35. These provisions were amended by Pt 7 of the Proceeds of Crime Act 2002 via the The Proceeds of Crime Act 2002 (Commencement No.5, Transitional Provisions, Savings and Amendment) Order 2003 S.I. 2003/333.

[70] S.I. 1993/1933.

[71] Council Directive 91/308/EEC.

[72] Proceeds of Crime Act 2002 ss.330–332.

[73] Performance and Innovation Unit, *Recovering the Proceeds of Crime* (Cabinet Office: 2000).

[74] Directive 2001/97/EC.

[75] Directive 2005/60/EC.

[76] S.I. 2003/3075.

[77] S.I. 2007/2157.

recently, HMG introduced the Crime and Courts Act 2013[78] the 2017 Money Laundering Regulations,[79] the Criminal Finances Act 2017[80] and the Sanctions and Anti-Money Laundering Act 2018.[81] In February 2018, the European Parliament adopted the fifth Money Laundering Directive, which seeks to increase the powers of EU Financial Intelligence Units (FIU) by establishing beneficial ownership registers, to improve the protection for financial transactions involving high-risk third countries, to enhance the access to information for FIUs and, of particular relevance to this article, to prevent the use of cryptoassets for terrorism financing.[82] In October 2018, the European Commission published the Sixth Money Laundering Directive, which contained a unified list of predicate offences, increased the minimum prison sentence for money laundering, extended the criminal liability for money laundering to corporations, and altered the confiscation provisions; Member States are required to create their own jurisdiction of money laundering offences.[83]

Within these legislative provisions, the most commonly used mechanism to tackle money laundering and/or terrorism financing is financial intelligence (FININT), obtained via the submission of a DATF SAR, an instrument used by a reporting entity to make disclosures on suspected instances of money laundering and/or terrorism financing. DATF SARs provide information and intelligence from reporting entities that would not traditionally be detectable by LEAs.[84] FININT is the collection of data that arises from transactions that are suspected of being linked to money laundering and/or terrorism financing, and it provides useful knowledge for "intelligence, law enforcement and regulatory authorities to reconstruct or piece together … and predict future terrorist activities".[85] The reporting entity monitors suspicious monetary activity via its internal Financial Transaction Unit (FTU), a process managed by a money laundering reporting officer (MLRO) or nominated officer.[86] The FTU receives and collects reports via two mechanisms, manual and automated, if the transaction(s) is deemed suspicious. It then undertakes an investigation to ascertain whether the DATF SAR needs to be submitted or consent is required from the National Crime Agency (NCA) to proceed with the financial transaction.[87] Once a DATF SAR has been submitted, access to the connected account is restricted by the reporting entity pending the outcome of the investigation.[88] A reporting entity is permitted to make two forms of disclosure to

[78] Crime and Courts Act 2013 Pt 1.

[79] S.I. 2017/692.

[80] Criminal Finances Act 2017, ss.10–12.

[81] Sanctions and Anti-Money Laundering Act 2018 ss.49–51.

[82] In February 2018, the European Parliament adopted the Fifth Anti-Money Laundering Directive. See European Commission, "Statement by First Vice-President Timmermans, Vice-President Dombrovskis and Commissioner Jourovà on the adoption by the European Parliament of the 5th Anti-Money Laundering Directive" (19 April 2018), *http://europa.eu/rapid/press-release_STATEMENT-18-3429_en.htm* [Accessed 18 September 2020].

[83] Directive (EU) 2018/1673 of the European Parliament and of the Council of Europe, 23 October 2018.

[84] National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2018* (2018), p.5.

[85] M. Normark and M. Ranstrop, *Understanding Terrorist Financing: Modus Operandi and National CTF-Regimes* (Swedish Defence University: 2015), p.26.

[86] A firm which is categorised as part of the "regulated sector" is required to appoint either a money laundering reporting officer or nominated officer to supervise the firm's compliance with its money laundering obligations. A nominated officer is a person nominated to receive disclosures under Pt 3 of the Terrorism Act 2000 or Pt 7 of the Proceeds of Crime Act 2002.

[87] Proceeds of Crime Act 2002 ss.335 and 336.

[88] For an illustration of the problems associated with banks not completing a financial transaction in these circumstances, see *Shah v HSBC Private Bank (UK) Ltd* [2010] EWHC 1283 (QB); and *N v Royal Bank of Scotland* [2017] EWCA Civ 253.

the NCA. The first is a required disclosure, which aims to provide financial intelligence to the LEA.[89] The second is an authorised disclosure that involves a DATF SAR being submitted, where the reporting entity seeks consent to complete the transaction.[90] After making an authorised disclosure, a statutory seven-day working notice period is imposed, thus allowing the NCA to process the DATF SAR and to determine whether consent should be granted or refused. If consent is refused, a statutory moratorium of 31 calendar days begins, which prevents the reporting entity from undertaking any additional action.[91] Failure to submit a SAR is a criminal offence under the Proceeds of Crime Act 2002[92] and the Terrorism Act 2000.[93] However, a criminal offence is not committed if the reporting officer has a reasonable excuse,[94] statutory legal privilege,[95] inadequate training by employer,[96] or if money laundering occurs outside the UK.[97]

All DATF SARs are "referred to the National Terrorist Financial Intelligence Unit, which is part of the Metropolitan Police Counter Terrorist Command".[98] The FATF stated that

> "the NTFIU analyses DATF SARs which are prioritised and screened by the UKFIU. The NTFIU has an officer embedded in the UKFIU to quicken the flow of information. It also has a dedicated Financial Intelligence Development team with an independent work stream dedicated to managing SARs".[99]

The information contained in the SARs is invaluable not only because it enriched ongoing operations but also result in new investigations. As a consequence, it can be stated that SARs have proven to be effective when tackling money laundering and the traditional sources of terrorism financing.[100] Whilst the Law Commission concluded that DATF SARs provide crucial intelligence to combat terrorism,[101] the NCA also stated that SARs could be utilised "in the analysis of suspicious activity before and after a specific event such as a terrorist incident".[102] SARs are used to report all types of suspicious activities and the FININT derived from the reports creates a paper trail of potential criminal activity that allows further investigation to focus on specific financial transactions that could be associated to acts of terrorism.[103]

[89] Proceeds of Crime Act 2002 ss.330 and 331.
[90] Proceeds of Crime Act 2002 ss.338.
[91] The Criminal Finances Act 2017 introduced a set of new powers to extend the moratorium period beyond 31 days. See Criminal Finances Act 2017 s.10(2).
[92] Proceeds of Crime Act 2002 ss.330–332.
[93] Terrorism Act 2000 s.19.
[94] Proceeds of Crime Act 2002 ss.330(6)(a), 331(6) and 332(6).
[95] Proceeds of Crime Act 2002 ss.330(6)(b), 330(10), 330(11) and 330(7B).
[96] Proceeds of Crime Act 2002 s.330(7)(b).
[97] Proceeds of Crime Act 2002 s.330(7A).
[98] Law Commission, *Anti-Money Laundering: The SARs Regime Consultation Paper* (2018), p.51.
[99] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures: United Kingdom Mutual Evaluation Report* (2018), p.50.
[100] HM Treasury, *Anti-money Laundering Strategy* (2004).
[101] Law Commission, *Anti-Money Laundering* (2018), p.51.
[102] National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2018* (2018).
[103] The intelligence provided by SARs has been crucial in finding sex offenders and murder suspects, and identifying people who are suspected of being involved in the exploitation of children and combating human trafficking. See National Crime Agency, "Suspicious activity reports" (n/d), *https://nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-terrorist-financing/suspicious-activity-reports* [Accessed 26 July 2019]. Also see "Help Stop Money Laundering: Act on your Suspicions" (28 February 2018", *The Independent*, *https://www.independent.co.uk/news/business/news/help-stop-money-laundering-act-on-your-suspicions-a8214286.html* [Accessed 18 September 2020].

Conversely, the SARs regime does have a number of weaknesses, which is not surprising given that there are approximately 39 billion financial transactions each year in the UK that could be monitored for money laundering and/or terrorism financing.[104] The first criticism relates to the length of completion of the SAR process. It has been suggested by the Law Commission that DATF SARs are often unable to provide FININT that could be used to prevent acts of terrorism:

> "[R]etrospective DATF SARs are less helpful in terrorism financing cases given the relatively short time period in which attacks were planned. Unsophisticated attacks could be planned and executed in less than six months and often no more than 12 months. Historic information is of little value."[105]

Second, terrorism financing in the UK is associated with very small amounts of funding which are often impossible to detect via a DATF SAR. Examples of low-cost acts of terrorism include the London terrorist attacks in July 2005, which, according to the Metropolitan Police cost approximately £7,235 (£4,600 for the deployment of devices and materials; international travel £1,810 and training weekends £825).[106] Another example of cheap terrorism occurred in March 2017 when Khalid Masood killed four people and injured approximately 50 more when he drove a car towards pedestrians on Westminster Bridge.[107] In June 2017, Darren Osborne rented a vehicle, at an estimated cost of £85 per day, and drove the vehicle into a crowd of people outside Finsbury Park Mosque at an estimated cost of £255.[108] In June 2017, eight people were killed by Khuram Shazad Butt, Rachid Redouane and Youssef Zaghba, who drove a van into pedestrians on London Bridge and launched a knife attack in Borough Market on Saturday, 3 June 2017. The terrorists rented a vehicle that was hired for approximately £30 per day, and used salad knives that cost approximately £3 each.[109] In September 2017, Ahmed Hassan was was convicted of attempted murder after he planted an improvised explosive device (IED) on the District Line in London. Hassan manufactured the IED using a £20 Amazon voucher.[110] In May 2017, Salman Abedi, who detonated an IED in the Manchester Arena, killing 22 people, acquired funding via two years of student loans (worth approximately £14,000) and misused benefit payments to fund this act of terrorism.[111] Several of these attacks have involved terrorists using

[104] See BBC News, "Millions choose a cashless lifestyle" (6 June 2019, *https://www.bbc.co.uk/news/business-48542233#:~:targetText=A%20total%20of%2039%20billion,spontaneous%2C%20rather%20than%20scheduled%20payments*. [Accessed 18 September 2020]. Of the 634,113 SARs submitted to the NCA between October 2015 and March 2017, only 422 related to terrorism financing. See National Crime Agency, *Suspicious Activity Reports Annual Report* (2017), p.6.

[105] See Law Commission, *Anti-Money Laundering: The SARs Regime Consultation Paper* (2018), p.57.

[106] HMG estimated that this terrorist attack cost approximately £8,000. See HMG, *House of Commons Report of the Official Account of the Bombings in London on 7th July 2005* (2005), p.23, para.63.

[107] Khalid Masood drove a hired car across Westminster Bridge, killing four people and he then murdered a police officer in Parliament Square.

[108] See *R. v Darren Osborne*, Woolwich Crown Court, 2 February 2018, sentencing remarks of Mrs Justice Cheema-Grubb, *https://www.judiciary.uk/wp-content/uploads/2018/02/r-v-osborne-sentencing-remarks.pdf* [Accessed 18 September 2020].

[109] BBC, "London Bridge Inquests: Attacker Bought Pink Knives from Lidl" (29 May2019), *https://www.bbc.co.uk/news/uk-48443724* [Accessed 18 September 2020].

[110] See *R. v Hassan*, 23 March 2018, sentencing remarks of the Hon. Mr Justice Haddon-Cave, *https://www.judiciary.uk/wp-content/uploads/2018/03/r-vhassan-sentencing.pdf* [Accessed 18 September 2020].

[111] See R. Mendick, M. Evans, and V. Ward, "Manchester Suicide Bomber Used Student Loan and Benefits to Fund Terror Plot" (27 May 2017), *The Telegraph*, *https://www.telegraph.co.uk/news/2017/05/26/exclusive-manchester-suicide-bomber-used-student-loan-benefits/* [Accessed 18 September 2020]; and T. Keatinge, "Terror on the Cheap: Financing Lone Actor and Small Cell Attacks" (17 August 2015), *https://rusi.org/commentary/terror-cheap-financing-lone-actor-and-small-cell-attacks* [Accessed 18 September 2020]. In July 2019, the younger brother of Salman

a rental vehicle to target pedestrians. Of course, anyone has the financial capability to self-fund the renting of a vehicle, thus providing more evidence that low-cost acts of terrorism exploit the loopholes in the DATF SAR system. If a terrorist or terrorist cell is financially self-sufficient, there is no need for them to be involved in funding activities that could lead to the submission of a DATF SAR by a reporting entity.

The third weakness with DATF SARs relates to a concept referred to as "defensive" or "preventative reporting", which has resulted in a significant increase in the number of SARs submitted to the NCA.[112] Therefore, the increase in SARs submitted to the NCA has resulted in the process becoming very time-consuming and slow, which has limited the reactionary capabilities of the system to detect terrorism funding. Defensive reporting involves a reporting entity submitting a DATF SAR because of the severe financial penalties that can be imposed for failing to report, as opposed to submitting a DATF SAR owing to genuine suspicion. The interpretation of the term "suspicion" is one of the most documented weaknesses of the DATF SARs regime. There is no definition provided by either the Proceeds of Crime Act 2002 or the Terrorism Act 2000, and it has been left to the judiciary to develop an interpretation.[113] Defensive reporting has been fuelled by the imposition of a numerous large financial penalties for breaches of the reporting obligations on the reporting entity or its MLRO.[114] This highest financial penalty imposed in the UK by the Financial Conduct Authority (FCA) was £163.1 million on Deutsche Bank in 2017.[115] Defensive or preventative reporting has resulted in record numbers of SARs submitted to the NCA. For example, in 2001 approximately 5,000 SARs were submitted, while, by 2018, the figure had increased to 463,939.[116] Therefore, the overall effectiveness of the SARs regime could be questioned, and its success is heavily reliant upon the accuracy of the reports completed by reporting entities and the quality of the subsequent investigations. Some of the above-identified issues could be partially tackled by putting more money into the mechanism so that SARs are analysed faster and by more experts in the field. Yet, a further, more important weakness, that has hardly been noticed in academic literature, must be highlighted: the DATF SARs regime does not apply to the transactions that are made by cryptoassets and those that are conducted via social media platforms.

Abedi, Hashem Abedi, was charged with murdering the 22 victims of the attack. See BBC, "Manchester Arena Attack: Bomber's Brother Appears in Court" (18 July 2019), *https://www.bbc.co.uk/news/uk-england-manchester-49029276* [Accessed 18 September 2020]. In November 2015, Yahya Rashid was convicted and sentenced to five years in youth custody for several breaches of the Terrorism Act 2000 after he spent his student loan and other grants on travelling to join ISIS. See *R. v Rashid (Yahya)* [2017] EWCA Crim 2.

[112] Defensive reporting is one of the most frequently referred to weaknesses of the SARs regime in the United Kingdom, Australia, Canada and the United States of America. See N. Ryder, *Money Laumdering: An Endless Cycle? A Comparative Analysis of the Anti-Money Laundering Policies in the USA, UK, Australia and Canada* (Abingdon: Routledge, 2012), pp.63, 64, 120, 128, 156, 164. Also see Law Commission, *Anti-Money Laundering: The SARs Regime Report* (2019), pp.19, 31, 33, 65, 66, 91, 93, 99, 104 and 112.

[113] See *R. v Da Silva* [1996] 2 Cr. App. App R. 35; *K. v National Westminster Bank* [2006] EWCA Civ 1039; *Parvizi v Barclays Bank* [2014] EWHC N2 (QB); and *Shah v HSBC* [2010] EWCA Civ 31.

[114] See, for example, Financial Conduct Authority, *Final Notice Steven George Smith* (2016). Here, Steven Smith was fined £17,900 and is an example of the FCA's "credible deterrence" enforcement strategy. See G. Wilson and S. Wilson, "The FSA, 'credible deterrence', and criminal enforcement — a 'haphazard pursuit'"? (2014) 21 *Journal of Financial Crime* 4.

[115] Financial Conduct Authority, *Final Notice: Deutsche Bank* (2017).

[116] National Crime Agency, *Suspicious Activity Reports (SARs) Annual Report 2018* (1918), at p.1.

The funding model identified in the first part one of this article is able to evade the DATF SARs regime and, in order to address this limitation, the article advocates an innovative approach that no longer sees DATF SARs used in isolation, but used in association with a broader information-sharing initiative that includes social media platforms. This is a significant weakness within the DATF SARs regime, and one that requires legislative amendment and a clear policy statement from the UK Government. The legislative shortfall can be compared to the weak and disjointed policy adopted by the UK Government towards the regulation of cryptoassets and the application of the DATF SARs, which is considered in the next section of the article.

## The regulation of cryptoassets

The flaws highlighted above in the DATF SARs regime are worsened by the UK not implementing the FATFs related Recommendation and its weak attempts to regulate cryptoassets, which is based on self-regulation. In response to the threat posed by cryptoassets, the FATF stated that they

> "create new opportunities for criminals and terrorists to launder their proceeds or finance their illicit activities … [it has] issued guidance on a risk-based approach to virtual currencies … there is an urgent need for all countries to take coordinated action to prevent the use of virtual assets for crime and terrorism".[117]

Therefore, the FATF recommended that:

> "All jurisdictions should urgently take legal and practical steps to prevent the misuse of virtual assets. This includes assessing and understanding the risks associated with virtual assets in their jurisdictions, applying risk-based AML/CFT regulations to virtual asset service providers and identifying effective systems to conduct risk-based monitoring or supervision of virtual asset service providers".[118]

Accordingly, the FATF revised its Recommendation 15, which now includes new definitions of "virtual assets" and "virtual asset service providers".[119] The current UK policy toward the regulation of cryptoassets contradicts the guidance issued by the FATF in June 2019.[120] Here, the FATF stated that the risk-based approach

[117] Financial Action Task Force, "Regulation of virtual assets" (19 October 2018), *http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html* [Accessed 18 September 2020].

[118] Financial Action Task Force, "Regulation of virtual assets" (19 October 2018), *http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets.html* [Accessed 18 September 2020].

[119] Recommendation 15 now provides: "Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations". See Financial Action Task Force, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation — The FATF Recommendations* (2018), p.15.

[120] Financial Action Task Force, "Outcomes FATF Plenary, 16–21 June 2019" (21 June 2019, *https://www.fatf-gafi.org/publications/fatfgeneral/documents/outcomes-plenary-june-2019.html* [Accessed 18 September 2020]. Also see Financial Action Task Force, *FATF Report to the G20 Leaders' Summit* (2019).

and its Recommendations apply to cryptoassets. Furthermore, the FATF stated that cryptoassets should be regulated by official, competent authorities and not self-regulatory agencies.[121] Therefore, the regulation of cryptoassets in the UK is in breach of FATF Recommendation 15, which could result in the UK being categorised as high-risk and other monitored jurisdiction. The FATF Recommendations are not legally enforceable, and the UK is not obliged to include cryptoassets within the DATF SARs regime. Nonetheless, the 5MLD provided that EU Member States were required to extend the remit of DATF SARS to include cryptoassets by June 2020. The UK began the process of preparing to implement the 5MLD when HM Treasury published a consultation paper in 2019.[122]

The current system of supervision and the regulation of cryptoassets is inadequate and has been hindered by HMG's "go and stop" policy that has led to self-regulation rather than state regulation of the sector. For example, in November 2014, HMG published a call for information on digital currencies,[123] followed by the publication of a summary of the evidence collected in March 2015.[124] Subsequently, in the 2015 budget, HMG announced that it intended to apply the AML regulations to digital currencies in the UK.[125] However, since the publication of these documents, there has been very little development in efforts by HMG to develop a formal system of regulation for cryptocurrencies. The inconsistent stance adopted by HMG might be explained by the difference of opinion between HM Treasury, the NCA and the FCA. For example, David Raw, the Deputy Director of Banking and Credit at HM Treasury stated that

> "the latest risk assessment from the National Crime Agency is that [crypto-assets'] use for … terrorist financing is currently low. They are seeing cases of it, but it is not widespread".[126]

Furthermore, Donald Toon of the NCA stated that

> "it is important that we place virtual currencies in the context of the whole money laundering/terrorism financing problem … [there are] other large-scale areas of the problem".[127]

Conversely, the FCA stated that their work and intelligence that

> "postdates the intelligence of the National Risk Assessment relied on shows evidence supporting wider-scale criminal use and we now view the potential harm in this space to be greater than previously assessed".[128]

[121] For a more detailed discussion of what amounts to competent authority see generally N. Ryder, *Financial Crime in the 21st Century: Law and Policy* (Cheltenham: Edward Elgar, 2011).

[122] HM Treasury, *Transposition of the Fifth Money Laundering Directive* (2019).

[123] See HM Treasury, "Chancellor on Developing FinTech" (6 August 2013), *https://www.gov.uk/government/speeches/chancellor-on-developing-fintech* [Accessed 18 September 2020].

[124] HM Treasury, *Digital Currencies: Response to the Call for Information* ( 2015).

[125] See HM Treasury, *Budget 2015* (2015), p.32.

[126] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018), p.25.

[127] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018), p.25.

[128] Financial Conduct Authority, "Financial Conduct Authority's Written Submission on Digital Currencies" (April 2018), *http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/treasury-committee/digital-currencies/written/81677.pdf* [Accessed 18 September 2020].

The Crypto Asset Task Force of the FCA supported the conclusions of the FCA in that it had

> "identified a range of risks associated with crypto assets, including risks of financial crime, including opportunities for crypto assets to be used for illicit activity and cyber threats".[129]

It added:

> "Cryptoassets pose risks around criminal activity such as money laundering and terrorist financing because of their accessibility online, their global reach and their pseudo-anonymous nature".[130]

In the absence of any clear, official policy, it has been left to the industry trade association, "Crypto UK", to develop a system of self-regulation.[131] CryptoUK have developed a voluntary code of conduct that provides that the sector is

> "in line with anti-money laundering regulations … [and its] members commit to undertaking due diligence checks on platform users to protect against illegal activity, including the financing of terrorism".[132]

The HM Treasury Select Committee on Cryptoassets was highly critical of this form of regulation, stating that "self-regulation within the crypto-asset industry is clearly insufficient",[133] and concluded that,

> "given the scale and variety of consumer detriment, the potential role of crypto-assets in money laundering and the inadequacy of self-regulation, the Committee strongly believes that regulation should be introduced. At a minimum, regulation should address consumer protection and anti-money laundering".[134]

The current system of self-regulation is unsatisfactory, and cryptoassets must fall within the regulatory remit of the FCA. At the moment, cryptoasset providers are under no statutory obligation to report any suspicious activity via a DATF SAR to the NCA. The obligation is voluntary, insufficient and inadequate to deal with the threat from terrorism financing. This could be rectified by extending the remit of the Financial Services and Markets Act 2000 Regulated Activities Order 2001 to include cryptoassets.[135] Such an approach has been advocated by the FATF, an intergovernmental body that was created in 1989 to set international AML and CTF standards.[136]

As cryptoassets do not fall within the regulatory remit of the FCA consumers and investors who purchase and sell cryptoassets, they are not subject to the same

[129] See Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), p.33.
[130] Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), p.33.
[131] CryptoUK, "Welcome to CryptoUK" (n/d), *https://www.cryptocurrenciesuk.info/* [Accessed 22 September 2020].
[132] CryptoUK, "Principles and Code of Conduct" (n/d *http://www.cryptocurrenciesuk.info/code-of-conducts/* [Accessed 18 September 2020].
[133] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018), p.32.
[134] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018), p.34.
[135] S.I. 2001/544.
[136] Financial Action Task Force, "Who we are" (n/d), *https://www.fatf-gafi.org/about/* [Accessed 18 September 2020].

levels of protection afforded to users of other financial services. This would include, for example, the protection provided by the Financial Services Compensation Scheme and the Financial Ombudsman Service.[137] Consumers and investors were warned in November 2017, by the FCA, of the inherent risks in purchasing or selling cryptoassets.[138] This was followed by a similar warning published by the FCA in June 2018, concerning investment scams involving cryptoassets.[139] Additionally, the regulatory loophole means that any transactions conducted by cryptoassets do not fall with the financial crime regulations of the FCA. In response to the growing threat, the FCA Cryptoasset Task Force (Task Force) published its report on how the FCA intended to regulate cryptoassets.[140] The Task Force highlighted three risks presented by cryptoassets: the harm they potentially present to consumers and market integrity, the use of cryptoassets for illicit activities, and potential future threats to financial stability.[141] In order to address these concerns, the Task Force proposed further consultation on whether cryptoassets fall within the regulatory remit of the existing FCA regulations, should there be a prohibition on the sale to retail consumers of derivatives relating to cryptoassets, how should cryptoassets be regulated and the proposed application of the 5MLD to cryptoassets.[142] The Task Force concluded that

> "cryptoassets pose risks around criminal activity such as money laundering and terrorist financing because of their accessibility online, their global reach and their pseudo-anonymous nature".[143]

In response to the threat posed by cryptoassets, the FCA published its "Guidance on Cryptoassets" Consultation Paper in January 2019.[144] Here, the FCA proposed its regulation of cryptoassets when they are deemed to be "specific investments" under the Regulated Activities Order,[145] "financial instruments" by virtue of the Markets in Financial Instruments Directive II,[146] the Payment Services Regulations[147] or the E-Money Regulations.[148] In relation to the application of the CTF reporting obligations, the FCA referred to the conclusions of the Task Force, which stated that HM Treasury could consult on extending the remit of the FCA's regulation to include cryptoassets.[149] The FCA concluded that this type of financial product is unsuitable for retail consumers for four reasons:

[137] See Financial Services Compensation Scheme, "FSCS Protects you when Financial Firms Fail" (n/d), *https://www.fscs.org.uk/* [Accessed 18 September 2020] and Financial Ombudsman Service, "Who Are we?" (n/d), *https://www.financial-ombudsman.org.uk/who-we-are* [Accessed 18 September 2020].

[138] Financial Conduct Authority, "Consumer Warning about the Risks of Investing in Cryptocurrency CFDs" (14 November 2017), *https://www.fca.org.uk/news/news-stories/consumer-warning-about-risks-investing-cryptocurrency-cfds* [Accessed 18 September 2020].

[139] Financial Conduct Authority, "Crypto Investment Scams" (27 June 2018) *https://www.fca.org.uk/scamsmart/cryptocurrency-investment-scams* [Accessed 18 September 2020].

[140] Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), p.11.

[141] Financial Conduct Authority, "Cryptoasset Taskforce Publishes Report on UK Approach to cryptoassets" (29 October 2018), *https://www.fca.org.uk/news/news-stories/cryptoasset-taskforce-publishes-report-uk-approach-cryptoassets* [Accessed 18 September 2020].

[142] Financial Conduct Authority, "Cryptoasset Taskforce Publishes Report on UK Approach to cryptoassets" (29 October 2018), *https://www.fca.org.uk/news/news-stories/cryptoasset-taskforce-publishes-report-uk-approach-cryptoassets* [Accessed 18 September 2020].

[143] Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), p.32.

[144] Financial Conduct Authority, *Guidance on Cryptoassets Consultation Paper* (2019).

[145] The Financial Services and Markets Act 2000 (Regulated Activities) Order 2001, S.I. 2001/544.

[146] Directive 2014/65/EU.

[147] S.I. 2017/752.

[148] S.I. 2011/99.

[149] Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), para.2.36, p.26.

- the uncertain nature of the underlying assets that have dependable basis for their valuation;
- the FCA acknowledged the threat posed to the cryptoassets by market abuse and financial crime;
- the extreme in the price movement of cryptoassets; and
- the insufficient understanding demonstrated by retail consumers towards the cryptoassets market.[150]

In response to the recommendations of the Task Force, the FCA announced that it proposed to introduce rules to prohibit the sale of crypto-derivatives.[151] The decision by the FCA to prohibit certain types of cryptoassets is an important development in its efforts to regulate cryptoassets because it recognises the threat posed by financial crime. However, the scope of consultation falls short of addressing fully the weakness in the regulation of cryptoassets.

Cryptoassets providers do not fall within the scope of the DATF SARs regime. The House of Commons Treasury Committee on Crypto Assets noted that while

> "cryptoassets will fall within the scope of the Fifth Anti-Money Laundering Directive and will have to comply with anti-money laundering and counter-terrorist financing rules, crypto-asset exchanges are not included in Anti-Money Laundering regulations that are currently in force".[152]

It added that

> "the UK will not tolerate the use of cryptoassets in illicit activity, and the authorities will take strong action to address these risks by bringing all relevant firms into anti-money laundering and counter-terrorist financing regulation".[153]

The aforementioned recommendations from the FCA Task Force and the publication of the FCA's "Guidance Paper" represent a positive move forward. However, the decision by the FCA and its Task Force to conduct a further period of consultation is unsatisfactory, given the threat posed by terrorism financing and cryptoassets. It is argued that, in order to address this deficiency, cryptoassets must be included within the regulatory remit of the FCA and be made subject to its CTF regulations. For example, the Systems and Controls (SYSC) part of the FCA's Handbook requires that a regulated firm must

> "ensure the policies and procedures established under SYSC 6.1.1 R include systems and controls that (1) enable it to identify, assess, monitor and manage money laundering risk; and (2) are comprehensive and proportionate to the nature, scale and complexity of its activities".[154]

[150] For a more detailed discussion, see Financial Conduct Authority, *Prohibiting the Sale to Retail Clients of Investment Products that Reference Cryptoassets — Consultation Paper 19/22* (2019).

[151] Financial Conduct Authority, "FCA Proposes Ban on Sale of Crypto-derivatives to Retail Consumers"(3 July 2019)*https://www.fca.org.uk/news/press-releases/fca-proposes-ban-sale-crypto-derivatives-retail-consumers* [Accessed 18 September 2020].

[152] House of Commons Treasury Committee, *Crypto-assets Twenty-Second Report of Session 2017–19* (2018), p.55.

[153] Financial Conduct Authority, "Cryptoassets Taskforce: final report" (2018), p.26.

[154] Financial Conduct Authority, *FCA Handbook* (2006), SYSC 6.3.1.

Furthermore, "firms must carry out a regular assessment of the adequacy of these systems and controls to ensure that they continue to comply with SYSC 6.3.1 R".[155] The Handbook also provides that

> "a firm must allocate to a director or senior manager (who may also be the money laundering reporting officer) overall responsibility within the firm for the establishment and maintenance of effective anti-money laundering systems and controls".[156]

Finally, an authorised firm is also required to appoint an MLRO who is responsible for maintaining the firm's compliance with these rules.[157] It is therefore contended that the inclusion of the cryptoassets within the CTF reporting requirements of the FCA Handbook would close an existing loophole, and it would place cryptoassets within the same regulatory framework as other reporting entities, thus representing a better model of regulation than the current voluntary self-regulatory reporting system. The regulation of cryptoassets within the UK has been hindered by a very inconsistent narrative from HMG which, as explained earlier, has largely dismissed the threat posed by cryptoassets. The inclusion of cryptoassets within the regulatory remit of the FCA would represent a stronger and more robust system of regulation than that provided by CryptoUK.

## Social media platforms and information-sharing

The ability of terrorism financiers to attract funding and support via the internet, as outlined above, has spread to social media platforms, which could indirectly facilitate the problem. For example, in November 2017, Facebook launched its Messenger payments service, which allows its users to send money to "friends".[158] Furthermore, Barclays Bank became the first UK bank to allow account holders to make payments to each other and small businesses using just their Twitter handle, through a mobile phone application—Pingit.[159] There is no need for the account number or sort code for the payments to be made. In June 2018, Facebook announced that it will launch a new cryptoasset called LIBRA, which will allow payments to be made via its mobile phone application and WhatsApp.[160] Facebook stated that the cryptoasset would be independently managed, but this is another example of self-regulation which, as previously noted in this article, is unsuitable. This area of finance will undoubtedly continue to grow, as illustrated by the decisions of Tencent and Telegram to launch their own cryptoassets.[161] This raises an important question: do these payments fall within the remit of the Money Laundering Regulations, and will these social media platforms be required to

[155] Financial Conduct Authority, *FCA Handbook* (2006), , SYSC 6.3.3.
[156] Financial Conduct Authority, *FCA Handbook* (2006), SYSC 6.3.8.
[157] Financial Conduct Authority, *FCA Handbook* (2006), SYSC 6.3.9.
[158] See Facebook, "Payments in messages" (n/d), *https://en-gb.facebook.com/help/863171203733904/?helpref=hc_fnav* [Accessed 9 March 2019].
[159] See Barclays Bank, "Barclays Pingit" (n/d), *https://www.barclays.mobi/BarclaysPingit/MP1242629610109* [Accessed 22 September 2020].
[160] K. Paul, "Libra: Facebook launches cryptocurrency in bid to shake up global finance" (18 June 2019), *https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions* [Accessed 18 September 2020].
[161] See I. Khrennikov and S. Kravchenko, "Telegram cryptocurrency offered at triple ICO price" (8 July 2019), *https://www.bloomberg.com/news/articles/2019-07-03/telegram-cryptocurrency-offered-for-sale-at-triple-ico-price* [Accessed 18 September 2020].

submit DATF SARs? The Facebook Messenger payments system does not support business payments. According to Facebook's terms of service, the "e-money account and the P2P service are for personal use only".[162] Therefore, businesses cannot use the service; the service only supports personal transactions between friends and family. Hypothetically, if a person in the regulated sector knew or suspected, or had reasonable grounds to know or suspect, that a person was utilising the Facebook Messenger payments system for the purposes of transferring criminal property, for money laundering, and that knowledge/suspicion came to them in the course of their business in the regulated sector, then he/she would be obligated to make a DAFT SAR.[163] However, it seems this scenario is unlikely. If a person not in the regulated sector considers they are at risk of committing one of the principal money laundering offences under the Proceeds of Crime Act 2002,[164] or Terrorism Act 2000,[165] when using the Facebook Messenger payments system, by becoming concerned in an arrangement which uses the system to facilitate the transfer of criminal funds, then it is a defence for them to make an authorised disclosure to the NCA. However, the relevant person must wait until consent is received before proceeding—making an authorised disclosure but proceeding without consent remains an offence. This scenario appears more plausible. Therefore, payments made via social media platforms fall within the remit of the DATF SARs regime. The inclusion of financial transactions conducted between "friends" on Facebook within the DATF SARs regime is logical and the correct mechanism to close the loophole. However, no guidance has been provided by either the NCA or the FCA that outlines the legal obligations of Facebook and other social media platforms. Therefore, a disparity exists within the application of payments made via social media platforms and the perceived scope of DATF SARs. In order to address this weakness, guidance must be provided so that social media platforms are made aware of their potential legal obligations, in conjunction this those already published by the FATF.

One solution would be the adoption of a joined-up or hybrid approach that involves social media platforms working and co-operating with reporting entities and the NCA to monitor payments made to social media platforms. This raises a number of important questions and concerns that need to be addressed. For example, what is the role of reporting entities to identify potential suspicious financial activity via social media platforms? Should the DATF SARs regime be extended to include social media platforms? Furthermore, would it be possible to identify terrorism financiers via the information available on social media platforms? There is evidence to suggest that US school shootings could have been prevented after the perpetrators posted images on social media stating that they intended to commit these crimes.[166] Conversely, there is no guarantee over the quality and reliability

[162] See Facebook, "Terms of service" (n/d), *https://www.facebook.com/terms.php* [Accessed 18 September 2020].
[163] Terrorism Act 2000 s.19.
[164] Proceeds of Crime Act 2002 ss.327–329.
[165] Terrorism Act 2000 ss.15–18.
[166] See A. Leibowitz, "Could Monitoring Students on Social Media Stop the Next School Shooting?" (6 September 2018), *https://www.nytimes.com/2018/09/06/us/social-media-monitoring-school-shootings.html* [Accessed 19 September 2020]. Conversely, see F. Patel, and R. Levinson-Waldman, "Monitoring kids' social media accounts won't prevent the next school shooting" ( 5 March 2018), *https://www.washingtonpost.com/news/posteverything/wp/2018/03/05/monitoring-kids-social-media-accounts-wont-prevent-the-next-school-shooting/?utm_term=.3f0dd39b0afe* [Accessed 22 September 2020]. The importance of monitoring social media platforms streaming was illustrated by the terrorist attack in New Zealand, where the perpetrator live-streamed the attack on Facebook. See BBC, "Christchurch

of the information that could be obtained via social media platforms. Would this information enhance the FININT that financial institutions already have when profiling customers? There are several examples of data providers who are often unwilling to share the release data. For example, in 2015 Syed Rizwan Farook and Tashfeen Malik murdered 14 people and injured 22 in a terrorist attack in San Bernardino, California.[167] While investigating the terrorist attacks, the DoJ asked Apple to unlock one of the terrorists I-Phone; however, Apple refused to do on the grounds that such a move would infringe human rights.[168]

The most important mechanism to prevent terrorism financing via social media platforms is the voluntary exchange of information.[169] The FATF has noted that "effective information is one of the cornerstones of a well-functioning CTF framework".[170] The success of information-sharing is reliant on the relationship between LEAs and reporting entities, which in the UK has been "plagued by mistrust resulting in poor information sharing where vital information possessed by each party has been kept in silos".[171] In order to redress these weaknesses, JMLIT was established as a private- public partnership with the NCA and the financial sector to tackle high-end money laundering.[172] High-end money laundering is regarded as

> "particularly relevant in major frauds and overseas corruption work, where the raw material of the crime is electronic and cash is only used further down the laundering process to disguise audit trails or extract profits. In this respect, it can be distinguished from the laundering of street cash generated by the activities of organised criminal groups".[173]

JMLIT was created in February 2015 to improve the sharing of information between reporting entities and LEAs.[174] This approach aims to increase the understanding of how the financial services sector has been exploited by money launderers and other financial criminals, thus enabling LEAs to obstruct the flow of the proceeds of crime.[175] The scope of JMLIT includes financial and credit

shootings: 49 dead in New Zealand mosque attacks" (15 March 2019, *https://www.bbc.co.uk/news/world-asia-47578798* [Accessed 19 September 2020].

[167] Federal Bureau of Investigation, "FBI Will Investigate San Bernardino Shootings as Terrorist Act" (4 December 2015, *https://www.fbi.gov/news/stories/fbi-will-investigate-san-bernardino-shootings-as-terrorist-act* [Accessed 19 September 2020].

[168] For an explanation of the reasons behind this decision, see Apple, "A Message to Our Customers" (16 February 2016), *https://www.apple.com/customer-letter/* [Accessed 19 September 2020].

[169] It is interesting to note that the approach towards money laundering can be contrasted to that adopted for tax evasion, where the exchange of information is automatic. See The International Tax Compliance Regulations 2015, S.I. 2015/878. A detailed discussion of this difference is beyond the scope of this article, but for a more detailed discussion see Organisation for Economic Co-operation and Development, *Global Forum on Transparency and Exchange of Information for Tax Purposes Automatic Exchange of Information Implementation Report 2018* (2018).

[170] Financial Action Task Force, *Private Sector Information Sharing* (2017), p.2.

[171] See Normark and Ranstrop, *Understanding Terrorist Financing* (Swedish Defence University: 2015), p.36. Also see Home Office, "Home Secretary on the work of the Financial Sector Forum: Theresa May announces launch of Joint Money Laundering Intelligence Taskforce" (24 February 2015, *https://www.gov.uk/government/speeches /home-secretary-on-the-work-of-the-financial-sector-forum* [Accessed 19 September 2020].

[172] National Crime Agency, Joint Money Laundering Intelligence Task Force, (n.d.), *http://www.nationalcrimeagency .gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit* [Accessed 7 July 2018]. High-end money laundering has been identified by the NCA as one of its national priorities. See National Crime Agency, *NCA Annual Plan 2017–2018* (2017), p.9.

[173] National Crime Agency, *High End Money Laundering: Strategy and Action Plan* (2014), p.2.

[174] For a brief discussion, see Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018) pp.40–41. Also see Law Commission, *Anti-Money Laundering* (2018), pp.42–43.

[175] HM Treasury, "Anti-money laundering taskforce unveiled" (25 February 2015), *https://www.gov.uk/government /news/anti-money-laundering-taskforce-unveiled* [Accessed 19 September 2020].

institutions in the regulated sector,[176] and it has access to 89 per cent of all UK personal current accounts.[177] The exchange of information, facilitated by JMLIT, has resulted in 63 arrests of individuals suspected of money laundering; over 1,000 investigations into bank customers suspected of money laundering; the recognition of over 2,000 accounts that were unknown to LEAs; enhanced monitoring by banks of over 400 accounts; the closure of a further 450 bank accounts suspected of being used for the purposes of money laundering; the restraint of £7 million of suspected criminal funds; and the obtaining of approximately 40 Proceeds of Crime Act 2002 orders.[178] Furthermore, as a result of the exchange of information and investigation facilitated by JMLIT, four members of a human trafficking gang were convicted in November 2016.[179] Importantly, there was success in relation to terrorism financing:

> "After the London Bridge attack NTFIU, with UKFIU support, initiated a 24/7 response and the case was brought to JMLIT within 12 hours of the attack. Within a few hours of the briefing, financial institutions were able to provide assistance to identify the payments for van hire and establish spending patterns, allowing further investigative strategies to be identified. This assistance was crucial in allowing investigators to conclude that the attack involved only three attackers with no broader network."[180]

JMLIT has "made very quick progress in aiding voluntary information sharing … and has quickly demonstrated the benefits of this kind of working".[181] The UK has become a global forerunner in its efforts to improve the exchange of information between reporting entities and LEAs. For example, the UK model has been adopted in Australia,[182] Singapore[183] and Hong Kong.[184] Indeed, the FATF concluded that

> "JMLIT is an innovative model for public/private information sharing that has generated very positive results since its inception in 2015 and is considered to be an example of best practice".[185]

[176] The Criminal Finances Act 2017 (Commencement No.3) Regulations, S.I. 2017 No.881, reg.2(b); the Criminal Finances Act 2017 (Commencement No.3) Regulations, S.I. 2017 No.1028, reg.2(a).

[177] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), p.47.

[178] National Crime Agency, "Joint Money Laundering Intelligence Taskforce (JMLIT)" (n/d), *http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-economic-crime-centre/joint-money-laundering-intelligence-taskforce-jmlit* [Accessed 14 February 2019]. See also Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), pp.46 and 48.

[179] Royal United Services Institute for Defence and Security Studies, *The Role of Financial Information-Sharing Partnerships in the Disruption of Crime* (2017) 12.

[180] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), p.192.

[181] Financial Conduct Authority, "Effectiveness and proportionality: our financial crime priorities — speech by Rob Gruppetta, Head of Financial Crime Department" (10 November 2016), *https://www.fca.org.uk/news/speeches/effectiveness-proportionality-financial-crime-priorities* [Accessed 19 September 2020]. The voluntary exchange of information sharing was introduced by the Criminal Finances Act 2017, which introduced by the Proceeds of Crime Act 2002 s.3392B to s.339ZG and the Terrorism Act 2000 s.21CA to 21CF.

[182] See AUSTRAC, "Fintel Alliance" (n/d), *http://www.austrac.gov.au/about-us/fintel-alliance* [Accessed 19 September 2020]. See Law Commission, *Anti-Money Laundering* (2018), p.171.

[183] See Monetary Authority of Singapore, "CAD and MAS Partner Industry Stakeholders to Fight Financial Crimes" (24 April 2017), *http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/CAD-and-MAS-Partner-Industry-Stakeholders-to-Fight-Financial-Crimes.aspx*, [Accessed 17 February 2019].

[184] Hong Kong Monetary Authority, "Fraud and Money Laundering Intelligence Taskforce launched" (26 May 2017), *https://www.hkma.gov.hk/eng/key-information/press-releases/2017/20170526-3.shtml* [Accessed 22 September 2020].

[185] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), p.6.

The exchange of information has been facilitated by the Criminal Finances Act 2017, which permits "voluntary disclosures within the regulated sector" as an additional exchange of information mechanism.[186] The aim of these statutory provisions is to permit reporting entities to share information with each other on a voluntary basis in relation to a suspicion that a person is involved in committing a money laundering or terrorist financing offence.[187] This provision supports the pre-existing statutory provisions introduced by the Crime and Courts Act 2013. which permits reporting entities to act as information gateways to facilitate the exchange of information between the private sector and law enforcement agencies.[188]FATF described this as a

> "strong feature of the system … [that] enables any person across the public or private sector to voluntarily share information with the NCA … this enables it to act as an information intermediary between LEAs and reporting entities. This gateway allows the sharing of confidential information without breaching any duty of confidence owed by the person sharing the information".[189]

Information provided via such mechanisms are referred to as "Super SARs".[190] Additionally, there are two other information sharing agreements—the Financial Crime Information Network (FIN-NET) and the Shared Intelligence Service (SIS), both of which are hosted by the FCA, which permits the sharing of information between LEAs and financial regulatory agencies.[191] It is important to note that this mechanism is voluntary and that a reporting entity is permitted to refuse an undertaking to exchange information. Information-sharing and increased co-operation could assist in ascertaining a more complete financial profile of the customer that would allow financial investigators to focus on certain financial instruments and transactions. However, the composition of JMLIT has been criticised for being too restrictive as noted by the FATF:

> "JMLIT has proved to be a successful partnership between the financial sector and law enforcement agencies. However, some stakeholders felt disenfranchised by their exclusion from it. Many felt that they could provide more useful intelligence if the membership of JMLIT were expanded or if there was greater dissemination of information, particularly regarding emerging trends in money laundering activity."[192]

Another criticism of JMLIT is that it does not apply to reporting entities which are particularly vulnerable to abuse by terrorism financiers. For example, JMLIT

[186] Criminal Finances Act 2017 s.11. The Criminal Finances Act 2017 introduced these measures into the Proceeds of Crime Act 2002 ss.339ZB-339ZG and the Terrorism Act 2000 ss.21CA-CF.

[187] The Home Office, *Home Office Circular: Criminal Finances Act 2017 — Money Laundering: Sharing of information within the Regulated Sector Sections 339ZB-339ZG* (2018), para.2.

[188] Crime and Courts Act 2013 s.7.

[189] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), p.57.

[190] See Law Commission, *Anti-Money Laundering* (2018), p.44.

[191] HM Treasury, "Call for information: anti-money laundering supervisory regime" (16 March 2017), *https://www.gov.uk/government/consultations/call-for-information-anti-money-laundering-supervisory-regime/call-for-information-anti-money-laundering-supervisory-regime* [Accessed 19 September 2020]. Also see Financial Conduct Authority Office for Professional Body Anti-Money Laundering Supervision (OPBAS), *Sourcebook for Professional Body Anti-Money Laundering Supervisors* ( 2018), pp.19, 20. For a brief discussion, see Royal United Service Institute for Defence and Security Studies, *Known Unknowns Plugging the UK's Intelligence Gaps on Money Laundering Involving Professional Services Providers* (2018).

[192] Financial Action Task Force, *Anti-money Laundering and Counter-terrorist Financing Measures* (2018), p.165.

has focused on working with the financial services sector, yet there is no evidence of it engaging with other professions such as accountants,[193] lawyers [194] and estate agents.[195] In 2018, the Law Commission published a consultation paper seeking views on proposals to reform DATF SARs.[196] The Law Commission considered if the remit of JMLIT should be extended to include a broader range of reporting entities from the entire regulated sector in order to "provide a better understanding of relevant intelligence through the sharing of information across multiple sectors".[197] In response, the NCA stated "we do not believe that a simple expansion of the current JMLIT would be the most effective mechanism for wide engagement".[198] Conversely, the City of London Police suggested that JMLIT could contain a number of "sub-sets … concentrating on different sectors thereby allowing full access or the ability for JMLIT to co-opt additional members on a short-term basis to allow for their resources/expertise in connection with a particular piece of work".[199]

Social media monitoring could assist with the voluntary exchange of information and would represent a far more cost effective mechanism than extending the DATF SARs regime. If social media platforms are brought within the scope of these reporting obligations, the exchange of information would be permitted under the Criminal Finances Act 2017[200] and there would be no breach of the General Data Protection Regulations.[201] In order for this process to work, it would require a higher level of collaboration between social media companies and financial institutions. The creation of JMLIT and the resultant information sharing between financial institutions and LEA has resulted in some notable successes and the inclusion of social media platforms could go some way to detecting and possibly preventing acts of terrorism. It is necessary for HMG to widen the scope of the information sharing model created by JMLIT to include social media platforms other industries.

## Conclusion

This article has presented evidence that there are a number of weaknesses with the scope of DATF SARs. Namely, they do not apply to payments made via cryptoassets or payments made via social media platforms. These problems have been exacerbated by HMG's piecemeal approach towards the regulation of cryptoassets. The policy response by HMG towards the evidence presented is all the more striking because of the increased association between terrorism funding and cryptoassets which has been recognised in other jurisdictions, most notably

[193] HM Treasury and HM Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (2017), Ch.6.

[194] HM Treasury and HM Office, *National Risk Assessment of Money Laundering and Terrorist Financing 2017* (2017), Ch.7. Also see Financial Action Task Force, *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals* (2013).

[195] See HM Government, "Estate agents targeted in money laundering crackdown" (4 March 2019), *https://www.gov.uk/government/news/estate-agents-targeted-in-money-laundering-crackdown* [Accessed 19 September 2020].

[196] Law Commission, *Anti-Money Laundering* (2018), p.51.

[197] Law Commission, *Anti-Money Laundering* (2018), p.174.

[198] Law Commission, *Anti-Money Laundering: The SARs Regime Report* (2019), p.44.

[199] Law Commission, *Anti-Money Laundering: The SARs Regime Report* (2019), p.166.

[200] Criminal Finances Act 2017 s.1.

[201] See General Data Protection Regulation (EU) 2016/679; and Information Commissioners Office, *Guide to General Data Protection Regulations* (2018).

in the US. For example, in its 2018 Budget Request, the FBI asked for additional funding to create 80 specialist cybercrime investigators in response to this threat.[202] Similarly, the US Drugs Enforcement Administration took the view that "transnational criminal organisation are increasingly using virtual currencies [cryptoassets] for illicit activities".[203] There is a clear disparity between the evidence as to the use of cryptoassets to fund terrorism and the perceived threat identified by HM Treasury and the NCA. The different opinions from HM Treasury, the NCA and the FCA are unhelpful, and it appears that they have underestimated this particular funding mechanism. HMG is required to implement the 5MLD by 2020, which will result in the formal inclusion of cryptoassets within the DATF SARs reporting regime. However, it is recommended that the HMG should hastily bring forward legislative measures to include this funding mechanism within the scope of the DATF SARs regime. HMG has adopted a rather cumbersome and unco-ordinated policy towards the regulation of cryptoassets, and the current system of self-regulation is insufficient and this lapse in regulation must be reconsidered. This article has presented evidence that terrorism financing has continued to evolve at an unprecedented rate, and that CTF legislation has failed to keep pace. As explained in the third part , terrorism financing has moved away from its traditional funding mechanisms towards exploiting the speed, convenience and anonymity provided by the internet and Dark Web. In particular, this article has identified several examples of terrorism financiers using cryptoassets, such as Bitcoin, and a wide range of social media platforms such as YouTube, Facebook and Twitter. There is no doubt that terrorism financing via social media platforms, the "Dark Web" and heavily encrypted mobile devices is an unprecedented problem. For example, the ability of any Facebook user to transfer money to a "friend" is almost impossible to police. This is further exacerbated by the uncertain application of DATF SARs to payments made by this platform. In order to address this weakness, this research advocates the extension of the information-sharing platform JMLIT to include social media providers. This would permit LEAs, supervisory agencies, the NCA and the UK security services to develop a greater understanding of the financial undertakings of a suspected terrorism financier who has been subject to a DATF SAR. The current facilitation of the exchange of information by JMLIT has proven to be a success, and the model has been adopted by several other countries including Singapore, Hong Kong and Australia. The inclusion of social media platforms within this exchange of information model would represent a bold and innovative step into the regulatory unknown, and it would go some way to redressing the current loopholes and uncertainty in the scope of the DATF SARs regime.

[202] United States Department of Justice, *FY 2018 Authorisation and Budget Request to Congress* (2017), paras 5.1 to 5.3.
[203] United States Department of Justice, *Drug Enforcement Administration* (2017), pp.13–131.