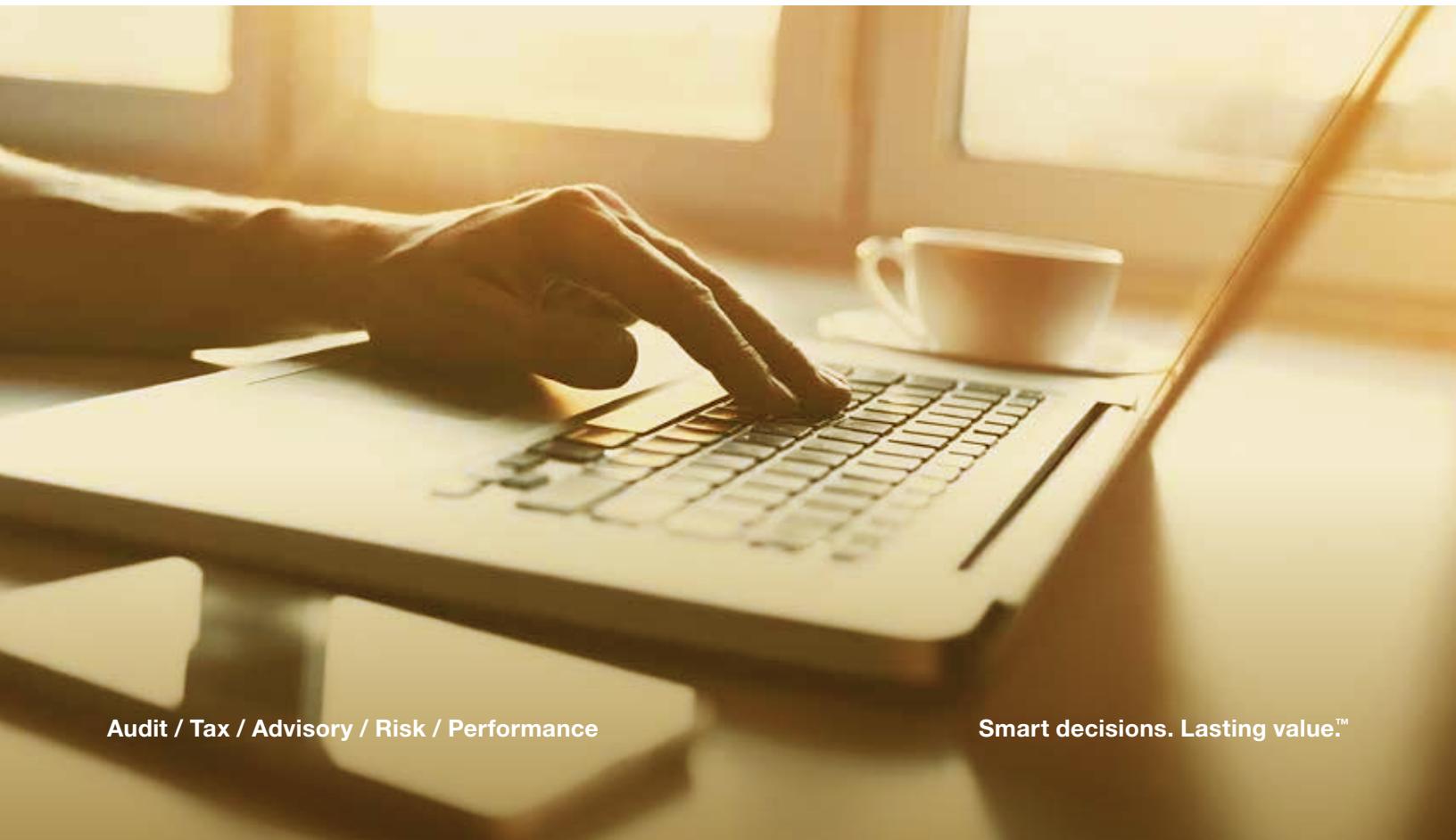




September 2017

Virtual Currency and Risks for Terrorist Financing

An article by Troy M. La Huis and Thomas E. McKeown, CFE



In recent years, virtual currencies such as bitcoin have garnered media attention and have become increasingly popular for both legitimate and nefarious activities. Despite their niche status, virtual currencies are rapidly gaining acceptance in the marketplace. While most individuals and groups using virtual currency are aboveboard, terrorist groups have also recognized virtual currencies as a means to an end, and that is a troublesome and dangerous development.

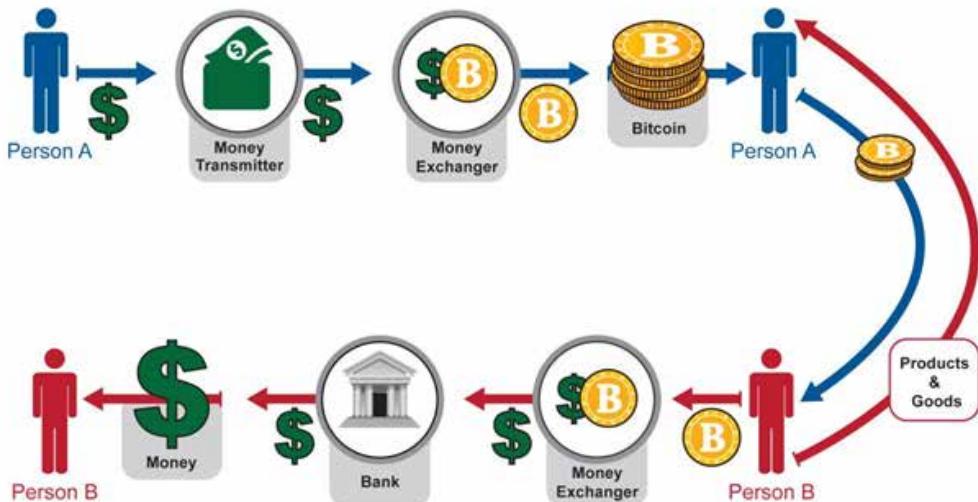
As virtual currencies gain traction in the general market, terrorist financing (TF) risks will also grow, forcing government and private sector entities to develop methods to combat the terrorist financing risks associated with virtual currencies.

Overview of Virtual Currency

Several types of virtual currencies exist in the market today, all of which fall into convertible/nonconvertible and centralized/decentralized virtual categories. The convertibility of a virtual currency refers to its ability to be converted into a traditional currency. A nonconvertible currency cannot be converted into traditional currency. However, a secondary market for a nonconvertible currency could develop. Centralized virtual currency refers to virtual currency that is administered by a central authority. Noncentralized virtual currency is not administered by a central authority and uses a peer-to-peer sharing network.

Virtual currency that is convertible and noncentralized is commonly referred to as cryptocurrency. Most popular virtual currencies, such as bitcoin and Ripple, are classified as cryptocurrency. The top 10 most common cryptocurrencies have a market cap of approximately \$75 billion, with bitcoin having the largest market cap (approximately \$45 billion).¹ In order for a cryptocurrency to be converted into a traditional currency, it must go through a virtual currency exchange. A virtual currency exchange is defined as a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency for a fee.² The exhibit below is an example of the flow of currency in a typical virtual currency transaction between two parties.³

Virtual Currency and Exchange of Products and Goods



Source: Jennifer Shasky Calvery, Statement Before the United States Senate Committee on Homeland Security and Government Affairs, Nov. 18, 2013, p. 4.

Current Trends

In 2015, the Financial Action Task Force (FATF) released a report summarizing current and emerging terrorist financing trends. Of these trends, the most significant is the financing of foreign terrorist fighters (FTFs) and their activities. Although FTFs are not new, there has been a significant increase of individuals in this group, and they are considered a main form of material support to terrorist organizations.⁴

Travel is the primary expense for FTFs. Typically, their modest funding needs include financial support for transportation, travel from their home countries into conflict zones, lodging, food, and other general living expenses. Since travel costs tend to be fairly low, it can be challenging to track and prevent these transactions. According to the FATF report, Saudi authorities concluded that many of their citizens who became FTFs had account activity that was difficult to flag because it appeared normal in relation to their income levels.⁵ The FATF has also identified social media and crowdfunding websites as resources terrorist groups use to gather information and employ large-scale fundraising efforts for operational needs.

The relative anonymity of social media makes it an appealing option for facilitating terrorist financing activities.⁶ Crowdfunding websites give these organizations a wider audience of potential sympathizers and recruits while simultaneously disguising

the true use of the funds. Additionally, crowdfunding websites can also be used to transfer funds abroad while avoiding regulated financial entities.⁷ For example, after receiving a tip that a terrorism suspect had left Canada, Canadian authorities discovered that the suspect had used an international crowdfunding website to conduct transactions to raise funds for his travel to the Middle East.⁸

Virtual Currency and Terrorist Financing

In its 2015 report “Emerging Terrorist Financing Risks,” the FATF identifies virtual currency as a serious potential risk for terrorist financing. Law enforcement agencies are also concerned about the use of virtual currency for terrorist financing and have identified terrorist affiliated websites used to promote bitcoin donations. Their investigations have also observed internet discussions among terrorists regarding the potential of using virtual currency to purchase weapons.⁹

A recent example is the case of Ali Shukri Amin. Amin was convicted for conspiring to provide material support and resources to the Islamic State (IS). He used Twitter to provide instructions on how to use bitcoin to mask funds being sent to IS, to develop financial support for IS using virtual currency, and to establish a secure donation system that would help facilitate the travel of supporters and FTFs

to conflict areas. One specific instance involved Amin tweeting an article about bitcoin and how it can be used to fund the efforts of jihadis.¹⁰ Although Amin was unsuccessful in his efforts to raise funds for IS, this incident demonstrates how terrorist groups are actively exploring new ways to obtain funds. The Amin case conclusively shows the attempted integration of virtual currency for use in operations, funding of FTFs, and the widespread reach of information through social media outlets.

What's the Appeal?

Several features of virtual currency make it an appealing option for terrorist organizations. First, the relative anonymity that virtual currency affords its users may be most appealing. Digital wallets, which serve as mediums for storing and transferring virtual currency, typically do not require a layered identification process from their owners, and what is required can often be fabricated to conceal the true identity of the owner. Some of the more popular digital wallets require only an email address to register in order to protect the personal information and privacy of the user. Although the virtual currency technology blockchain technically records all the details of a transaction, it is of little use in identifying terrorist financing activities if the information behind the corresponding wallets is fabricated.

Uneven regulation and ease of use are two other appealing features of virtual currencies. The FATF has recommended the regulation of virtual currency exchanges to include controls to prevent terrorist financing, but not all jurisdictions have implemented this recommendation.¹¹ Since some unregulated virtual currency exchanges do not require or verify the personal information of the transaction parties, transferring virtual currency to finance operations is an appealing option for terrorist organizations.¹² The relative ease of conducting a virtual currency transaction is also a valuable feature since it allows groups and individuals that lack in-depth technical expertise to conduct and facilitate financial transactions.¹³

The decentralized nature of most virtual currency also makes it an attractive financing option. Since there is no central authority for decentralized virtual currency, the currency exchanges are largely unregulated and lack adequate controls for preventing terrorist financing. Decentralization also makes it difficult for law enforcement to target and investigate a central location or single administrator.¹⁴

The global reach and speed of virtual currency transactions is especially useful for terrorist groups. Virtual currency technology allows transactions to be conducted nearly instantaneously and across any borders. These characteristics are important for a group trying to quickly move illicit funds to and from a wide variety of places around the world.¹⁵

Current and Potential Future Regulations

Although considerable terrorist financing risks associated with virtual currency exist, various governments have acknowledged its potential benefits for legal financial transactions, and they have begun implementing regulations and rules for its use. Countries around the world have adopted varying stances regarding virtual currency, ranging from overall acceptance to an outright ban of any type of virtual currency transactions.

Of the countries that do allow virtual currency transactions, the degree of regulation varies substantially. In the United States, virtual currency exchangers and administrators are subject to the same Financial Crimes Enforcement Network (FinCEN) regulations that govern money service businesses.¹⁶ Some of these regulations include establishing an anti-money laundering and counterterrorist financing program, submitting currency transaction reports, and adhering to various record retention requirements, among other rules.

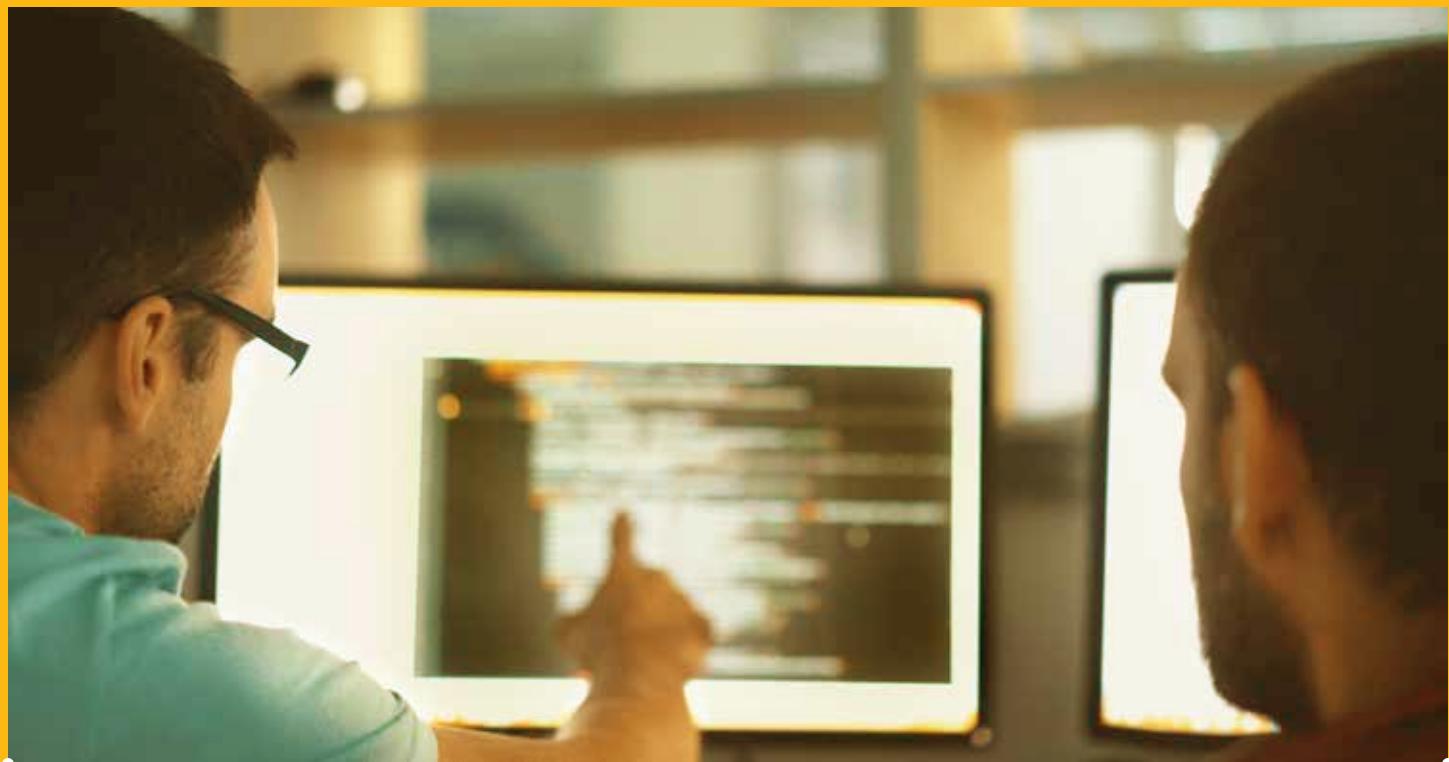
These regulations are a positive step; however, it remains to be seen how effective they are in practice. In the future, it may prove beneficial to require exchangers to establish customer due diligence and enhanced due diligence requirements for virtual currency exchanges in an effort to identify potential transactions used for terrorist financing. Since most virtual currency exchanges operate without a central administrator or are based outside of the United States, enforcing regulations could prove difficult. To help combat this potential problem, international cooperation will be necessary to effectively address the potential terrorist financing risks associated with virtual currency.

The international community will need to establish uniform regulatory requirements and restrictions on virtual currency and continue to monitor and assess risks that arise as the virtual currency market continues to grow and develop.¹⁷ Governments around the world must also understand the risk that too many regulations could drive the exchange of virtual currency underground, making it more difficult to monitor and prevent its use for terrorist financing.¹⁸ Moving forward, it will be important for the public and private sectors to share intelligence regarding the use of virtual currency for illicit use in connection with terrorist financing.

Challenges Ahead

The use of virtual currency will likely become more accepted in the financial community. In the future, the value of bitcoin, the most prevalent virtual currency, is expected to increase due to several factors such as growing popularity and acceptance of bitcoin payments by large companies.¹⁹ Additionally, the use of virtual currency is expected to grow in both the Middle East and Africa in the coming years because of its potential to reduce the costs of international remittances.²⁰

Even though the financial sector is becoming more efficient at detecting and preventing terrorist financing methods, these groups will undoubtedly seek out alternative methods to fund their organizations. As terrorist groups continue to look for innovative ways to finance their organizations and conceal the nature of their transactions, virtual currency use may become more widespread, requiring the international community to join forces to combat them.



Learn More

Troy La Huis, Principal
+1 616 233 5571
troy.lahuis@crowe.com

Thomas McKeown
+1 312 966 3020
thomas.mckeown@crowe.com

¹ CryptoCurrency Market Capitalizations, online resource, <http://coinmarketcap.com/>

² "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," Financial Action Task Force Report, June 2014, p. 7, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

³ Jennifer Shasky Calvery, Statement Before the United States Senate Committee on Homeland Security and Government Affairs, Nov. 18, 2013, p. 4, <https://www.fincen.gov/news/testimony/statement-jennifer-shasky-calvery-director-financial-crimes-enforcement-network-0>

⁴ "Emerging Terrorist Financing Risks," Financial Action Task Force Report, October 2015, p. 24, <http://www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html>

⁵ Ibid, p. 24.

⁶ Ibid, p. 30.

⁷ Ibid, p. 31.

⁸ Ibid, p. 31.

⁹ Ibid, p. 36.

¹⁰ Ibid, p. 36.

¹¹ Dong He et al., "Virtual Currencies and Beyond: Initial Considerations," International Monetary Fund Staff Discussion Note 16/03, Jan. 20, 2016, p. 28, <http://www.imf.org/en/Publications/SPROLLS/Staff-Discussion-Notes?page=2>

¹² Ibid.

¹³ Alan Brill and Lonnie Keene, "Cryptocurrencies: The Next Generation of Terrorist Financing?," Defence Against Terrorism Review, Vol. 6, No.1, Spring & Fall 2014, p. 14, <http://www.coedat.nato.int/publication/datr/volumes/datr9.pdf>

¹⁴ "Virtual Currencies," Financial Action Task Force Report, p. 9.

¹⁵ Brill and Keene, "Cryptocurrencies," p. 27.

¹⁶ Federal Financial Institutions Examination Council, "Nonbank Financial Institutions – Overview," Bank Secrecy Act Anti-Money Laundering Examination Manual, https://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_091.htm

¹⁷ "Guidance for a Risk-Based Approach to Virtual Currencies," Financial Action Task Force Report, June 2015, p. 8, <http://www.fatf-gafi.org/publications/fatfgeneral/documents/guidance-rba-virtual-currencies.html>

¹⁸ Ibid, p. 9.

¹⁹ Jemima Kelly, "Record Highs Predicted for Bitcoin in 2016 as New Supply Halves," Reuters, Dec. 23, 2015, <http://www.reuters.com/article/us-global-markets-bitcoin-analysis-idUSKBN0U60GM20151223>

²⁰ He et al., "Virtual Currencies and Beyond," p. 21.