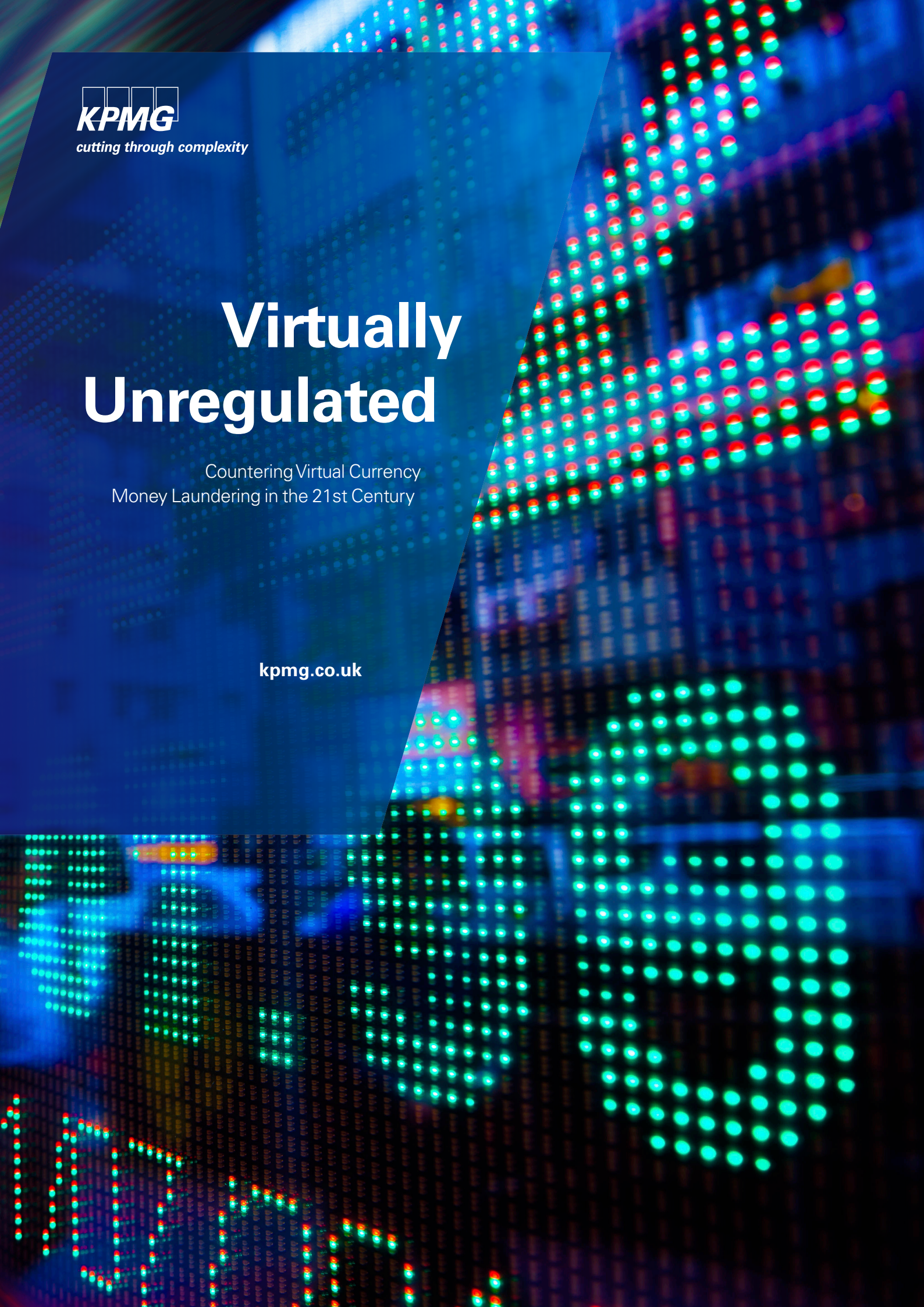


KPMG
cutting through complexity

Virtually Unregulated

Countering Virtual Currency Money Laundering in the 21st Century

kpmg.co.uk

The issue

The virtual currency industry has been under increased scrutiny to implement robust Anti Money Laundering (AML) controls by regulators, investors, and businesses alike. Virtual currencies have been around for many years, but recent evolutions in the industry through the emergence of Bitcoin and other similarly structured forums have resulted in the development gaps in regulations. Whether this means virtual currencies become a money launderers dream for the 21st Century, or the current concerns are proved to be little more than a storm in a teacup remains to be seen. However, what is certain is, while virtual currencies previously existed in the form of bonus points or loyalty rewards, valued within a specific company or limited virtual community, they can now be converted into traditional forms of currencies on a global scale, and can be transferred across borders with limited regulatory or industry oversight.

The implications of this change in dynamics loom large, as it poses a threat to the traditional banking industry as well as the current safeguards that protect legitimate, law-abiding customers, end users, intermediaries, and investors. Virtual currencies present similar risks to physical cash in terms of anonymity and the lack of audit trails around transactions, but with a wider reach due to the emergence of global market places and exchanges where they can be traded freely across the globe on a real-time basis. This paper considers the types of virtual currencies that exist, the regulatory landscape, and the extent of money laundering risks posed by the industry in order to consider the long-term sustainability of the virtual currency industry.

A closer look at virtual currencies

Virtual currencies hold a particular value within a particular community and are used to buy both real and virtual goods and services. Not to be confused with e-money which is simply the electronic trading and exchange of traditional currencies, virtual currencies are not regulated and exist as a digital commodity relying largely on customer demand. According to the European Central Bank 2012 report on Virtual Currency Schemes, there are three types of virtual currencies that exist: A closed system, unidirectional system, and bidirectional system[i].

While a closed system represents the ability to use real value currencies to buy virtual currencies that can only be used for virtual goods and services, a unidirectional system allows the virtual currencies to be used for real goods and services as well. In a bidirectional system virtual currencies can buy both real and virtual goods and services, and the virtual currencies to buy *real value* currencies[ii]. This paper is concerned with the last of these models as this is becoming increasingly prevalent with the rise of Bitcoin, and is the model which is causing greatest concern to regulators and law enforcement around the world.

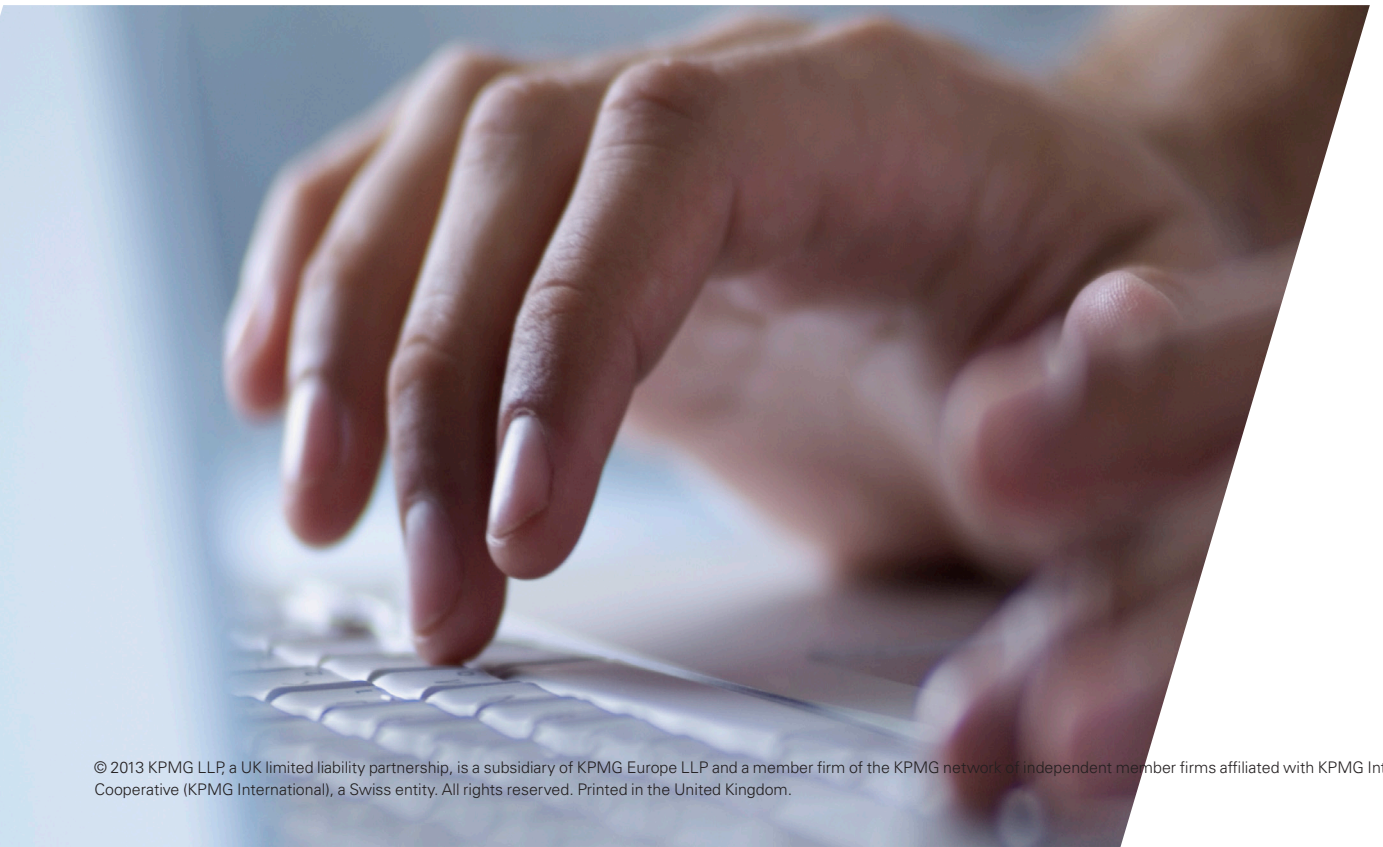
The Financial Crimes Enforcement Network (FinCEN) in the United States has identified that those who operate in the virtual currency world will fall under one of three categories: Users, exchangers, or administrators[iii]. Users are defined as those who buy or use the virtual currency while exchangers are those who operate in the business of exchanging virtual currencies for real or other virtual currencies. Lastly, administrators are those that have the authority to issue, withdraw or redeem the virtual currencies.

---

[i] "Virtual Currency Schemes". European Central Bank. October 2012. Last retrieved on 16/09/2013 **here** pg 14-15

[ii] "Virtual Currency Schemes". European Central Bank. October 2012. Last retrieved on 16/09/2013 **here** pg 14-15

[iii] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. US Financial Crimes Enforcement Network. Guidance FIN 2013-G001. Issued March 18, 2013. Last retrieved on September 16, 2013. **here**



Regulatory landscape

On a global scale, many regulatory bodies and other government agencies have been assessing the vulnerabilities of the virtual currency industry to money laundering risks, and have been issuing guidance and performing industry-specific reviews to better understand and manage these risks. However, regulators have not yet developed a consistent approach tailored to the distinctive aspects of virtual currencies, which represents a particular challenge as these are global networks, whilst regulation has traditionally been developed in a localised manner.

For example, Tom Robinson, the co-founder of a Bitcoin currency exchange called Bitprice, has recently suggested that UK regulators are lagging behind those in Germany and the US in terms of regulating and legitimising the virtual currency industry through classification and regulation[iv]. It is easy to understand his conclusions when we look at the recent regulatory reaction to Bitcoin in each of those three countries.

FinCEN has provided industry guidance that establishes that certain administrators and exchangers of virtual currencies must register as MSBs and have a legal obligation to comply with the Bank Secrecy Act (BSA)[v]. Simultaneously, the US Federal Bureau of Investigation (FBI) and the US Senate have announced an initial investigation into Bitcoin and its involvement in money laundering schemes[vi].

While the US regulators have chosen to focus on the obligations of the exchangers and administrators, German regulators have concentrated their efforts on regulating the users by classifying virtual currencies such as Bitcoin as "unit of account"; this classification has both legal and tax implications for users as it now subjects them to a capital gain tax if held for less than one year[vii] .

In contrast to both the US and German approach, the UK Financial Conduct Authority (FCA) has recently confirmed its position of "keeping an eye on Bitcoin developments" rather than actively pursuing regulation at this time[viii]. Other examples of the inconsistent approach to regulation include China's prohibition of all virtual currencies from purchasing real goods and services[ix] as well as Thailand's country-wide banning of Bitcoin trading in July 2013[x].

With the virtual currency industry expected to continue to grow, guidance from Supra-national bodies like the Financial Action Taskforce to help shape the regulatory landscape in a more consistent way is necessary and much-needed.

[iv] Moodley, Kiran. UK downplays talk of regulating Bitcoin. CNBC. September 5, 2013. Last retrieved on 16/09/2013. **here**

[v] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies. US Financial Crimes Enforcement Network. Guidance FIN 2013-G001. Issued March 18, 2013. Last retrieved on September 16, 2013. **here**

[vi] DHS and FBI Input on Bitcoin Sought. Economic Policy Journal. August 15, 2013. Last retrieved on 16/09/2013. **here**

[vii] "Germany plans tax on bitcoin after virtual currency recognised as 'private money'. Telegraph. August 19 2013. Last retrieved on 16/09/2013. **here**

[viii] Moodley, Kiran. UK downplays talk of regulating Bitcoin. CNBC. September 5, 2013. Last retrieved on 16/09/2013. **here**

[ix] Wortham, Zach. Virtual Money Prohibited for Trading in Real Goods. December 2, 2010. Last retreived on 16/09/2013. **here**

[x] Davidson, Kavitha. "Bank of Thailand Bans Bitcoins". The Huffington Post. July 31, 2013. Last retrieved on 16/09/2013. **here**

Money laundering – Virtual currencies

It is evident that virtual currencies currently pose a wide range of money laundering risks which are particular to its industry, but also compound the more traditional money laundering challenges that financial institutions face today. The leading challenge for the virtual currency industry is its anonymous nature which allows criminals to participate in financial markets and convert, transfer, and withdraw funds without detection.

The difficulties posed by anonymity are exacerbated by the ease in movement of funds across borders, and the speed at which the industry operates. The challenges of identifying suspicious activity and tracking customer activity increase significantly when anonymity shields the customer identity, hinders the identification of sources of funds and the economic purpose of a transaction.

The fact that anonymity thrives in the virtual world means that regulators and the industry at large will have to manage the inevitable risk of facilitating money laundering and enabling criminal activities. Similarly, industry-specific money laundering training and staff awareness are also areas of weakness for those operating within the virtual industry. AML staff training, including familiarisation with red flags and suspicious customer activity, will be paramount to preventing and reporting money laundering activity.

Testing the robustness and effectiveness to systems and controls relating to anti-money laundering initiatives has become paramount to safeguarding against criminal activities. While traditional banking systems have a relatively secure technology framework in place and typically employ ongoing assurance programmes, virtual currencies operate on a peer-to-peer basis which may allow criminals to evade these systems and controls in order to facilitate criminal activities linked to money laundering, cybercrime, and even national security. One of the more publicly known attempts to hack Bitcoin operating systems occurred in April 2013 when MTGox Exchange underwent a series of attacks through Distributed Denial- of-Service. There has been speculation that security breaches have been caused as a means of manipulating the value of the currency in order to capitalise on the fluctuation in prices as a result of the publicity of a technology failure[xi].

According to an academic study at Carnegie Mellon University, Bitcoin has helped transfer approximately $1.2 million dollars in sales of illegal narcotics associated with the Silk Road Marketplace (the largest online drug marketplace) through the use of its virtual currency[xii]. This study illustrates the exploitation of the virtual currency industry as a breeding ground for laundering money associated with various illegal activities. Following this report, the Silk Market was shut down in October 2013, after the US Federal Investigation Bureau arrested its alleged founder Ross Ulbricht for charges relating to money laundering, narcotics trafficking, and cybercrime[xiii]; Bitcoin was featured throughout the FBI report in relation to these charges as a means of payment[xiv]. The report supports the assertion that criminals engaging in a wide range of illegal activities are attracted to the use of virtual currencies due to the anonymity which they offer. While there are many legitimate businesses and individuals that use this service, it can also be exploited by terrorists, human traffickers, drug smugglers, illegal weapons dealers, ponzi scheme operators and other types of fraudsters.

Similarly, there is also the risk of virtual currency firms unwittingly enabling transfers to and from sanctioned individuals and geographies. This risk is inherent in an anonymous environment where screening is almost impossible in the absence of identifying information on the individuals or entities involved in a transaction.

[xi] Hack Attacks Hit Bitcoin Exchange Rates. BBC News. April 2013. Last retrieved on 08 October 2013. **here**

[xii] Cristin, Nicholas. Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. Carnegie Mellon University. July 30, 2012. Last retrieved on 16/09/2013. **here** pg 24-25.

[xiii] Hodson, Hal. New Scientist. Last retrieved on October 8 2013. **here**

[xiv] **https://www.cs.columbia.edu/~smb/UlbrichtCriminalComplaint.pdf**

Recent examples of AML failures

Virtual currency exchanges that enable conversion of virtual currencies into traditional forms of currency as well as anonymous withdrawal of such funds currently face significant fines, penalties and regulatory action for not effectively addressing the inherent risks of money laundering and associated financial crime. For example, in May 2013, Liberty Reserve SA, a virtual currency exchange incorporated in Costa Rica, was charged by the US Department of Justice (DOJ) for conspiracy to launder money through a $6 billion money-laundering scheme[xv]. This case represented the largest successfully prosecuted international money-laundering case brought by the US[xvi]. Regulators employed a cooperative approach in pursuing this particular case and also set precedents as the investigation rested on the first search warrant to be executed by the US against a cloud-based server.

It is also worth considering the third party risk the virtual industry could pose to regulated financial institutions through this same example. Liberty Reserve SA maintained a business relationship with approximately 35 different registered exchange companies and payment service providers, whereby customer transfers were conducted through intermediaries that included a number of well known Payment Service Providers and Credit Card companies[xvii]. As the virtual currency industry develops, third party and intermediary liability will be an area of growing consideration, and regulated institutions will have to consider whether their systems and controls are sufficient to identify suspicious behaviours in relation to the virtual currency industry.

Similarly, Bitcoin exchanges have been under investigation for potentially enabling money laundering and related illegal activity. Mt.Gox, a Japan-based organisation that claims to process about 80% of the world's Bitcoin exchanges[xviii], had its accounts at various financial institutions frozen, estimated at $2.9 million dollars pending a US FinCEN investigation related to registration and licensing breaches[xix].

Conclusion

The recent high profile cases in the virtual currency industry involving account seizures and money laundering indictments imply that regulators are moving virtual currencies closer to the top of their agenda and will continue to monitor this industry going forward. As innovations in payments emerge, regulators will continue to respond to ensure a safe and compliant environment in which businesses and individuals operate, but the challenge remains on coordinating a globally consistent approach. Implementing robust AML systems and controls which promote transparency and address the issues associated with anonymity is the first step those operating in the virtual currency industry can take to promote the regulatory support required for the industry to achieve sustainable long-term growth and mitigate regulatory risks.

Financial institutions and exchanges that provide the link between traditional and virtual currencies will also need to consider whether their existing systems and controls to prevent and detect money laundering remain fit for purpose in dealing with this emerging industry, and should continually monitor these as the industry evolves in future.

[xv] Flitter, Emily. U.S. accuses currency exchange of laundering $6 billion. Reuters. May 28, 2013. Last retrieved on 16/09/2013. **here**

[xvi] Sandler, Linda. Liberty Reserve Joe Bogus Account Said to Reflect Evasion **here**

[xvii] Flitter, Emily. U.S. accuses currency exchange of laundering $6 billion. Reuters. May 28, 2013. Last retrieved on 16/09/2013. **here**

[xviii] Wolf, Brett. "U.S. seizes accounts of major Bitcoin exchange based in Japan." Reuters. May 17, 2013. Last retrieved on 16/09/2013. **here**

[xix] "US govt seized $2.9m from MT. Gox's Dwolla account". Finextra. August 20, 2013. Last retrieved on 16/09/2013. **here**

Contact us

Brian Dilley
Global Head of AML Services
T: + 44 (0) 20 7896 4843
E: brian.dilley@kpmg.co.uk

Neal Dawson
KPMG Senior Manager, Forensic
T: + 44 (0) 20 7694 5552
E: neal.dawson@kpmg.co.uk

Jodi Schutze
KPMG Assistant Manager, Forensic
T: + 44 (0) 20 7694 5192
E: jodi.schutze@kpmg.co.uk

Designed and produced by Create Graphics CRT006265