United States anti-money laundering efforts in 2013

While the potential stores of value other than standard currency as conduits for money laundering is nothing new, technological innovations such as Bitcoin have troubled regulators, especially in the US. Raymond L. Sweigart, Aaron R. Hutman and Stephanie Rohrer of Pillsbury Winthrop Shaw Pittman LLP, describe how US anti-money laundering policy is developing due to this new frontier.

In recent developments in US anti-money laundering ('AML') policy, the US Treasury Department has been marching on seemingly unrelated fronts, wrestling with virtual currencies, providing guidance for money services businesses ('MSBs') and pursuing consensus on new standards for investigating beneficial ownership. What ties these efforts together? US officials appear focused in the face of technological and legal innovation on reinforcing the gatekeeping obligations of financial institutions, new and old, including maintaining an anti-money laundering program, filing of suspicious activity reports, and maintaining customer and transactional information.

Virtual currency, prepaid access and MSBs

Whether the popular, fast-appreciating digital or 'crypto' currencies like Bitcoin represent just a passing fad or a form of exchange with staying power, they are just one of the many new electronic and internet stores of value. Virtual gold or money in online games, credits relating to gambling sites, and prepaid value cards can have real-world monetary value and be traded, transferred and purchased. This poses a challenge to AML regulators and law enforcement. Criminals, terrorist groups and rogue regimes have long used stores of value other than currency to launder and transfer funds.

In response, the US Government and regulators around the world have sought to expand the definition of 'financial institution' and the range of businesses requiring AML programs and reporting to include gambling enterprises, gems and precious metals, real estate, and vehicles/aircraft sales. Large cash purchases require reporting in the US and Europe. All of these reflect stores of value that can be used in lieu of, or to hide, ill-gotten or ill-intended funds.

In response to this fast evolving scene, the US Treasury Department's Financial Crimes Enforcement Network ('FinCEN'), as primary AML regulator, has issued recent guidance on virtual currency, prepaid access and for MSBs.

(1) Virtual currency guidance

On 18 March 2013, FinCEN issued interpretive guidance identifying the virtual currency activities that it considers to be 'money transmission' services under the Bank Secrecy Act ('BSA') and hence subject to AML requirements as well as the appropriate regulatory treatment of users, exchangers and administrators[1]. This guidance distinguishes 'virtual' and 'real' currency, defining the former as a medium of exchange that operates like a currency in some environments but does not have all the attributes of real currency, and the latter as 'the coin and paper money of the United States or of any other country that is designated as legal tender.'[2]

Not subject to AML requirements are 'users' of virtual currency, those who obtain - including purchasing, earning or 'mining' - virtual currency to purchase goods or services. However, exchangers and administrators[3] generally are subject to AML regulations where they accept and transmit a convertible virtual currency, or buy or sell convertible virtual currency for any reason[4]. The guidance goes on to address the following scenarios:

A) Electronic trade in virtual currencies

Trade, exchange and brokering of virtual currency or e-precious metals in many situations will constitute money transmission and give rise to AML requirements. The exception would be *bona fide* exchange where a customer purchases or sells the currency. Otherwise, where an exchanger or administrator transfers funds to a third party not part of a currency transaction, this would be money transmission. The guidance provides examples of this sort of money transmission: (i) the transfer of funds between a customer and a third party, funding a customer's account; (ii) the transfer of value from a customer's currency or commodity position to the account of another customer; and (iii) the closing out of a customer's currency or commodity position, with a transfer of proceeds to a third party.

B) Centralised convertible virtual currencies

FinCEN concluded that where a convertible virtual currency has a centralised repository, the administrator is a money transmitter and therefore an MSB where the administrator allows (i) transfer of value between persons or (ii) from one location to another. This is the case whether the value is denominated in real or

convertible virtual currency.

C) De-centralised convertible virtual currencies

With a de-centralised virtual currency like Bitcoin, FinCEN provides that a person that creates units of virtual currency and sells those units for real currency or an equivalent value is transmitting it to another location, making them a money transmitter and thus an MSB. However, someone only mining or purchasing Bitcoin and then using it to purchase actual or online goods/services is not an MSB. On the other hand, a person who accepts a virtual currency like Bitcoin from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency is a money transmitter and an MSB.

(2) Prepaid access

Another store of value sometimes identified with, but differing from, virtual currency is prepaid access. Prepaid access includes things like public transportation cards, retail gift certificates and university cafeteria programs. US regulators consider certain features or dollar amounts in prepaid access to present a heightened risk of money laundering. FinCEN updated its rules for prepaid access (formerly 'stored value') in 2011 and provided further direction this year[5].

Providers and sellers of prepaid access are subject to AML program and reporting requirements, while providers have an additional registration requirement. The 'provider' of prepaid access is normally the person with principal oversight and control over the program while a 'seller' includes the retailer or seller of prepaid access products with some exceptions.

There are a few carve outs from what is considered prepaid access for AML purposes that help prevent over-inclusion. Exempted are prepaid access products of $1,000 or less; closed loop prepaid access products sold in amounts of $2,000 or less; certain health and dependent care prepaid access programs; and payroll products with restrictions including no international transmission or transfer among users.

In November 2013, FinCEN published an administrative ruling that compared and contrasted prepaid access with virtual currencies, addressing what happens when closed loop prepaid access (e.g. a retail card with dollar value in store) is traded on an online secondary market. See FIN-2013-R003 (13 November 2013). FinCEN determined that the use or availability of a secondary market does not affect the character of the prepaid access product, or the obligations of the original provider or seller. Thus, if the product originally met the requirements for exclusion under the closed loop exception, then it will continue to be excluded.

In the virtual currency guidance discussed above, FinCEN differentiated prepaid access, determining that a 'person's acceptance and/or transmission of convertible virtual currency cannot be characterized as providing or selling prepaid access because prepaid access is limited to real currencies.'

While FinCEN's virtual currency and prepaid access guidance helps ensure that AML controls are not circumvented at the electronic frontier, US regulators have also faced challenges in clarifying standards for knowing one's customer in more traditional financial institutions.

(3) Enforcement actions

In an example of the concerns raised by the misuse of virtual currency systems, on 28 May 2013 the US Treasury named Liberty Reserve S.A. of Costa Rica as a financial institution of primary money laundering concern under Section 311 of the US Patriot Act[6]. Liberty Reserve offers a web-based money transfer system or virtual currency. FinCEN took this action in conjunction with an indictment charging Liberty and seven of its principals 'for their alleged roles in running a $6 billion money laundering scheme and operating an unlicensed money transmitting business.'[7]

The US investigation found that Liberty Reserve had become 'a preferred method of payment on websites dedicated to the promotion and facilitation of illicit web based activity, including identity fraud, credit card theft, online scams, and dissemination of computer malware.' Liberty Reserve's virtual currency provided users with the capability to conduct anonymous transactions around the world. There was no customer due diligence and the site asked only for a working email address, allowing individuals to open an unlimited number of accounts. By paying an additional 'privacy fee,' users could hide their account number when sending funds within the Liberty Reserve system. With an established account, Liberty Reserve virtual currency could be sent, instantly and anonymously, to any other account holder within the global system.

This enforcement represents the first use of Section 311 special measures by the US Treasury against a virtual currency provider and indicates that AML and anti-terrorism enforcement resources are being targeted at virtual currency risks.

Beneficial ownership

While FinCEN's virtual currency and prepaid access guidance helps ensure that AML controls are not circumvented at the electronic frontier, US regulators have also faced challenges in clarifying standards for knowing one's customer in more traditional financial institutions. Customer

due diligence ('CDD') is a core AML requirement, but both new and long-standing legal artifices can make it difficult for banks and other financial institutions to determine beneficial ownership. Who is truly on the other end of that series of companies, trust funds or agents?

To that end, in March 2012 FinCEN provided an advance notice of proposed rulemaking (the 'ANPR') that would clarify and standardise the requirements that financial institutions have in knowing their customers, and in particular, who the actual, or 'beneficial,' owner is of an account[8]. This has proven a complicated undertaking and, after over a year of comments and stakeholder meetings in major cities around the country, the proposed rule is still pending. Financial institutions are eager for clarity but concerned that FinCEN's requirements might prove unrealistic, too costly or prone to creating competitiveness issues if not applied across all relevant industries.

Present US CDD rules only require financial institutions to obtain beneficial ownership information in two situations: 1) private bank accounts in covered financial institutions; and 2) certain foreign bank correspondent accounts. For these two situations, the ANPR indicates the definition of beneficial ownership would continue as currently defined: 'an individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account.'[9] For other situations, the ANPR proposes a new definition of beneficial ownership that would include either each individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, owns more than 25% of the equity interests in the entity; or if there is no such individual, then the individual who, directly or indirectly, through any contract, arrangement, understanding, relationship, intermediary, tiered entity, or otherwise, has at least as great an equity interest in the entity as any other individual; and the individual with greater responsibility than any other individual for managing or directing the regular affairs of the entity[10].

The current level of effort in determining ownership varies among financial institutions, as does the definition of owner. For example, according to public comments, the threshold used to determine beneficial ownership currently can range from 10 to 25%[11]. How and when ownership information is updated by banks also varies from never refreshing the information, to only upon a triggering event, or periodically. Particular challenges facing financial institutions include: trusts, where the beneficiary information may not be available; intermediated relationships, common in the futures and securities industries, where the customer is another financial institution (including foreign financial institutions) serving its own underlying customers; pooled investment vehicles, where ownership may fluctuate too often to identify a beneficial owner according to a percentage threshold; and agents with confidential relationships, like lawyers and accountants, opening accounts.

Consistent guidance from US regulators is expected to have a significant impact for financial institutions both in the US and around the globe.

Conclusion

US AML efforts continue to place an emphasis on maintaining and strengthening the gatekeeper obligations of financial institutions in national and global efforts to combat laundering, weapons proliferation and terrorist financing. Financial institutions and any parties involved in virtual currency, online systems and prepaid access should continue to monitor regulatory developments and consider whether they have current or potential AML responsibilities or liabilities. It is a brave new world and regulators are watching closely.

Raymond L. Sweigart Partner
Aaron R. Hutman Attorney
Stephanie Rohrer Associate
Pillsbury Winthrop Shaw Pittman LLP
raymond.sweigart@pillsburylaw.com
aaron.hutman@pillsburylaw.com
stephanie.rohrer@pillsburylaw.com

1. http://fincen.gov/statutes_regs/guidance/html/FIN-2013-G001.html
2. 31 C.F.R. § 1010.100(m).
3. An 'exchanger' is a person 'engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.' An 'administrator' is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) that virtual currency.
4. The determination of whether a person is a 'money transmitter' is a matter of facts and circumstances, and specific exceptions are identified in the BSA implementing regulations. See 31 C.F.R. § 1010.100(ff)(5)(ii). Such a person may be an MSB for other reasons, however.
5. 76 Fed. Reg. 45403 (29 July 2011).
6. 31 U.S.C. 5318A. Section 311 grants FinCEN the authority to require domestic financial institutions and financial agencies to take 'special measures' to address a primary money laundering concern (e.g. prohibiting correspondent banking relationships).
7. www.treasury.gov/press-center/press-releases/Pages/jl1956.aspx
8. 77 Fed. Reg. 13046 (5 March 2012).
9. 31 C.F.R. § 1010.605(a).
10. 77 Fed. Reg. 13046 (5 March 2012).
11. http://www.fincen.gov/whatsnew/pdf/20121130CHI.pdf