Bloomberg Law

Privacy Law Watch Bulletin™

Reproduced with permission from Privacy Law Watch, 106 PRA, 6/5/17. Copyright © 2017 by The Bureau of National Affairs, Inc. (800-372-1033) http://www.bna.com

Cryptocurrency

Companies and individuals are concerned about the legality of methods to hide their identity in blockchain transactions, such as those used in bitcoin exchanges, through a mechanism known as ''tumbling.'' The author examines the legality of tumbling under U.S. and Canadian regulations and offers insights on the business effects of tumbling.

Data Security

Bloomberg Law Insight: (Crypto)financial Privacy and Security

By Bijou Lee

Cryptocurrency is digital currency that is not issued or controlled by a central authority. The most well-known cryptocurrency is Bitcoin. Most cryptocurrencies, including Bitcoin, are not totally anonymous because their transaction details are permanently recorded on and visible to anyone looking at the blockchain, i.e. the digital public ledger where details of cryptocurrency transactions are recorded.

There are many effective methods for identifying parties to a blockchain transaction (Transactors). Once a Transactor is identified, their funds and associated transactions can easily be monitored by watching the blockchain. This compromises (crypto)financial privacy and security, and puts parties transacting with that Transactor at risk of identification and monitoring.

A key way to address these privacy and security concerns is to use a privacy-protection tool called ''cryptocurrency tumbling'' or ''mixing'' (''tumbling'', for short). Tumbling works by hiding transaction details by mixing those details with details from other transactions. Without tumbling, it is easy to look at a blockchain, analyze the data, and follow the flow of funds from sender to receiver.

Bijou Lee is the president of B.G.L. Legal in Vancouver.

Tumbling protects privacy by making it difficult for someone to surveil you by tracing your transactional history. The degree of privacy you enjoy increases with each layer of tumbling you perform. The rationale behind tumbling is to make the *cost* outweigh the *benefits* of tracing for the person surveilling you. (The cost of tracing consists of the resources required for tracing transactional history, such as time, computational power, and manpower.) Although absolute privacy or security can never be assured, tumbling is an invaluable tool for protecting parties you transact with and ultimately yourself.

An international discussion has emerged around the question, ''Is tumbling legal''? This article navigates U.S. and Canadian regulations from the perspective of different tumbling participants, and offers a determination on the legality issue. The article concludes with insights on the business impacts of tumbling.

Tumbling methods and types of participants Cryptocurrency tumbling is done in three main ways:

- (1) **Peer-to-peer (P2P) tumbling networks** (such as CoinJoin/JoinMarket),

- (2) **Cryptocurrency tumblers**, also known as ''mixing services'' (such as TumbleBit), and

- (3) **Built-in tumbling cryptocurrencies** (such as Monero).

P2P tumbling networks are a *transaction anonymization method* that operates by users (Peers) joining a ''peer network''. The underlying strategy is, ''When you want to make a payment, find someone else who also wants to make a payment and make a joint payment together.'' Peers can tumble for personal privacy purposes (personal-use Peers) or as a business (business-use Peers).

Cryptocurrency tumblers (tumblers) are *service providers*. Hence, in this article, we will refer to tumbler users as ''Customers''. When a Customer wants to tumble some Bitcoin, for example, they first send the amount to the tumbler. The tumbler takes that amount and tumbles that Customer's Bitcoins with their other Customers' Bitcoins according to an algorithmic method. After the service is complete, the tumbler sends the tumbled Bitcoins back to their customers.

Built-in tumbling cryptocurrencies are *alternative currency products*. Hence, in this article, we will refer to users of built-in tumbling cryptocurrencies as ''Consumers''. These cryptocurrencies are separate and distinct from other cryptocurrencies such as Bitcoin. They are developed specifically to optimize privacy and decentralization. Their methods of tumbling are algorithmically designed and built into the protocol of these cryptocurrencies.

Participants in cryptocurrency tumbling (tumbling participants) should each be conceptualized differently:

- Peers are *active* participants in the network who autonomously collaborate with other Peers.

- Customers are best described as *passive* because they pay to enjoy a service and do not participate in the algorithmic method by which that service is provided. (Note: Algorithms are not created equal, so the effectiveness of tumbling services varies.)

- Consumers of built-in tumbling cryptocurrencies do not decide when or how to tumble their funds. Rather, Consumers *passively* benefit from algorithmically enhanced privacy simply by using the built-in tumbling cryptocurrency to make payments or send/receive remittances. (Note: Monero provides increased transaction privacy settings for an added fee.)

Legality of Tumbling in U.S. and Canada The U.S. and Canada each have legal frameworks that address anti-money laundering and counter-terrorist financing (AML/CFT). FinCEN and FINTRAC are the lead AML/CFT regulators for the U.S. and Canadian federal governments respectively. They perform their duties according to their respective regulatory frameworks: the *Bank Secrecy Act* (BSA) and its regulations (the U.S. Regulations), and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) and its regulations (the Canadian Regulations). The U.S. Regulations and Canadian Regulations impose numerous legal obligations on reporting entities such as record-keeping, identity verification, reporting of suspicious transactions and registration.

Tumbling participants always must be cognizant of whether they are a reporting entity and required to meet these legal obligations. Of the different types of reporting entities, tumbling participants are most likely to be a ''money services business'' (MSB). The U.S. and Canada have their own criteria for determining if a person/business is an MSB; FinCEN and FINTRAC oversee these determinations.

U.S. FinCEN has issued interpretive guidance on how the U.S. Regulations apply to virtual currencies (the Guidance). The Guidance considers the use of virtual currencies within the framework of the relevant U.S. Regulations' definitions.

According to the Guidance, persons dealing with virtual currencies fall under three categories (the Guidance Categories): ''Users,'' ''Administrators,'' and ''Exchangers,'' which the Guidance defines. The Guidance Categories are not based on the U.S. Regulations' definitions, though they do make reference to them. When determining whether a person is an MSB, the U.S. Regulations' definitions take precedence over the Guidance Categories. Tumbling participants must be mindful of the U.S. Regulations' definitions and their domino effect: a person that accepts and transmits virtual currency is providing ''money transmitting services''; providing ''money transmitting services'' makes that person a money transmitter; and a money transmitter is a type of MSB.

In the U.S, it is legal to participate in cryptocurrency tumbling as a Peer, Customer and Consumer. The main issue is whether a tumbling participant is an MSB. If so, they are a reporting entity and subject to the legal obligations under the U.S. Regulations.

Of the three main types of tumbling participants, Peers (specifically, business-use Peers) will most definitely be deemed money transmitters, MSBs, and therefore reporting entities.

Generally, Customers and Consumers will not be deemed MSBs. However, if they alter their tumbling methods, they risk being deemed MSBs. For example, if a Consumer becomes a Peer with the idea of doubling privacy protections, they could transform from a non-MSB to a money transmitter-MSB.

Canada In Canada, it is legal to participate in cryptocurrency tumbling as a Peer, Customer and Consumer. This is because virtual currencies are currently outside the scope of Canada's AML/CFT regime. However, upcoming amendments to the Canadian Regulations may affect the legality of cryptocurrency tumbling.

Since Canada will likely take cues from the U.S. as they complete their regulations, we can use our analysis of the U.S. Regulations to hypothesize about how the upcoming amendments to the Canadian Regulations will affect tumbling participants. If the Canadian Regulations do follow the U.S. Regulations, then tumbling participants in Canada should be treated similarly: Peers (specifically, business-use Peers) will most definitely be deemed MSBs and therefore reporting entities; and generally, Customers and Consumers will not be deemed MSBs.

Business Impact of Tumbling Blockchain technology does not automatically ensure confidentiality and privacy. This is why tumbling is highly beneficial, if not necessary. Indeed, the business impacts of tumbling are far-reaching. Some entities that would be affected by tumbling are high-net-worth individuals, family offices, venture capital firms, investment funds and banks, as well as consulting and technology companies who ser-

 COPYRIGHT © 2017 BY THE BUREAU OF NATIONAL AFFAIRS, INC., WASHINGTON, D.C. PRA ISSN 0000-0000

vice these entities. In this section we analyze the impact of cryptocurrency tumbling using the Innovation Adoption Lifecycle (IAL) for new technologies as expressed by Rogers' bell curve.

Three main groups of potential users correspond to the different IAL stages. The first are already invested in cryptocurrency and blockchain technology (the Technology) and are willing to embrace privacy-protection tools like tumbling. Moreover, they are on the lookout for such tools because they see them as a necessary part of using the Technology. The second are interested in the Technology and want to learn more about its more practical uses. They want to get a thorough understanding of the Technology and all of its potential pros and cons before adopting it. The third are cautious about the Technology and are not interested in adoption until the Technology is mature and widespread. We can categorize the entities into groups according to the following IAL terminology: early adopters, early majority and late majority. Essentially, early adopters are visionaries who dominate the early market, while the early majority and late majority are mainstream pragmatists.

Tumbling is currently in the early adopter stage of the IAL. Entities that implement tumbling now are early adopters who are building on their established beliefs in the Technology's merits. They are aware that existing tumbling options lack the supplementary features offered by ''whole products'' such as best practices, standards and procedures, staff training and support, installation and debugging, and integration with existing systems. In other words, early adopters believe in the tumbling's potential and accept its current limitations. Entities that choose to wait will act in the early or late majority stages of the IAL. They will wait until virtually all legal uncertainties associated with tumbling are accounted for. For these entities, minimizing the risk to their business and their customers has top priority. They knowingly forfeit the first-mover advantage.

Different tactical approaches will appeal to early adopters, early majority and late majority. We classify the different approaches into ''sword'' (offensive) and ''shield'' (defensive) actions. Sword actions are taken by vigilant entities who proactively seek out new technologies that improve their business and customer service. They will benefit most from the current legal incipience that surrounds tumbling. Conversely, shield actions appeal to the early and late majority because their approach to tumbling is more reactionary than anticipatory: they are watching the market and waiting for tumbling to mature before implementing it. An example of a sword (offensive, anticipatory) action is being the first to market and educate clients on the advantages of privacy protection tools. Early adopters may offer tumbling as a premium add-on service for clients who are heavily invested in protecting their privacy due to the nature of their industry or financial circumstances. An example of a shield (defensive, reactionary) action that early and late majority groups would employ is implementing tumbling to uphold the confidentiality, privacy, and security of customer data. They do so at this later stage because the tumbling ecosystem has matured—implementational risk has been minimized by ''whole products'' with supplementary features (like tested turnkey solutions).

Although technology is ever evolving, the business necessity of concealing operational information (such as revenue and cash flow) from competitors remains constant. Entities are mandated to protect sensitive information from data leaks, which can damage reputation, stock prices, asset valuation, acquisition deals and market confidence. Blockchain analysis can expose sensitive data such as asset types, product pricing, account balances, transaction details, Transactors' identities and smart contract components. Blockchain data exposure, if exploited by competitors or malicious actors, may cause the same damage as a traditional data leak. Shield actions aim to protect entities from blockchain data exposure and damage.

Each IAL group has different options for sword and shield actions. All groups can choose to shield themselves today or in the next IAL stage. However, sword actions are only available at the present stage. Early adopters have the option of using sword actions before anyone else; they can use shield actions as insurance as tumbling technology evolves. The early and late majority can only capitalize on shield actions. There are two parallel applications for shield actions: internal and external. An entity can integrate tumbling into its own internal systems. This implementation is not extended to its customers. An entity can also offer tumbling services externally to the public alongside or instead of its internal use of tumbling.

If you are an entity considering tumbling you should ask yourself two questions. Firstly, which IAL category applies to you? The answer to this depends on the range of stakeholders involved in the decision to engage in tumbling, which can include your clients, partners, and your IT and legal departments. Would your clients understand the value proposition and share your belief in the advantages of being an early adopter of tumbling or are they conservative and expect you to wait? Do you have the internal means to implement or do you need outside consulting and technical support? If you lack the means to implement in-house, then you would need a third-party to educate you on the ecosystem, regulatory issues, and best practices. Your decision-making process should include an evaluation of how comfortable you are with the current maturity level of the tumbling ecosystem, the Technology and the legal landscape. This evaluation will guide you towards the conclusion of whether to engage in tumbling now or wait until the next IAL stage. Secondly, if you choose to proceed, ask yourself whether you will be pursuing an internal or external implementation, or a combination of both.

In conclusion, all entities currently engaged or interested in tumbling should monitor the legal landscape on this topic. As the international discussion grows, regulatory changes are sure to follow. These changes could eliminate the currently available options, that is, they may close the window of opportunity sooner than the IAL suggests. When these changes emerge, you must ensure that you are up-to-date and in compliance.