ComplyFirst

COMPLIANCE BRIEF

Digital Asset

Monero (XMR)

December 7, 2020

EXECUTIVE SUMMARY:

The Monero cryptocurrency offers transactors of its XMR value token anonymity by default through the use of one-time addresses for the receiver and ring signatures for the sender.[1] The use of these one-time addresses prevents any third-party from being able to identify who controls the receiving address. Ring signatures enable verification that someone from a fixed set of individuals created the transaction without identifying the specific sender.[2] Moreover, Monero's use of the cryptographic tool known as *confidential transactions* (perhaps more accurately called "confidential amounts") keeps the amounts transferred visible only to participants in the transaction and those they designate.[3] Essentially, the combination of an XMR transaction's three components (one-time addresses, ring signatures and confidential transactions) enables obfuscation of the parties and amounts involved in a given transaction from public view while still allowing for selective disclosure of certain information. Moreover, unlike interactive mixing services and software, Monero's ring signature creation process is non-interactive. This means that the decoys included are chosen randomly, without the participation of their true owners.

Due to the above-mentioned privacy features, Monero is considered *fungible* or *coin-equal* where there is no significant difference between different coins and their histories. Monero provides protocol-level privacy protections for all transactions, not just a select few.

Monero's two private keys (the *view key* and *spend key*) allow an individual to determine if an output is addressed to them (view key) and enables the individual to send XMR and determine whether it has been spent (spend key).[4] The private view key may be given to others to grant transparency into certain details of particular transactions associated with the address(es). Specific view keys can be shared with any third-party to enable users, financial intermediaries and financial institutions to disclose certain transaction details associated with a given account to a third-party, without publicly disclosing that user's transactional information. Financial intermediaries and institutions can require up-front disclosures as part of their registration process and on an ongoing basis to meet their obligations, though this is advised only in specific, higher-risk cases. When combined with private key images[5], a comprehensive accounting of all inbound and outbound transactions for a given address can be provided.[6]

With a combination of enhanced due diligence, enforcing limitations on types of customers and acceptable jurisdictions, ongoing transaction monitoring, and requesting the disclosure of additional information such as counterparty information and proofs as needed, *financial intermediaries can indeed allow customers to use services related to XMR in compliance with FIN-2019-G001.*[7]

BACKGROUND INFORMATION:

Originally named BitMonero, Monero and XMR came into existence in April 2014.[8] XMR, as a cryptocurrency, can be classified as a payment currency and as a privacy-preserving cryptocurrency (or "privacy coin"). XMR was designed to be used in day-to-day commerce as a means to purchase goods and services in the same way as Bitcoin, Litecoin or even the US Dollar.[9] However, as a privacy-preserving cryptocurrency, XMR is designed to safeguard its users' financial privacy, thus distinguishing it from the

[1] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[2] *See* https://www.getmonero.org/resources/moneropedia/ringCT.html
[3] *See* https://www.getmonero.org/resources/moneropedia/ringsignatures.html
[4] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[5] *See* https://monerodocs.org/cryptography/asymmetric/key-image/
[6] *See* https://monero.stackexchange.com/a/1284
[7] *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), §4.1; *see also id.* at §4.5.3; *see also* 31 C.F.R. §1022.210.
[8] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[9] See https://www.getmonero.org/get-started/what-is-monero/

likes of Bitcoin and Litecoin which permanently store all information relating to any transaction or wallet in a publicly available ledger.[10]

Circulating and Total Supply
As of the date of this brief, there are 17.78MM XMR in public circulation with a value of $2.44B.[11] Unlike Bitcoin, Monero's total supply is not fixed. The coin's primary emission curve issues approximately 18.4 million coins over an eight year timeframe, with an unending "tail emission" of 0.6 XMR per block after that.[12]

Common usage
Like all cryptocurrencies, the value of XMR fluctuates considerably relative to any fiat currencies, and thus there is a large community treating it as a speculative investment in the hope that it will increase in value and can be sold for a profit. As a payment currency, XMR may theoretically be used to purchase any goods and services. However, in practice, there are a limited number of vendors accepting XMR.[13] Monero is mineable using an accessible proof of work algorithm RandomX. Thus, many CPU and GPU hobby miners prefer to mine XMR using common computer hardware over other coins.[14]

PRIVACY MECHANISMS:

Monero includes three core privacy elements: one-time addresses; ring signatures; and confidential transactions. These are enabled for all transactions, not a select few.

One-time addresses, known as stealth addresses, protect the privacy of receivers of XMR. Stealth addresses are randomly generated addresses created for each transaction by the sender on behalf of the recipient so that different payments made to the same payee are unlinkable.[15]

Ring signatures, which protect the privacy of senders of XMR, have two characteristics - a ring of public keys ("ring") and a signature. The ring consists of the corresponding public key for the sender's private key, as well as a set of other, unrelated public keys (called *decoys*).[16] Each signature is generated with a single private key and decoys. When verifying a signature, third-parties cannot determine which public key in the Ring corresponds to the private key that created it.[17] This enables unforgeable, signer-ambiguous transactions that allow for reasonably untraceable XMR transactions.

The confidential transactions feature is a cryptographic tool that allows for verification that no additional XMR has been created or destroyed as part of a given transaction, without revealing the exact transaction amount.[18]

At the network transport level, Monero uses Dandelion++ as an IP address obfuscation technique whereby the originating user delegates another peer (randomly chosen in the network) to widely broadcast the transaction, thereby making it more difficult to track and ascertain the originating user. Dandelion++ is so-called because the transaction broadcast resembles a dandelion. First, nodes narrowly broadcast transactions to only one other node in the "stem" phase. Then, after nodes have relayed the transaction through a sufficiently long "stem," a node is selected as the "fluff" node, whereby this node shares the transaction widely. Dandelion++ assists in dissociating the real IP address from the transaction's origin. Regulated entities usually do not need to concern themself with this privacy feature impairing their

[10] *See* https://getmonero.org/get-started/what-is-monero
[11] *See* https://coinmarketcap.com/currencies/monero/
[12] *See* https://monero.stackexchange.com/questions/4205/what-is-the-total-supply-of-monero-and-when-will-it-be-finished-mining
[13] A useful resource of online retailers and service providers accepting XMR as payment can be found at https://getmonero.org/community/merchants/
[14] *See* https://github.com/tevador/RandomX
[15] *See* https://hackernoon.com/blockchain-privacy-enhancing-technology-series-stealth-address-i-c8a3eb4e4e43
[16] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[17] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[18] *See* https://en.bitcoin.it/wiki/Confidential_transactions

compliance requirements, since they can more easily collect the user's IP address when the user visits the website.

Monero private and public key mechanics

Unlike the Bitcoin protocol, Monero users have two sets of private keys and public keys (four keys total). The pair of public keys make up the wallet address of a Monero user, whereas the two private keys (the view key and spend key) allow an individual to determine if an output is addressed to them (view key) and enables the individual to send XMR and determine whether it has been spent (spend key).[19] To verify transfers of XMR, a third-party observer must know that the XMR is owned by the individual using it. To enable this verification, the individual using the XMR signs the previously received XMR with the one-time address used, thereby proving that individual knows the private keys and therefore rightfully controls the XMR the individual is using. The private view key may be given to others to grant transparency into certain details of all inbound transactions associated with the address.

To allow others to determine which outbound transactions the address made, a list of private key images (one per outbound transaction) must also be provided.[20] With these two elements (private view key and the list of private key images) a comprehensive accounting of all transactions, as well as the addresses' balance, can be determined. Furthermore, omitted key images -- as well as an invalid private view key, for that matter -- can be detected, so a third party can be certain that such information is both authentic and comprehensive when provided.[21]

Without the view key and private key images, a third party cannot access any meaningful transaction data relating to any wallet or transactions. On the public blockchain, one can see that transactions are occurring but is unable to ascertain any input or output amounts nor identify any of the sending or receiving wallets for these arbitrary transactions for which the user is not a counterparty.

Multiple private companies and state agencies have attempted to access information on the Monero blockchain but have largely failed to overcome the cryptographic protections.[22] Monero has undergone many network upgrades that improved its privacy; thus, Monero offers far greater privacy protections today than it did in 2014. Non-RingCT outputs created before 2017 may have significantly weaker ring signature and transaction amount protections, though RingCT outputs since then are not vulnerable.[23] The Breaking Monero series describes some of Monero's past and current limitations.[24]

Monero also contains an optional text field called `tx_extra` that can store arbitrary data in encrypted format. While this can be used for a variety of compliance purposes, this use has not been widely recommended by researchers and developers.[25] Further, there is some community support for the removal of this field, so it should not be relied upon.

ANTI-MONEY LAUNDERING COMPLIANCE:

XMR poses an inherent AML risk in the approximate range of traditional payment types such as cash, card, or paper payment instruments. There is no single method for completely addressing risks, so each entity must evaluate its own risks when supporting XMR. However, through the use of appropriate controls, these risks can be mitigated considerably. These include:

A. Enhanced Due Diligence (EDD)

[19] *See* https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf
[20] *See* https://monero.stackexchange.com/a/1284
[21] *See* https://monero.stackexchange.com/q/281
[22] *See* https://www.reuters.com/article/us-crypto-currencies-altcoins-explainer/explainer-privacy-coin-monero-offers-near-total-anonymity-idUSKCN1SL0F0
[23] *See* https://www.getmonero.org/resources/research-lab/pubs/MRL-0007.pdf
[24] *See* https://www.monerooutreach.org/breaking-monero/
[25] *See* https://getmonero.org/2019/12/05/funds-travel-rule.html

Intermediaries providing services relating to XMR should require customer due diligence at onboarding. To take FinCEN rules as an illustration, this would include requiring collection and verification of a customer's name, date of birth, address, and identification number.[26] FinCEN and other regulatory agencies, following the FATF recommendations, indicate that the use of privacy features (including the use of privacy-preserving cryptocurrencies) could indicate higher risk and could signal a need for institutions to conduct enhanced due diligence. In cases where institutions deem enhanced due diligence is necessary to manage risk, institutions should expect to collect more information about the source of funds to limit the risk of these privacy features shielding illicit activities. They should consider additionally collecting a user's profession and taking steps to further understand the user's source of funds, as well as requiring basic verification details such as a user's ID and residential address at lower transaction limits. Should the intermediary request a reason for the customer's transacting in XMR, this information would not only help the intermediary determine whether that customer is unlikely to use the XMR for undesirable activities, but also to construct a robust and detailed customer profile against which the customer's ongoing activity could be assessed. Of course, the use of XMR should only be one factor in a risk-based approach in determining if EDD is necessary, and other factors may increase or lessen risk. Institutions may determine that their AML controls are already sufficient to reasonably handle the additional risks inherent to XMR, for example if this information is already collected or if reasonable limits are already in place.

B. Limitations on types of customers and geographies

Certain categories of customers (e.g. politically exposed persons) and certain geographies (e.g., jurisdictions on the FATF's "grey list") pose a presumptively higher inherent AML risk. Although it would be a blunter instrument for risk mitigation than per-customer analysis, an intermediary could reasonably and effectively lessen the overall AML risk by categorically prohibiting customers who are in higher risk categories or geographies from accessing and or using XMR-related services.

C. Ongoing transaction monitoring and diligence

The use of traditional methods and tools when tracking customer transactions enables an intermediary to determine a customer's typical activity and allows for identification of atypical activity. In addition, there are a number of private blockchain-specific monitoring tools which may be employed. However, none of these have had much success at monitoring activities in the Monero protocol due to its privacy-centric design.[27] Intermediaries could also require supplemental information from a customer before processing an XMR transaction (e.g., details regarding the purpose of a transaction, the name and address of the recipient, and/or the contact information of the recipient). Collecting this information could help deter illicit activity in the first instance, while also providing verifiable data that could assist the intermediaries' compliance and audit processes. Even if it is impractical to verify all such information before a transaction is executed, implementing risk-based policies and procedures to verify supplemental information from a certain percentage of such transactions (whether before or after execution) could help an intermediary detect and address a sufficient amount of suspicious activity involving XMR. Finally, and arguably as a last resort, an intermediary could limit all incoming and outcoming transactions involving XMR to originating or receiving addresses that the account holder demonstrably controls. This however leads to poor user experience and should generally not be necessary for the vast majority of cases.

[26] 31 CFR § 1022.210(d)(1)(iv).

[27] *See* https://beincrypto.com/chainalysis-adds-dash-monero-still-too-strong/

D. Sanctions screening

Monero addresses and Monero payment IDs can be screened against sanctions lists.[28] Entities should review Monero withdrawal addresses and Monero withdrawal payment IDs to ensure that they are not on the OFAC sanctions list or any other relevant list. This process is similar to screening a withdrawal address with compliance software such as Chainalysis KYT.

E. Requesting additional information for Travel Rule compliance

In the United States, the Funds Travel Rule requires, among other things, the transmitting financial institution or intermediary to include the name of the transmittor and the amount of the order for transmittal orders to another financial institution. In usual circumstances, the sender's intermediary will already know the required information about the sender (i.e. its customer) through its own KYC process, and can require the sender to provide all other required transactional and beneficiary information as a prerequisite to executing the transaction. Notably, the Travel Rule applies only to transactions involving more than one regulated intermediary, so an exchange is not required (for example) to transmit a sender's Travel Rule information to a beneficiary's unhosted XMR wallet. Since the sending and receiving intermediaries are required to conduct KYC on their respective customers prior to providing services, the privacy-preserving nature of XMR therefore does not hinder compliance with the Travel Rule.[29]

F. Reporting suspicious transactions

Entities should report suspicious transactions to relevant regulators should they detect suspicious Monero-related transaction activities. Entities should have monitoring systems in place to identify suspicious activities. Entities should report the information they collected via their due diligence process.

G. XMR-specific controls - disclosure of the view key and private key images

As discussed earlier, users can reveal an XMR transaction's details that are specific to their account via key-based functionality that is built into the Monero protocol. Specific keys can be shared with any third-party to grant insight into the account associated with the keys. This enables entities to disclose certain transaction details associated with a given account to a third-party, without publicly disclosing that user's transaction information. In addition, entities can require up-front disclosures as part of their registration process and on an ongoing basis to meet their obligations. Institutions should bear in mind that while this option is available, disclosure of this information adds friction on both ends, and is most likely not needed except for high-profile investigations, for example at the request of law enforcement or a banking partner.

Through the mechanisms detailed above, financial intermediaries can indeed provide XMR transaction details in compliance with FIN-2019-G001.[30]

ANTI-MONEY LAUNDERING COMPLIANCE EXAMPLES:

Here are some example applications of the above AML compliance suggestions for specific types of cryptocurrency businesses:

A. Cryptocurrency ATM

Cryptocurrency ATM companies may decide to only allow Monero purchases and sales from low-risk geographies. They may determine to collect basic identifying information such as the user ID and residential address of customers with low transaction volumes, such as trades under $3,000. This customer information should be properly screened against sanctions lists and against

[28] *See* https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20200916
[29] *See* https://getmonero.org/2019/12/05/funds-travel-rule.html
[30] *See* FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001), §4.1; *see also id.* at §4.5.3; *see also* 31 C.F.R. §1022.210.

other risk factors. Cryptocurrency ATM companies should place reasonable upper-limit transaction volumes, and they should report all transactions deemed suspicious to the appropriate regulators. Monero addresses to which users request funds be sent should be screened against sanctions lists.

B. Cryptocurrency Exchange

Cryptocurrency exchanges may decide to only allow Monero deposits, withdrawals, and trades from low-risk geographies. They may require users to only deposit or withdraw USD or other fiat currencies to verified bank accounts. Exchanges should collect basic information on users, including their ID and address. Exchanges may require users to pass a higher verification level to trade Monero, or to trade Monero with higher limits. Customers and their requested Monero withdrawal addresses should be screened against sanctions lists. Suspicious trading, deposit, or withdrawal histories should be reported to the appropriate regulators. Exchanges should have a record of expected trading volumes and activities, and they should have monitoring in place to see if users exceed these expected activities.

C. Payment Processor or Money Transmitter

Payment processors may choose to only allow Monero payments from customers in low-risk geographies to entities in low-risk geographies. Payment processors should more closely scrutinize the businesses that receive Monero payments, possibly prohibiting high-risk business types from accepting Monero payments or requiring these businesses to provide more information. Payment processors can lower risk by requiring the recipient business to convert and withdraw funds to a verified bank account or to withdraw cryptocurrencies to a compliant cryptocurrency exchange. Processors and transmitters should screen customers, businesses, and Monero addresses against sanctions lists and report suspicious transactions to appropriate regulators.

ABOUT COMPLYFIRST

This report reflects an independent analysis by ComplyFirst and is intended as a tool to help law enforcement, regulators and industry participants understand and evaluate information that may be relevant to AML compliance. ***The report does not reflect a legal conclusion and is no indication of qualitative value of an asset or suitability for investment or any other purpose and is solely for use by ComplyFirst and not for reliance by any other party.***

ComplyFirst's analytical framework is based on relevant federal law, including FinCEN Guidance issued on May 9, 2019 (FIN-2019-G001). Neither the report nor our framework constitute an exhaustive treatment of the legal and regulatory issues relevant to conducting an analysis of AML compliance and ComplyFirst does not analyze other laws or regulations which may apply. The analysis concerning AML compliance may evolve over time as the nature of digital assets, applicable precedent and FinCEN statements and interpretations change and evolve. ComplyFirst's framework has not been endorsed by FinCEN or any other government authority.

The report is based on a limited review of factual information publicly available or otherwise made available to ComplyFirst. Not all potentially relevant factual information has necessarily been reviewed and no independent investigation or analysis, apart from ComplyFirst's own efforts, has been taken to confirm information on which this analysis is based. We do not assume any responsibility for the completeness of the information upon which our analysis and determination is based. It is possible that if additional facts where known or assumed or understood facts prove to be incorrect, the analysis would be materially different.

DOCUMENT HISTORY

Date	Description
11/20/2020	Initial public release
12/7/2020	Terminology changes