ComplyFirst

COMPLIANCE BRIEF

Digital Asset

Grin (GRIN)

December 7, 2020

EXECUTIVE SUMMARY:

The Grin cryptocurrency is a privacy-preserving cryptocurrency (or "privacy coin") which provides certain anonymity features by default. The core features of Grin privacy are its use of confidential transactions, the Dandelion Relay, and the Cut-through Technique.

The *confidential transactions* feature (perhaps more accurately called "confidential amounts") is the most important privacy mechanism in the design of Grin and shields certain details from the larger public. When creating a Grin transaction, the sending party unlocks the amount to be spent using the original mathematical proof, and the receiving party uses a separate, new proof to create a destination for the received virtual currency. This process adds a layer of protection between the parties so that the transaction is given effect, and to the transaction to obfuscate its details from outside parties. These proofs allow users to shield sensitive information while granting other parties the capability to verify that information while also creating the basis for the Grin network to validate the transaction. These proofs also include provisions for verifying the total supply of Grin.[1]

The *Dandelion Relay* is 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. The term Dandelion Relay is used 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.

The *Cut-through technique* is a process whereby transactions are merged so that the inputs, outputs, and parties are obfuscated, and parts of the data that normally needs to be stored by other blockchains is removed when the data is no longer necessary. This technique makes it difficult to determine which parties send or receive funds.

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 GRIN in compliance with FIN-2019-G001.*[2]

BACKGROUND INFORMATION:

Launched on January 15, 2019, Grin uses the Mimblewimble[3][4] blockchain protocol.[5] The stated objective of Grin is to empower anyone to transact or save modern money without the fear of external control or oppression through the creation of a virtual currency that is private, scalable, and open.[6] As a cryptocurrency, GRIN was designed to be used in day-to-day commerce as a means to

[1] *See* https://github.com/mimblewimble/grin/blob/master/doc/grin4bitcoiners.md#if-transaction-information-gets-removed-can-i-just-cheat-and-create-money

[2] *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.

[3]

[4]

[5] *See* https://www.coindesk.com/information/what-is-grin-cryptocurrency. "Beam" is another example of a native AEC on the Mimblewimble blockchain protocol.

[6] *See* https://grin.mw/

purchase goods and services in the same way as Bitcoin, Litecoin or even the US Dollar.[7] However, Grin is also designed to safeguard the users' financial privacy, thus distinguishing it from the likes of Bitcoin and Litecoin which permanently store all information relating to any transaction or wallet in a publicly available ledger.[8]

Circulating Supply
As of the date of this brief, there are 59.53MM Grin in public circulation with a value of $16.56MM.[9]

Common usage
Like all cryptocurrencies, the value of Grin coins fluctuate 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, Grin coins may theoretically be used to purchase any goods and services. However, in practice, there are a limited number of vendors accepting it as a means of payment. GRIN has a relatively low market-capitalization, and its overall adoption is more limited than Monero, Zcash, and Dash.

PRIVACY MECHANISMS:

Grin's core privacy mechanisms include confidential transactions, the Dandelion Relay, and the Cut-through technique

As stated earlier, the confidential transactions characteristic is the most important privacy mechanism in the design of Grin. Similar to other privacy-preserving cryptocurrenies, the confidential transaction feature for Grin transactions shields certain details from the larger public.[10] This method protects all Grin transactions by shielding the amounts.[11] Grin transactions have three components: inputs (that reference past outputs), outputs (that detail transaction amounts, ownership and proof that the amount is not negative), and a proof that confirms the sum of the inputs corresponds to the sum of the outputs plus a fee (the *Transaction Kernel*).[12]

Grin transactions originate from the sending party who must know two pieces of information: (1) the amount of Grin available for spending, and (2) the private key, known as the *blinding factor*, that the party used when receiving this amount.[13] Blinding factors allow users to shield sensitive information while granting other parties the capability to verify that information. Unlike other privacy-preserving cryptocurrencies that use private keys, proof that an individual owns the blinding factor is not achieved by directly signing the transaction.[14]

When creating a Grin transaction, the sending party unlocks the amount to be spent using the original blinding factor, and the receiving party uses a separate, new blinding factor to create a destination for the received virtual currency. This process adds a layer of protection between the parties so that the transaction is given effect, and to the transaction to obfuscate its details from outside parties.[15]

[7] *See* https://grin.mw/
[8] *See* https://grin.mw/
[9] *See* https://coinmarketcap.com/currencies/grin/
[10] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md
[11] *See* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer
[12] *See* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer
[13] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md
[14] Unlike bitcoin and other cryptocurrencies, addresses are not written to the Mimblewimble blockchain.
[15] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md

The blinding factors used also create the basis for the Grin network to validate the transaction. Additionally, each transaction includes a signature[16] and certain additional data (e.g. mining fees)[17] created from the blinding factors.[18] The network uses the Transaction Kernels to ensure that no new Grin was created or double-spent.[19] Essentially, the Grin network verifies that all inputs minus all outputs (including fees) equals zero.[20]

Grin transactions use a protocol, known as the Dandelion Relay or Dandelion++ protocol, to obfuscate the IP address of the user that sent a given transaction.[21] The Dandelion Relay is a technique whereby the originating user delegates another peer (randomly chosen in the network) to broadcast the transaction,[22] thereby making it more difficult to track and ascertain the originating user.[23]

Another component that increases privacy (and scalability) is the Cut-through technique. The Cut-through technique is a process whereby transactions are merged so that the inputs, outputs, and parties are obfuscated and parts of the data that normally needs to be stored by other blockchains is removed when the data is no longer necessary.[24] This technique enables the block to appear as one large transaction, rather than a combination of smaller transactions, thereby increasing the scalability of the network and the privacy of its users over time.[25] Use of the Cut-through technique makes it difficult to tell which output matched with each input, while maintaining the ability to validate the block,[26] though archival nodes which choose to store full transaction data can counteract the Cut-through technique's effectiveness at preserving privacy.

It should be noted that in late 2019, privacy researcher Ivan Bogatyy observed that it is not difficult to associate transaction inputs and outputs when network usage is low. For his tested time period, he was able to do so for 96% of Grin transactions.[27] While transaction amounts were not discoverable, Bogatyy's work was able to extensively link specific nodes to specific transactions. This highlights Grin's relatively weak transaction graph privacy protections, which opens up many opportunities for regulators and blockchain analytics companies to learn information about many Grin transactions.

ANTI-MONEY LAUNDERING COMPLIANCE:

Grin, like all privacy-preserving cryptocurrencies, poses an inherent AML risk in the approximate range of traditional payment types such as cash, card, or paper payment instruments. However, through the use of appropriate controls, these risks can be mitigated considerably. These include:

A. Enhanced Due Diligence (EDD)

[16] For Grin transactions, the signature uses the kernel excess as the public key.

[17] This additional data comprises part of the Transaction Kernel.

[18] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md

[19] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md

[20] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md

[21] *See* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer

[22] Such action is also known as "fluffing" a transaction.

[23] This delegation may also be aggregated with other transactions that use the same method, further obscuring details. *See* https://github.com/mimblewimble/grin/blob/master/doc/dandelion/dandelion.md; *see also* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer

[24] *See* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer

[25] By automatically removing unnecessary data from the network, over time, historical data will no longer be viewable. This is colloquially referred to as the "right to be forgotten" feature. *See* https://github.com/mimblewimble/docs/wiki/Grin-Privacy-Primer

[26] *See* https://github.com/mimblewimble/grin/blob/master/doc/intro.md

[27] *See* https://medium.com/dragonfly-research/breaking-mimblewimble-privacy-model-84bcd67bfe52

Intermediaries providing services relating to Grin transactions 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.[28] 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 also consider collecting a user's profession and proof of address. Should the intermediary request a reason for the customer's transacting in Grin, this information would not only help the intermediary determine whether that customer is unlikely to use it for money laundering, 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 any privacy-preserving cryptocurrency 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 Grin, 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 privacy-preserving cryptocurrency services.

C. Ongoing transaction monitoring and diligence

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, few of these tools have been used to monitor Grin transactions so their effectiveness remains unclear.[29] Intermediaries could also require supplemental information from a customer before processing a Grin transaction (e.g., details regarding purpose of a transaction, name and address of recipient, and contact information of 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 still help an intermediary detect and address a significantly greater amount of suspicious activity involving privacy-preserving cryptocurrencies. Finally, and arguably as a last resort, an intermediary could limit all incoming and outcoming transactions involving Grin to originating or receiving addresses that the account holder demonstrably controls. This too is a blunt measure that should generally not be necessary for the vast majority of cases.

[28] 31 CFR § 1022.210(d)(1)(iv).

[29] Though certain privacy-preserving cryptocurrencies such as Monero remain secure and untraceable. *See* https://beincrypto.com/chainalysis-adds-dash-monero-still-too-strong/

D. 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 Grin 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 the coin therefore should not hinder compliance with the Travel Rule, just like other anonymity-enhanced currencies[30]

E. Grin-specific controls - disclosure of blinding factors

Like transactions on the Monero network, the Grin network uses privacy features that automatically create opaque transactions that are verifiable, yet publicly hidden. While the Grin network's privacy features obfuscate the identity of the sending party, the intermediaries can still determine the identity and amounts received by their users as they can require specific KYC information during onboarding and as part of each user's continued use of their services.

Moreover, the employment of the Dandelion Relay and Cut-through technique further provides privacy in addition to increasing the efficiency of the Grin network. The use of these two concepts does not negatively affect the intermediary's ability to meet their respective compliance obligations as they merely obfuscate the originating user from the public and remove unnecessary transaction verification data from the network. When the transaction is first effectuated, the sending user's intermediary will be able to determine who sent Grin coins and how much, while the receiving user's intermediary will be able to determine how many Grin coins were received and who received it because in both cases, the intermediaries can require upfront and ongoing disclosure requirements.

Through the mechanisms detailed above, financial intermediaries can indeed allow customers to use services related to GRIN in compliance with FIN-2019-G001.[31]

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 Grin 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 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. Grin addresses to which users request funds be sent should be screened against

[30] *See* for Monero, which also largely applies to Grin https://getmonero.org/2019/12/05/funds-travel-rule.html

[31] *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.

sanctions lists and run through chain analysis software.

B. Cryptocurrency Exchange

Cryptocurrency exchanges may decide to only allow Grin 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 Grin, or to trade Grin with higher limits. Customers and their requested Grin 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. Grin deposits and withdrawals should be screened with chain analysis tools.

C. Payment Processor or Money Transmitter

Payment processors may choose to only allow Grin payments from customers in low-risk geographies to entities in low-risk geographies. Payment processors should more closely scrutinize the businesses that receive Grin payments, possibly prohibiting high-risk business types from accepting Grin 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 Grin addresses against sanctions lists and report suspicious transactions to appropriate regulators. Grin deposits and withdrawals should be screened with chain analysis tools.

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 the 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