CipherBlade

Blockchain Investigation Agency

MEMORANDUM

Shakepay Proof of Reserves and Security Report

Date: August 24, 2020

Contents:

Executive Summary

On July 15th and 16th, 2020, CipherBlade Lead Case Manager, Paul Sibenik (author of this Memorandum), was present at Shakepay's operational address in Montreal, Quebec, Canada. Prior to this visit, Shakepay had provided CipherBlade with extensive pertinent details concerning the setup and storage of their cryptocurrency wallets, along with security measures they had in place in order to streamline the review on these days, both prior to the on-site visit and during the visit itself, so that this review could be conducted over the two day time-span.

This review was conducted to evaluate 'Proof of Reserves'[1], cryptocurrency management, fiat management, cryptocurrency hot and cold storage policies and accessibility, security protocols, and staff risks.

The results of this review are the following:

- All customers funds and all Shakepay funds held by Shakepay, were verified via an online view-only access account with Shakepay's financial institution, who also directly provided CipherBlade with a statement of their account, and were also accurately reflected in Shakepay's back-end systems.

- All fiat Customer Balances[2] were verified via a combination of records found in back-end systems, in conjunction with a historical record of past transactions and past data, and show that as of the date of this report, all Customer Balances as per Shakepay's records match[3] fiat Customer Assets[4] held in segregated bank accounts.

- All customer cryptocurrency held with a cold storage provider was verified via the multi-signature wallet interface that Shakepay utilizes (for their hot wallets), and through account statements (for cold storage wallets held with their cold storage provider, which the cold storage provider directly attested to CipherBlade for) and was

[1] CipherBlade defines 'Proof of Reserves' as verifiably having enough customer cryptocurrency assets to cover cryptocurrency Customer Balances.
[2] CipherBlade defines 'Customer Balances', as the financial obligations from Shakepay to its customers, involving either customers' fiat and/or cryptocurrency assets held in storage and which correspond to customers' account balances.
[3] Very minor differences are observed, which are accounted for by normal day-to-day operations.
[4] CipherBlade defines 'Customer Assets' as customers' fiat and/or cryptocurrency held by Shakepay.

further independently verified through a combination of Satoshi tests[5], a UTXO consolidation[6], and ample transaction data found on the Bitcoin and Ethereum blockchains. This methodology provided a full Proof of Reserves of Shakepay's cryptocurrency Customer Assets.

- All cryptocurrency Customer Balances were verified through back-end systems, in conjunction with historical records of past transactions and past data, and show that as of the date of this report, all cryptocurrency Customer Balances as per Shakepay's records match cryptocurrency Customer Assets[7] held in different wallets from company-owned cryptocurrency.

- There was a 100% match between transaction data found in back-end systems and amounts credited to user accounts accordingly relative to actual transaction amounts observed on the Bitcoin and Ethereum blockchains (for cryptocurrency transactions) and bank account records (for fiat transactions) in all transactions observed.

- Based on the setup procedures and security protocols necessary to access cryptocurrency Customer Assets, cryptocurrency holdings held in hot wallets are unlikely to be compromised, while cryptocurrency holdings held in cold wallets with a cryptocurrency cold storage provider are extremely unlikely to be compromised in any way, while at the same time having adequate redundancy measures in place.

- CipherBlade was provided with criminal background checks of all Shakepay employees, including the founders, and Shakepay claimed past referenced checks had been conducted on all personnel prior. There is no evidence to suggest any employee would elect to compromise Shakepay operations, nonetheless, tiered access measures have been implemented effectively to both prevent or mitigate a breach of Shakepay's systems, customer data, and cryptocurrency Customer Assets.

[5] The spending of a small amount of Bitcoin, in some cases as little as 0.00000001 BTC (1 Satoshi) but more often multiple Satoshi from a given wallet address(es) as a way of proving ownership or control of the wallet address.
[6] Unspent Transaction output. Effectively, a Bitcoin UTXO is any output of a Bitcoin transaction that has not already been spent i.e. that has an (unused) balance.
[7] Very minor differences are observed, which are accounted for by normal day-to-day operations.

The Shakepay Platform

The Shakepay corporate group, operating as 'Shakepay', is composed of Shakepay Inc. and Shake Labs Inc., and is headquartered in Montreal, Canada. Shakepay is a service-based platform that allows Canadians to buy and sell Bitcoin and Ethereum. Shake Labs Inc. was originally registered in 2015, but the Shakepay platform, as it is now known, was launched in early 2018 under Shakepay Inc.

Customers access Shakepay through the Shakepay app available for Android and iPhone which allows users to buy, sell, deposit[8], and withdraw[9] both Bitcoin and Ethereum, and allows users to manage their accounts accordingly. Additionally, customers can perform most actions on the Shakepay website, however, some functionality is strictly done via the Shakepay app.

Shakepay restricts its services strictly to Canadian clientele. Shakepay allows customers to add and withdraw fiat (exclusively Canadian dollars) to/from their account. Shakepay offers customers the ability to add or withdraw CAD via Interac e-Transfer, Electronic Funds Transfer (EFT), or wire transfer. The vast majority of customers elect to fund and withdraw CAD via Interac e-Transfer, as it historically has been an extremely fast, hassle-free, efficient, and free (or almost free) way for Canadians to transfer CAD. Shakepay does not charge users for fiat fundings and withdrawals nor cryptocurrency deposits or withdrawals.

Shakepay's founders are Jean Amiouny (Chief Executive Officer) and Roy Breidi (Chief Technology Officer). Shakepay personnel currently comprises a total of 13 employees and 2 contractors. While Shakepay describes themselves as a remote-friendly company, they do have team members who regularly work out of their Montreal office. Shakepay is operated by Shakepay Inc with a registered address of 410-500 rue Saint-Jacques, Montreal, Quebec H2Y 1S1. Their operational/office address is not publicly disclosed for security reasons, however the author of this report conducted a 2-day on-site visit at their operational address as part of the report.

While customers can utilize Shakepay to buy and sell Bitcoin, Shakepay is not an exchange. That is, they do not facilitate the trading of cryptocurrency between a buyer and a seller. They

[8] The use of cryptocurrency 'deposit' in this report pertains to transferring Bitcoin or Ethereum into a Shakepay account, for which the account is credited accordingly.
[9] The use of cryptocurrency 'withdrawal' in this report pertains to transferring Bitcoin or Ethereum out of a Shakepay account, for which the account is debited accordingly.

don’t have an ‘order book’ (which exchanges have) and thus Shakepay would be better described as a dealer that allows its customers to buy and sell cryptocurrency directly from or to Shakepay, which sources cryptocurrency to fulfill buying and selling demand as needed.

Reasons for this Report

Shakepay commissioned CipherBlade to conduct this Proof of Reserves and Security Report for 2 main reasons:

1. Digital currency businesses deal in coins and tokens that can be publicly verified on blockchains, but their own operations don't have transparency. Shakepay retained CipherBlade to inspect its internal processes and systems and then publish this report so that users can have more insight into the steps the company takes to ensure that it's a trusted supplier of digital currency to Canadians.

2. Shakepay anticipates that technical security will become an increasingly important reason for customers to select a digital currency dealer and this report explains some of the measures the company has voluntarily adopted to help keep customers safe.

About CipherBlade

CipherBlade is a blockchain investigation agency that provides a variety of investigative and consulting services in a wide range of niches, some of which include:

- *Blockchain Investigations and Incident Response* - blockchain forensics and investigative services are at the core of what CipherBlade offers. Most of the incidents that CipherBlade investigates are cybercrime-related and include hacks and thefts (including those involving SIM-Swaps), frauds (such as investment frauds), and scams (including ‘exit scams’ and impersonation scams). CipherBlade has been involved in a considerable number of large-scale investigations and has helped to track down cryptocurrency assets, conduct exchange intercepts, gather evidence and actionable intelligence on persons of interest, and has ultimately worked closely with law

enforcement to assist in prosecution and asset recovery in these cases. A combination of on-chain forensics, off-chain forensics, open-source intelligence (OSINT), and in some cases social engineering are utilized in our investigations, and data is compiled into an actionable report for law enforcement demonstrating what we know, how we know it, and what should be done about it, effectively streamlining the next steps to resolve the situation. CipherBlade's investigative methodology has been developed internally, and multiple law enforcement agencies regularly consult with CipherBlade to improve internal practices.

- *Expert Witness Services* - CipherBlade personnel have served as expert witnesses in numerous high-profile cases involving Bitcoin, cryptocurrency, blockchain forensics, and cybercrime. CipherBlade personnel have also written declarations and have collaborated with a lengthy list of law firms involving civil matters, that have included cases involving ICO mismanagement, embezzlement, OTC disputes, SIM-Swapping, and hidden assets in divorce cases. CipherBlade has provided clear and concise insight involving Bitcoin and cryptocurrency to legal experts who have often had little to no prior technical knowledge about Bitcoin.

- *Security Advisory and Consulting* - CipherBlade provides security advisory and consulting services to various companies with a particularly strong focus on fraud prevention via control measures and staff awareness training. Furthermore, CipherBlade assists businesses and high net worth individuals in the set up and on-going security of their cryptocurrency holdings, including the implementation of inheritance and estate planning services.

Simply put, CipherBlade is in an optimal position to conduct a report of this nature for a couple of main reasons:

1. CipherBlade regularly investigates thefts, exchange hacks, embezzlement (and fake hacks), various types of frauds including 'exit scams', investment fraud, ransomware, and many other types of cybercrime incidents involving cryptocurrency, which enable us to better understand the risks inherent in the setup of any cryptocurrency platform.

2. Given the sheer number of security breaches and avenues through which we've seen users and companies lose their cryptocurrency assets, CipherBlade has an intricate

understanding of the various breach vectors, which for cryptocurrency platforms range considerably and include everything from impersonation scams, to embezzlement to hacking efforts undertaken by nation-state actors. CipherBlade is thus able to help pinpoint such security vulnerabilities and breach vectors, including via 'red teaming'[10] , so that proactive action can be taken to prevent a breach and/or asset loss and make the cryptocurrency platform as unbreakable as possible.

CipherBlade drafted this report without undue influence from Shakepay, and was free to decide the content and substance of this report.

Disclosure: The reviewer is not a professional accountant, and CipherBlade has not performed a professional financial audit or an audit of internal controls and expresses no assurance on the accounting records of Shakepay. This report is for use solely in connection with the objectives specified in the previous section, and should not be used for any other purpose.

Fiat Management

With regards to fiat assets and Customer Balances, the author of this report was provided with online view-only access to Shakepay's bank account with their financial institution, which is in their company name, 'Shakepay Inc'. Their financial institution also directly attested to CipherBlade that the balances held in applicable accounts were accurate. Shakepay has segregated bank accounts with their financial institution for different purposes. One account is specifically to hold CAD belonging to Shakepay customers who hold a CAD balance on their Shakepay account, and holds the entirety of fiat Customer Assets.

Shakepay has a segregated bank account with highly restricted permissions for the sole purpose of receiving wire transfers. Shakepay stated to CipherBlade that this account cannot be debited by themselves or any other party apart from a banking officer at their financial institution. Shakepay's premise for implementing an account specifically for this purpose was

[10] Red teaming involves a third party taking an attacker-like approach and mentality in an effort to discover and exploit security vulnerabilities, often in conjunction with one another, so that an organization can better understand how they would fare against a real-life adversary.

because funds can be withdrawn from almost any Canadian bank account without necessarily having the consent of the account owner via a pre-authorized debit (PAD), once the pertinent account numbers and details are known by the other party. Shakepay would, of course, need to disclose to customers an account number in order to receive wire transfers from clients, thus Shakepay took these precautions accordingly to prevent any risk of an unauthorized withdrawal. As a work-around, in order to prevent a breach of this account via a PAD, Shakepay elected to segregate an account specifically for receiving wire transfers and permissions are set on this account so that it can only be debited by a banking officer at their financial institution, and not via a PAD or even by Shakepay themselves.

Furthermore, Shakepay utilizes additionally segregated bank accounts for the purpose of sending and receiving Interac e-transfers, the primary way they send and receive CAD to customers. As will be discussed in more detail later, Shakepay has more cryptocurrency buying demand than selling demand, thus they receive more CAD from customers than they send to customers. The additional CAD received[11] goes towards purchasing cryptocurrency from the providers they source cryptocurrency from, in order to be able to fulfill the higher cryptocurrency withdrawal demand they have on their platform.

To further verify that these fiat assets held in these bank accounts were accurate, CipherBlade viewed reported amounts in their back-end systems and found that they were consistent with fiat balances reported by their financial institution.

CipherBlade examined data found in Shakepay's back-end systems and verified that the fiat Customer Assets matched the reported Customer Balances, save for some very minor differences that are explained by normal day-to-day operations.

As part of the report, the author of this report performed a fiat cashin and fiat withdrawal to/from a pre-existing Shakepay account of theirs and observed how their back-end systems accounted for the Customer Asset and Customer Balances accordingly and found no inconsistencies. The author of this report also examined a fiat withdrawal they had performed months prior to when Shakepay had engaged CipherBlade and found pertinent records in their back-end systems.

To further verify that reported fiat Customer Balances were not fabricated (i.e. that their actual overall Customer Balances were not higher than what they reported), CipherBlade examined buy and sell volumes and how fiat Customer Assets and reported Customer

[11] Shakepay uses their own funds to purchase cryptocurrency, not customer funds.

Balances had changed between January 2020 and mid-July 2020. This is because Shakepay indicated to CipherBlade that they had seen a significant increase in volume over the past year. Thus, it would be logical to deduce that as assets have increased over time (which was ascertained independently via on-chain data, among other ways mentioned in this report), reported Customer Balances would have increased by similar amounts as well, in addition to the number of cashins, withdrawals, and activity increasing somewhat proportionally. Based on observational data observed, CipherBlade found that generally speaking, volumes increased in the range of 175% (2.75x) between early January 2020 and mid-July 2020. As one example, the number of inbound Interac e-Transfers from customers increased by 180% (2.8x) between early January 2020 and mid-July 2020. The consistencies found in such data further suggest that Customer Balances found in Shakepay's back-end systems are accurate and that they hold enough fiat assets to account for their fiat Customer Balances.

Cryptocurrency Management, Proof of Reserves, and Cold Storage Policies

Shakepay has 4 main internal cryptocurrency wallets[12] per cryptocurrency that they use to store cryptocurrency Customer Assets. CipherBlade has verified that the 2 'hot' wallets (per currency) are multi-signature wallets. One wallet (per currency), the 'receiving wallet' is used for the purpose of initially holding cryptocurrency received from customers (from customer deposits). One wallet (per currency), the 'sending wallet' is used for the purpose of sending cryptocurrency to customers (processing customer withdrawals). The other two wallets (per currency) could both be described as cold storage wallets, one of which has higher restrictions and signature requirements than the other, held with a well-known cryptocurrency cold storage provider, in trust, which is also insured under both the cold storage provider's policy and Shakepay's own policy. This cold storage provider is a trust company registered under the NYDFS[13] and is both SOC 1 Type II and SOC 2 Type II certified.

CipherBlade has reviewed the setup, security protocols, withdrawal processes, restrictions, and accessibility of all 4 wallets per cryptocurrency. There are a variety of security protocols

[12] Bitcoin wallets that are utilized are Hierarchical Deterministic wallets, and involve a collection of addresses per wallet, while Ethereum wallets are 'solo' addresses.
[13] New York Department of Financial Services

implemented to prevent both internal and external breaches or otherwise unauthorized access. This includes address whitelisting, which requires additional permissions to add, modify, or remove. There are a variety of other security features implemented to prevent unauthorized access to their cold storage wallets which CipherBlade has assessed, but which CipherBlade will not disclose for security reasons.

CipherBlade also examined the percentage of cryptocurrency Customer Assets they held in cold storage relative to the amount in both cold and hot storage overall. At the time of the report, approximately 93% of Bitcoin and 91% of Ethereum was held in cold storage wallets. Technically, the percentage of customer cryptocurrency held in cold storage relative to cold and hot storage overall would have been something in excess of these percentages. This is because while all cryptocurrency assets in cold storage can be said to belong to customers, a portion of the cryptocurrency in the hot wallets belong to Shakepay, since Shakepay needs to have cryptocurrency on-hand in those wallets to facilitate customer purchases and to pay miner fees for withdrawals. It was not practical for CipherBlade to independently determine precisely what cryptocurrency in the hot wallets belonged to Shakepay themselves, so CipherBlade did not calculate the exact percentage of cryptocurrency Customer Assets held in cold storage, nonetheless CipherBlade can confidently conclude it was in excess[14] of 93% and 91% respectively at that time. In CipherBlade's opinion the percentage of cryptocurrency Customer Assets held in cold storage is both adequate and reasonable given customer withdrawal demand. While these percentages of course vary periodically to some degree throughout the day based on when wallets are topped up with funds, CipherBlade did not observe any *major* deviations from this ratio.

While some other platforms and exchanges have advertised a 95% cold storage reserve as the optimal percentage that should be strived for, CipherBlade disagrees; we believe a more nuanced view is warranted based upon the nature of the centralized platform that facilitates the buying and selling of cryptocurrency. Namely, Shakepay does not charge customers for cryptocurrency withdrawals as most cryptocurrency platforms and exchanges do. If they did, it would act as a disincentive for customers to withdraw cryptocurrency. We may suppose a larger percentage of customers would keep cryptocurrency on their Shakepay account, and thus Shakepay would likely have a higher percentage of their customers' cryptocurrency in cold storage. The vast majority of Shakepay customers who purchase cryptocurrency on the

[14] A portion of the cryptocurrency in the sending wallet are not 'customer funds'. Rather, Shakepay has advanced a portion of their own funds to this wallet to facilitate upcoming customer withdrawals. Thus we know the cold storage reserve ratio is something in excess of these amounts at that time.

Shakepay platform withdraw it promptly thereafter. Furthermore, given that Shakepay has relatively high cryptocurrency withdrawal demand relative to the amount of cryptocurrency purchased on their platform, Shakepay takes appropriate measures to ensure there are enough funds in their sending wallet to be able to process the high withdrawal demand otherwise, customers would sometimes experience withdrawal delays due to Shakepay not having sufficient cryptocurrency on-hand for withdrawals. Once accounting for the nature of Shakepay's business, it is CipherBlade's assessment that Shakepay maintains a safe and sound cold storage reserve ratio.

In terms of verifying control of the wallets Shakepay claimed to control which Shakepay held customer cryptocurrency in, the way CipherBlade has been able to ascertain control varies depending on the cryptocurrency and the type of wallet in question. For the 2 cold wallets (per currency), as they are controlled by a cold storage provider, neither a digital signature verifying control of those wallets was possible, nor would a Satoshi test be practical[15]. Instead, CipherBlade can confidently conclude that Shakepay controls these cold wallets that they claim for 2 main reasons:

1. Shakepay provided CipherBlade with an account statement of their account with the cold storage provider, which includes applicable wallet addresses and balances held. Furthermore, the cold storage provider directly attested to CipherBlade that these statements were accurate. Data found on the blockchain was also in line with information found on these statements.

2. Data found on the blockchain shows the wallets that these cold storage wallets send and receive BTC and ETH from, which are the providers they source cryptocurrency from and their hot wallets.

Shakepay's sending and receiving wallets, apart from being multi-sig wallets[16], implement a variety of additional features to prevent a breach of these wallets and limit the amount of funds that could theoretically be stolen in the event of a breach. These include a variety of thresholds and limits that each wallet can send over various periods of time. Address whitelisting is also implemented for the receiving wallet, but is not practical to implement for

[15] This is because the cold storage provider ultimately holds the private keys necessary to access these wallets.
[16] Shakepay uses a service to access its sending and receiving multi-signature wallets. The specific service is not mentioned in this report for security reasons, but CipherBlade is aware of the service utilized and can verify it is a well-known service without any known security risks, and redundancy measures are in place as well. Nonetheless, this service does not have control over cryptocurrency in the hot wallets.

the sending wallet, as this wallet needs to be able to send cryptocurrency to thousands of different wallet addresses each day in line with customer withdrawal requests. No single individual has the ability to change, alter, or remove thresholds, limits, or the whitelist for these wallets either. Furthermore, a variety of additional security practices are implemented to prevent these from being changed without genuine permission from applicable parties.

For the Ethereum receiving wallet, ETH is automatically forwarded from customer deposit wallets to a consolidated receiving wallet controlled by Shakepay via a smart contract. This receiving wallet was additionally found in the interface of the multi-signature wallet service they utilize. From the receiving wallet, CipherBlade observes that both in Shakepay's wallet interface, and also on the blockchain, that the vast majority of cryptocurrency, if not being sent to cold storage, is periodically moved to Shakepay's sending wallet once accrued. When an Ethereum withdrawal is requested, ETH is again sent from the sending wallet through a smart contract to applicable user wallets.

The flow of Bitcoin Customer Assets held by Shakepay resembles the flow of Ethereum Customer Assets but there are two main differences. First, there are no smart contracts utilized that automatically forward BTC from a user's deposit address to a consolidated receiving address for Bitcoin, as smart contracts don't exist on the Bitcoin blockchain. Second, there is no single Bitcoin address in Shakepay's receiving wallet address that BTC is consolidated into. Rather, from receiving/deposit wallet addresses, BTC is sent to either cold storage wallets, or more often the sending wallet which then goes towards processing customer BTC withdrawals, which as previously stated, they have more of than customer BTC deposits.

CipherBlade observes that Shakepay had buying demand for both Bitcoin and Ethereum that was multiple times larger than selling demand, and thus had higher withdrawal demand relative to Bitcoin and Ethereum deposits received from customers. Thus, Shakepay would not be able to fulfill customer withdrawal requests solely with the cryptocurrency received from their customer receiving wallet. CipherBlade observes, based on data found in their wallet interface and supported by data found on the blockchain itself, Shakepay received BTC and ETH in its receiving wallets from the entities from which they source cryptocurrency from in order to fulfill customer withdrawals, as Shakepay generally wants to limit how often they access cryptocurrency held in cold storage, which is also more cumbersome to access.

CipherBlade reviewed the two entities Shakepay sources cryptocurrency from as needed, which they often do on a daily basis. Typically, as Shakepay has higher buying (and withdrawal) demand for cryptocurrency than selling demand, Shakepay sends wire transfers to these entities as needed from their Canadian bank account, and receives cryptocurrency in their wallets in return. CipherBlade has verified that both are registered under the Nationwide Multistate Licensing System (NMLS) in the United States. CipherBlade does not assess the involvement of these entities as being a risk factor.

CipherBlade did not observe the generation of the sending and receiving multi-signature hot wallets currently in use, but as part of the report, CipherBlade observed Shakepay generating non-customer wallets that they state they used the exact same setup procedures for when they set up their sending and receiving multi-sig wallets. A single-use laptop was utilized for the setup, which was sourced directly from the Apple Store, which Shakepay also provided CipherBlade the receipt for. Without going into additional specifics of their setup for security reasons, it is CipherBlade's opinion that the procedures and methodologies utilized are both sound and secure.

CipherBlade has verified that Shakepay is in control of the appropriate amount of customer's cryptocurrency that they purport to control at the time of the report, which was also found in their back-end systems. CipherBlade was able to verify the quantity of cryptocurrency assets through multiple methodologies, including by cross-referencing with data found on the blockchain itself. The method through which control of those wallet addresses was ascertained, has already been described for the cold storage wallets.

For the ETH sending and receiving wallets, CipherBlade was able to independently ascertain that Shakepay controls these wallets through the smart contract functionality and transaction history, which is clear given that sending and receiving wallets and solo addresses. CipherBlade was able to independently ascertain control of the BTC sending wallet via a Satoshi test. CipherBlade was able to independently ascertain control of the BTC receiving wallet addresses via a manual UTXO consolidation, which was done in-person, and included input addresses that CipherBlade can independently ascertain they control, and effectively confirms they control the BTC they claimed as part of their BTC receiving wallet.

As part of the report, the author of this report performed BTC and ETH deposits and withdrawals to a pre-existing Shakepay account of theirs and observed the flow of cryptocurrency assets on the blockchain as well as how their back-end systems recorded the

Customer Asset and Customer Balance accordingly and found no inconsistencies. The author of this report also examined a BTC deposit they had performed months prior to when Shakepay had engaged CipherBlade and found pertinent records in their back-end systems.

Reported cryptocurrency Customer Balances found in Shakepay's back-end systems were found at the time to be in line with cryptocurrency Customer Assets, save for minor differences that are accounted for by day-to-day operations. To further verify that reported cryptocurrency Customer Balances were not fabricated (i.e. that their actual overall Customer Balances were not higher than what they reported), CipherBlade examined buying and selling volumes and how cryptocurrency Customer Assets and reported Customer Balances had changed between January 2020 and mid-July 2020, as we had done with fiat Customer Balances, and found that, over time as cryptocurrency assets they held for customers increased, Customer Balances for cryptocurrency did in tandem as well. The consistencies found in such data further suggest that cryptocurrency Customer Balances found in Shakepay's back-end systems are accurate and that they hold enough cryptocurrency assets to account for Customer Balances.

CipherBlade also observes that in the event that the cold storage provider Shakepay utilizes is breached (which in our opinion, is quite unlikely) and that the cold storage provider's insurance does not end up paying out the full balance owed to Shakepay, CipherBlade has verified that as of July 17, 2020, Shakepay had cryptocurrency held in cold storage (with the cold storage provider) additionally insured up to a liability limit that was in excess of the total value of the cryptocurrency held in cold storage. The policy is designed to cover theft primarily from external actors, as well as employees of either company that are not in the position of a director, officer or an individual holding more than 5% of share capital, as well as most conceivable causes of damage or destruction of the physical media on which the keys to access the cryptocurrency are stored.

Security, Systems Access, and Staff Risks

As part of the security report, CipherBlade assessed the risks of an internal breach or theft by Shakepay personnel, including by the founders themselves. CipherBlade was provided with a list of all employees and contracts Shakepay works with and a tiered access list for all

important systems, keys, infrastructure, and credentials personnel have access to. It is CipherBlade's opinion that access to such systems and infrastructure is reasonably segregated, limited, and restricted to personnel who need access to those systems, to minimize possible breach vectors and the damage personnel could do if acting in a malicious manner or if their credentials were breached themselves. CipherBlade also reviewed employee offboarding procedures, as one inherent risk with any business would be a disgruntled ex-employee stealing, leaking customer data, or otherwise attempting to sabotage the business. We found their offboarding procedures to be largely sound, although we did make some recommendations for improvements, which Shakepay promptly made.

CipherBlade was shown criminal background checks Shakepay had performed on all 13 employees (including the founders themselves) earlier in 2020. These background checks all showed no irregularities, matched applicable names Shakepay had provided CipherBlade, and all showed no criminal history for applicable employees. Shakepay also stated that they conducted background and reference checks on all personnel during the hiring process for each employee. While background checks on the 2 contractors had not been performed, CipherBlade observes that these 2 contractors have a low level of tiered access to Shakepay's infrastructure[17] and considerably less than other Shakepay personnel.

The threat of the Shakepay founders absconding with cryptocurrency Customers Assets is also a matter which CipherBlade considered as part of the report. Ultimately, while eliminating the threat of a centralized cryptocurrency platform absconding with Customer Assets can never be guaranteed, there are a number of factors that considerably mitigate the risk of such an event occurring. CipherBlade has determined that neither founder (nor any other Shakepay personnel) have access to the necessary credentials that would allow either of them, if acting alone, to abscond with Customer Assets held in cold storage nor hot storage should either choose to do so due to the security protocols and procedures they have in place. In CipherBlade's opinion, not even the founder of the company should have the ability to control cryptocurrency Customer Assets held in cold storage by themselves. Most Shakepay personnel, including the founders are public-facing. These factors collectively contributorily mitigate the likelihood of internal theft.

CipherBlade has reviewed contingency plans Shakepay has in place in the event that one of the founders, or both of them were to suddenly pass away or were to become incapacitated. In

[17] For example, these 2 contractors are only guest users in the password management application utilized by Shakepay personnel.

the event that one of them were to suddenly pass away, accessing any of Shakepay's cryptocurrency wallets would be a non-issue. If *both* the founders died suddenly, accessing cryptocurrency held in cold storage would still also be a non-issue as these wallets are held and technically controlled by a cold storage provider. With regards to cryptocurrency held in sending and receiving wallets, without going into specifics, CipherBlade is of the opinion that even if *both* founders were to die suddenly, cryptocurrency held in these wallets would still be accessible.

CipherBlade has reviewed how Shakepay personnel store, manage, and secure various credentials, including applicable credential recovery options, which often play a key role in breaches. While we cannot go into specifics about the practices Shakepay employs for security reasons, it is of CipherBlade's opinion that overall, Shakepay employs sound security practices in this regard. Hardware-based U2F[18] authentication or a TOTP[19] application like Google Authenticator is utilized across the company for accessing infrastructure and accounts whenever possible, as opposed to utilizing SMS or no 2FA at all. Shakepay personnel have sound and password generation practices, and manage those passwords appropriately. Recovery options for various accounts and applicable 2FA backups are heavily limited, restricted, and in CipherBlade's opinion, secure, which considerably minimizes the likelihood of a breach via this breach vector.

Concerning physical security and the threat of a physical breach causing loss of cryptocurrency Customer Assets, CipherBlade observes that Shakepay takes a variety of steps to ensure that a physical breach does not occur. The (public) address on rue St-Jacques is merely a mailing address. Shakepay does not disclose its operational or office address from which they work. At Shakepay's operational address, there are no markings on the outside of the building, inside the building, or on a visible internal directory listing Shakepay as being located at this address. There are not even any markings visible outside the door to the suite itself. The fact that their operational address is not disclosed mitigates the risk of an attempted breach. That being said, even if their office was breached, there's no reason to believe it would result in the theft of cryptocurrency Customer Assets. Shakepay does not store critical hardware or devices at this location that would allow one to access cryptocurrency holdings.

As Shakepay is a dealer and platform, and not an exchange, there is no order book. Given the nature of Shakepay's business which can be described as an easy and quick 'on-ramp' and

[18] Universal 2nd Factor
[19] Time-based one-time password algorithm

'off-ramp' for customers looking to buy or sell smaller to medium amounts of Bitcoin and Ethereum, and who typically use Interac e-Transfers in the process, it further naturally suggests most customers do not keep a significant balance on their Shakepay account, at least relative to other cryptocurrency platforms. This is in part because of the inherent transactional limits associated with Interac E-transfers. While each financial institution has some control over applicable e-transfer limits, financial institutions generally impose a limit of roughly $3000 CAD per transaction, and seldom have an allowable limit higher than $5000 CAD per transaction.

This type of business model suggests it is unlikely there are many customer accounts which have large or extremely large balances, relative to other major cryptocurrency platforms and exchanges, particularly in excess of 100k CAD, and thus the size of the 'honeypot' on both a per-customer basis, in addition to cryptocurrency Customer Assets overall, is noticeably lower.

Shakepay has a policy of not charging customers any fees for withdrawing cryptocurrency or fiat currency (or depositing it), even though they incur transaction fees and banking fees for such actions. This type of policy is consistent with their active effort to avoid holding Customer Assets since customers sometimes may neglect to withdraw cryptocurrency Customer Assets due to not wanting to pay the fees associated with such withdrawals. Removing costs for the customer associated with such withdrawals eliminates one of the main excuses customers have for not withdrawing cryptocurrency assets.

Shakepay employs a variety of practices, beyond those which have already been mentioned to prevent a breach of their back-end systems and a breach of confidential client information, which could in turn lead to identity theft, SIM-Swap attacks, etcetera. Shakepay's back-end systems that contain this data are accessible via separate URL's that are not publicly disclosed and which are not indexed by major search engines. Furthermore, these URL's are hosted behind Cloudflare DNS, which requires Shakepay personnel to re-authenticate periodically on a per-device basis prior to accessing the website. These two practices help to mitigate against DDOS attacks on their back-end infrastructure. Finally, Shakepay personnel need to log-in to the back-end each time they need to access back-end systems, which as previously mentioned, use strong and appropriately managed passwords for and require 2FA authentication. Overall, CipherBlade's opinion is that Shakepay has taken appropriate measures to prevent a breach of confidential data by external actors.

Registration, Compliance, Training, and KYC Policies

CipherBlade has independently reviewed Shakepay's registration with FINTRAC as a Money Services Business (MSB) and their registration with Autorité des marchés financiers (AMF) under registration numbers M17065696 and 904007, respectively, and has verified they are actually appropriately registered as they claim[20].

Shakepay personnel receive robust training pertaining to Canadian Anti-money laundering (AML) and terrorist financing regulations and make an active effort to be compliant with applicable Canadian laws and regulations. The training Shakepay personnel receives helps to stop their platform from being utilized to launder money. Shakepay personnel also receive training and are provided strict guidelines concerning security and the storing of credentials to prevent any type of breach. However, CipherBlade identified one major area of training that was lacking for Shakepay personnel; impersonation scams, which have become increasingly prevalent for most businesses. Impersonation scams come in many different forms, and without sufficient training, Shakepay personnel are at increased risk of being deceived in an impersonation scam, which might involve phishing links, email spoofing, or caller ID spoofing of another employee, founder, or business partner. In order to rectify this threat, Shakepay immediately designed and implemented training regarding both preventing and identifying impersonation scams into the training all employees receive, which CipherBlade believes is adequate.

While an in-depth review of Shakepay's compliance policies was not part of the scope of this report, CipherBlade did briefly review compliance policies, their Know Your Customer (KYC) policy, account tiers, and limits. CipherBlade also reviewed factors that raise internal red flags and calls for a review. This includes flags such as banned IPs or banned country IPs, cross-referencing AML lists, duplicate accounts, among a variety of other measures designed to mitigate money laundering via the Shakepay platform.

The Shakepay platform is possible to use to some degree without verifying the customer's identity in accordance with their compliance program. However, CipherBlade observes that accounts are heavily limited regarding functionalities that can be performed, and very low

[20] These registration numbers are also found on their website, https://shakepay.com.

limits apply to cryptocurrency and fiat withdrawals for accounts that haven't completed identity verification. This minimizes the likelihood that Shakepay would be utilized for laundering money. It is more likely for laundering to occur on platforms that don't, or at least those that perform less rigorous checks that can easily be bypassed.

Conclusion

This report was written with the intention to take a proactive approach to assess the appropriateness of Shakepay' security measures and to provide transparency to its customers into its practices. CipherBlade is of the opinion that this is a good way to help customers gain insight into the steps that Shakepay takes to ensure that it's a trusted supplier of digital currency to Canadians.

In CipherBlade's opinion, Shakepay has adequately and transparently demonstrated they have a net cryptocurrency position, having enough cryptocurrency assets to cover cryptocurrency Customer Balances, while also being adequately secure given the current climate. Their use of CipherBlade as an external reviewer that was able to verify much of the data found in this report independently (without relying on Shakepay's records) confirms they have taken proactive steps in this regard.

// ENDS

Paul Sibenik
Lead Case Manager
CipherBlade
paul@cipherblade.com