aml

From: [redacted]@bitprime.co.nz>
Sent: Thursday, 9 December 2021 6:00 pm
To: [redacted] aml
Cc: [redacted] @ BitPrime
Subject: BitPrime AML/CFT Act review submission
Attachments: BitPrime AML Submission FINAL.pdf

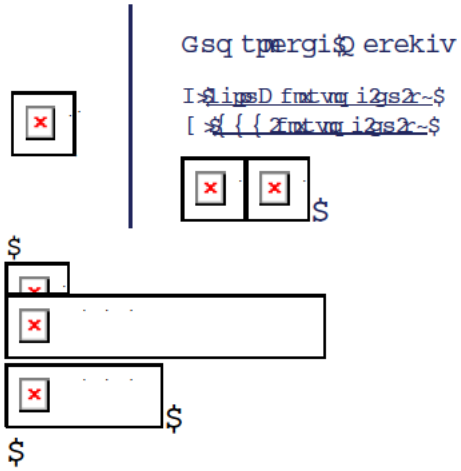
Hi Nick

Thanks for the extension granted, it helped a lot!

Attached is our submission. We tried to touch on many points important to us, but many more need to be discussed.

Looking forward to IAG workshops next year!

Regards,
[redacted]



Review of the AML/CFT Act - December 2021

Submission by BitPrime Ltd.

Compiled by

[redacted] **(Chief Executive Officer)**
[redacted] **(Compliance Officer)**

Any questions, please contact us at admin@bitprime.co.nz or [redacted]@bitprime.co.nz

Table of Contents

Introduction

BitPrime appreciates the opportunity to participate in the AML/CFT Act review. We are grateful to the Ministry of Justice for inviting us to be a part of the Industry Advisory Group.

Overall, our opinion is that the existing AML/CFT legislation is effective. Supervisors are doing a good job educating and guiding reporting entities on this path. It is necessary to recognise that the economic environment is constantly changing and the risk-based nature of the legislation enables us to meet the pace of that challenge. We encourage regulators to continue their good work in that direction.

It is fair to say that there is a lot to comply with under the current AML/CFT Act. The industry has to carefully consider if more requirements need to be added to the Act. It should be balanced against the benefits and be agreed to by the industry players. We believe that there are plenty of existing regulations that we can improve: adding some definitions, clarifying the requirements, and improving current systems. If we unify our resources and work together to build a robust AML infrastructure, a lot can be done using our existing frameworks. It is not always necessary to create something new to improve things; sometimes, it is worth looking back and working on lessons learned during past experiences.

BitPrime has a strong belief that New Zealand can be a difficult place for money laundering to occur. However, it should not become a challenging place to undertake legitimate business. We have to assess the effects of new legislation before introducing it. And, as long as we work as a team, we believe we can reach mutually beneficial decisions. Embracing new technologies and finding unorthodox solutions that suit our national financial agenda should be part of a new AML plan going forward.

1. "Prevention" purpose addition to the Act

Should a purpose of the Act be that it seeks to actively prevent money laundering and terrorism financing, rather than simply deterring or detecting it?

Adding "Prevention" to the Act's purpose might generate unintended consequences. Some criminal activities could be treated as "preventable" (i.e. entities can implement controls to detect and stop their customers' activity *before* starting a business relationship). We could be responsible for preventing our customers from becoming victims of scams, ransomware attacks and fraud. However, these crimes are difficult to prevent, especially when the victim is an accomplice of the perpetrator of the crime. The cost to the business to try to stop these crimes is likely to outweigh possible benefits.

If so, do you have any suggestions how this purpose should be reflected in the Act, including whether there need to be any additional or updated obligations for businesses?

Prevention can only be added if an entity is able to determine it transacts with a known criminal or offender and stop from transacting with them. A defined list of known criminals should be established to avoid ambiguity. In the same way that entities are prohibited from starting business relationships with terrorist entities, they can be prevented from beginning business relationships with known money launderers and other offenders. Businesses can scan official databases to identify those

people. Suppose a customer commits a money laundering offence during their relationship with the entity - That customer could then be added to the list of criminals, and the business can cease trading with the customer.

Only if conditions are well defined can we add "prevention" to the purpose of the Act.

2. Risk-based approach

What is the right balance between prescriptive regulation compared with the risk-based approach? Does the Act currently achieve that balance, or is more (or less) prescription required?

Legislation should allow for assessing and using cryptocurrencies, other virtual assets, and related distributed ledger technologies. As practice shows, risk-based legislation is more future-proof when regulating the latest technologies.

Fast-paced environments, such as the cryptocurrency sector, require an analytical approach to identifying risks and ranking those risks accordingly. No rule-based framework can move at the pace of the industry.

As seen with the AML/CFT Act 2009, a risk-based approach is far more effective than a rules-based approach. This approach is especially true when the sector that the government is trying to regulate is in a state of rapid change, perpetually. If they are locked into prescribed boxes, rules become outdated and ineffective in months, not years.

The European Central Bank advised financial institutions with exposure to crypto assets to put in place appropriate risk-management frameworks. Any introduced legislation must adapt to the technological environment and fast transformation of crypto-assets' risks and activities. A dynamic systems approach has successfully worked for evolving anti-money laundering risks. The same technique should be considered for the financial/market legislation applicable to the virtual assets and blockchain industry.

Brouwer (2019) states that risk-based management is superior to strict rule-based legislation based on the constantly changing digital environment. A risk-based approach to regulation can change the method of legislators and the regulated firms based on the nature of the risk.

In New Zealand, both our AML/CFT and Privacy legislation are deliberately principles-based legislative frameworks. This type of system sets out necessary standards at a high level, making them inherently flexible. Each firm must then consider carefully and adopt an approach of controls that meet the high-level standard proportionately to its risks and type of business. Each firm is then held accountable for its decision-making and the effectiveness of the system it chooses to apply.

In the DIA's AML Guideline for VASPs (referred to above), it explains the principle this way as it applies to AML/CFT Compliance Programme Guidelines:

"…the guidance is generic in nature. It does not provide prescriptive instructions on how businesses can ensure they are compliant with the Act. This is because each business has unique circumstances that determine their exposure to ML/TF risks, which they need to understand and factor into their unique AML/CFT programme. Businesses will need to apply their judgement, and where there are

questions about compliance, they can either ask the Department for general information or seek independent advice."

We would agree with that. Although risk-based legislation involves some uncertainty and discretionary choices, it can react better to changing digital uses/inventions that policymakers may not have foreseen.

Could more be done to ensure that businesses' obligations are in proportion to the risks they are exposed to?

The DIA supervises multiple sectors, and most of them are distinctly different from each other, including their AML/CFT risks exposure. We suggest creating a sector-specific approach which was in part done to the VASP sector when the DIA made the VASP guideline in 2020. As long as the Act states that the business's obligations are proportionate to the risks the business faces, the rest can be done via guidance and Codes of Practice.

3. Licensing/registration

Should there be an AML/CFT-specific registration regime which complies with international requirements? If so, how could it operate, and which agency or agencies would be responsible for its operation?

BitPrime believes that there are positive and negative aspects of introducing the registration/licensing regime for VASPs in New Zealand. On the one hand, it will add credibility to the existing businesses and help to avoid issues when dealing with other financial institutions (e.g. Banks). On the other hand, licensing creates an additional regulatory burden from multiple perspectives – costs, barriers to entering the market, reputational risks if any licensing issues arise, etc. We are convinced that the pros and cons should be carefully weighed and a cost-benefit analysis performed.

VASPs have been captured under the existing AML/CFT legislation for at least three years. Being a legitimate provider in New Zealand, we already comply with all obligations imposed by the Act. A licensing regime legitimises the industry and offers some assurance to Financial Service Providers, making it easier for them to onboard VASPs (i.e. more straightforward to access banking services).

It should be carefully considered what purpose the licensing/registration regime is pursuing and what benefit it adds.

Licensing can be beneficial from a more comprehensive perspective than just the AML/CFT Act – it can involve collaboration between the AML Supervisor, the FIU, FMA and RBNZ, and include monetary/currency oversight and the risky aspects of cryptocurrency businesses.

A licensing system needs to be established to incorporate areas not currently being addressed.

That may include developing frameworks such as an industry code of conduct, custody rules and controls, measures for consumer protection, fair dealing, and disclosure upfront to traders.

BitPrime's proposal for the licensing regime is to give licensing power to the industry-led body composed of crypto/Fintech experts, government members and representatives from other involved sectors, and make it voluntary to start with. It could be a good precursor for the comprehensive

government licensing regime that will address burning issues and give the industry a chance to balance all pros and cons. If the VASPs/high-risk entity licenses are not legislative, then there is much more room for improvement and flexibility to adjust in line with the market.

In the long run, any entity that executes transactions, manages wallets, or collects and maintains KYC data, should be captured by the licensing regime. These entities should include custodial exchanges, OTC desks (like BitPrime), custody providers, and peer-to-peer platforms. Other VASP firms that hold custody of assets or wallets, hosting them in a way similar to banks, are particularly exposed to digital assets/data loss.

The cryptocurrency industry in New Zealand is still tiny compared to the broader financial services industry. Therefore, consideration must be given to the costs of compliance and small firms in meeting the requirements for licensing. The licensing system must be transparent and streamlined with standardized channels of reporting, consistent with our industry's online, FinTech nature, and preferably automated.

It may seem unusual for an industry player to ask for this type of regulation, as it will inevitably cost us in the compliance area. However, BitPrime has a vested interest in keeping any "cowboy" operators out of the market and growing the credibility of our industry. We are already leading the way with many of these best practices. What is desirable is frameworks to ensure a level playing field and consequences for those who do not comply (or are unwilling to invest in it properly). A voluntary licensing regime will address some temporary issues and build the path towards a permanent licensing regime.

With regulatory initiatives in this field only just finding their feet, AML bodies have been leading the way so far. BitPrime supports this; as we want to ensure criminals cannot misuse our services.

The AML community refers to 'VASPs' as an umbrella term for the ecosystem of firms transacting in cryptocurrencies or offering digital services. Two pieces of guidance have been particularly valuable: at the international level, the Financial Action Task Force "Guidance for a Risk-Based Approach" (June 2019); and locally, the DIA's VASP Guideline "Complying with AML/CFT Act 2009" (March 2020).

We attempt to follow and integrate these principles into our business. They include a helpful set of risk factors and 'red flags' around which the industry can organise its compliance.

Currently, VASPs in New Zealand must meet many requirements for initial regulatory oversight. That includes such things as having a compliant AML/CFT risk assessment and programme and compliance officer; being registered on the FSPR; undergoing regular control checks and AML audits; being a member of an approved consumer disputes resolution scheme and being a registered reporting body to pass suspicious matters to the Police FIU.

But no specific licensing system exists, unlike the one that governs deposit-taking finance companies, financial advisors, and derivative trading exchanges. That represents a growing regulatory gap.

All proposed new legislation or regulation must be considered in the context of approaches taken in other jurisdictions. Any licensing regime should require regulators to monitor VASPs both within the regime and overseas entities that are targeting New Zealand users. Enforcement action should be equally applied to both domestic and international operators serving NZ residents.

Only taking Enforcement actions domestically will push New Zealand residents to overseas based VASPs and place users at greater risk due to the subsequent lower operating costs of international operators marketing to and targeting New Zealanders. Failure to apply Enforcement evenly will result in more harm to the New Zealand public with less visibility of transactions for regulators and the associated increase in money laundering.

Some players can relocate or 'shop around' for more accessible forums to base themselves in a global market. That would help avoid the 'waterbed' effect, where one lax operator is pressed down by quality regulation in New Zealand but pops up in another place or under another guise.

If an overly expensive or hard to comply with regime is enacted, it will push cryptocurrency trading to overseas jurisdictions with weaker regulations or a lack of effective enforcement.

Apart from simply sending problem operators elsewhere, it may leave the legitimate New Zealand industry uncompetitive and at a disadvantage.

A vital part of this is having a deep understanding of how cryptocurrencies work from a technical perspective. Some regulatory requirements that might be easy for a bank to comply with would need to be completely re-engineered to work with cryptocurrencies. However, other aspects of cryptocurrencies have some advantages over the banking sector in risk scoring. Advanced blockchain analytics tools allow us to risk-score a wallet or transaction in seconds, tracing them through dozens of previous transactions on the public blockchain or looking forward and seeing where the funds may have gone afterwards. The same exercise in the banking sector would take considerable manual resources, information requests between banks and correspondent banks.

The NZ Law Foundation report "Regulating Cryptocurrencies in New Zealand" (2018) noted back at that stage that there was not yet any standard international treatment of cryptocurrencies. It was of the view that while New Zealand is not alone in using existing laws to stretch over the uncertainty of where cryptocurrencies sit legally, a few other jurisdictions have been proactive and introduced regulations with the intent of fostering the industry.

Since New Zealand has not progressed far since the report was written (apart from in the crucial area of AML/CFT), our country urgently needs to ensure that it is not left behind other countries in weaving regulatory and policy fabrics.

4. Supervisors

Cryptocurrencies and their underlying technology are evolving at a rapid rate. What may have been current even as recently as 2017-18, when BitPrime started, may seem like decades ago in the tech-world now.

Understandably, traditional law-making processes, and conventional approaches by regulators to guidance or rules, cannot keep up. New coins, applications, use cases, and companies join the market all the time from international sources.

An ongoing working group would be highly desirable for the New Zealand government to stay across these changes. It should consist of experts from across the regulatory, monetary policy,

cryptocurrency, and banking sectors. Overseas, similar steering groups or public-private advisory task forces have helped navigate a regulatory path in which none previously existed.

We recommend that an independent working group is created to fill this need for providing 'real-time' information and expert advice to the government. The working group could consist of members appointed from:

AML sector supervisors
- RBNZ
- DIA
- FMA

Law enforcement/Justice/Security
- NZ Police
- DIA
- CERT
- MOJ

Cryptocurrency Industry
Industry experts, including academia
Technical experts
Legal and regulatory bodies – e.g. NZ Law Commission
Banking sector representatives
Treasury

5. New technologies

The best way (perhaps, the only way) for customers and regulators to effectively deal with new technology is to start using it – in safe, experimental methods at first. Only then will its benefits and potential risk areas come more clearly into view. We encourage all agencies to engage directly to experience cryptocurrency and digital assets.

As well as use in commercial applications, law enforcement and cyber-security agencies can find real benefits in the transaction monitoring capability for cryptocurrency transactions. Using technology to track cryptocurrency transactions is much easier than tracing any other financial records. As a secure and reliable ledger, blockchain records the path of cryptocurrency coins from the origination (fiat-crypto exchange, or minting of the crypto coins) up to the extraction from the system (crypto-fiat).

The endpoints of the crypto flow (i.e. when it converts to the mainstream financial system again) are typically regulated by the AML/CFT legislation, where the DIA understands and excels already.

At any step of the path, the enforcement agencies can obtain the CDD/KYC information about the initiator of the transaction or the owner of the wallet address that was provided. Blockchain analytics companies like Chainalysis, MerkleScience, and Coinfirm can track connections between the customer wallet and any risky or suspicious activity (Darknet, scams, ransomware, extortion). These technological solutions provide an excellent opportunity for the enforcement agencies to identify the criminal and receive proof of the wrongdoing that has been documented on the blockchain and can be presented as evidence in court.

There are endless possibilities to improve transaction monitoring for cryptocurrency tracking. One such option is to retain potential bad actors under the umbrella of legitimately operating companies. These crypto businesses can proceed with the standard CDD but enhance the transaction monitoring processes. The users (legitimate or otherwise) will then not move towards unregulated peer-to-peer exchanges and still be captured by the regulated industry players.

Despite (currently) being perceived as a criminal tool, cryptocurrency represents a legitimate investment opportunity for many people. A significant factor behind the illicit use of cryptocurrency is that enforcement agencies sometimes fall behind the technological curve.

Once adequately equipped and trained, enforcement agencies can leverage the inherent transparency of blockchains against the criminal element. The shift towards learning and developing computer science, economic, and forensic knowledge in the enforcement agencies will help facilitate crypto investigations. We would encourage the MOJ to seek the views of experts in the NZ Police FIU as to the technology's potential for good outcomes.

Cyber threats to cryptocurrency are similar to those in other types of remittance. Caution must be exercised equally by the user of traditional payment networks (credit cards & online banking) as with cryptocurrencies. Users must store their credentials (password for bank accounts and private keys for wallets) at a secure and protected location. Cyber threats affect users of all payment networks in similar ways.

We reject the assertion by many in the banking industry that interbank transfers are reversible (compared to cryptocurrency transactions being irreversible). To reverse a domestic bank transfer, the receiver of the funds must first give explicit permission. International money transfers are even harder to recall. By the time a transaction has been identified as fraudulent, it is usually too late to recall the transaction from the beneficiary bank, assuming that they're even co-operative in the first place.

The most significant hacking attacks and thefts the industry has observed have been directed at private key information stored at exchanges. There are no inherent security flaws in cryptocurrency technology itself. Like any other financial infrastructure, the vulnerability lies at the level of the individual user or institution.

The gatekeepers must protect the customers' data and privacy, whether banks or a cryptocurrency exchange. Investors have to make sure they trade and hold their crypto on a platform that offers robust security measures at an individual level. They should consider keeping a significant amount of holdings in their own cold storage and use two-factor authentication. Some exchanges may offer private insurance policies in case of theft or hacking.

BitPrime does not store customers' wallet keys and does not provide direct custodial services, significantly reducing the possibility of hacking or other such cyber attacks.

The 2020 Sentinel Data Book produced by the U.S. Federal Trade Commission indicated that the most significant fraud reports by the payments method recorded in 2020 were attributed to credit and debit cards (91K and 63K reports, respectively). Cryptocurrency-related reports were significantly lower at 11K reports per annum. The total loss for cryptocurrency fraud equalled USD 129 million compared to

the USD 3.3 billion total fraud losses. The most considerable losses came from bank transfers and payments (USD 314 million) and wire transfers (USD 311 million). The share of cryptocurrency in the total fraudulent activity remains small, although frequently overstated by mainstream media.

At BitPrime, we exert great effort in educating the public about the risks of cryptocurrency investments and the impossibility of retrieving funds if sent to bad actors. A considerable portion of vulnerable customers (mostly older people who invest retirement funds), whom we come across often, are aware of the risks and very cautious making decisions about their money. That is an obvious sign of growing investor awareness of the dangers of the industry.

The latest Chainalysis Crypto Crime report (2021) demonstrates a downward trend of the criminal transaction volume from 2.1% in 2019 to 0.34% in 2020 of all cryptocurrency volume. The most significant share of crimes includes scams, ransomware attacks, darknet markets, and stolen funds. Cryptocurrency-related crime remains a small part of the overall cryptocurrency economy. The development of technologies to track down crypto crimes does not go unnoticed by the bad actors. At the same time, the infrastructure surrounding cryptocurrency continues to improve and offer more and more protection. The most prominent players in the industry (e.g. Cardano blockchain) continue to become AML/CFT legislation compliant. This is additional proof that cryptocurrency follows the path of a legally accepted means of trade and is here to stay indefinitely.

As far as possible, other existing regulatory work-streams already underway could be considered and co-opted to assist in these changes.

We note just a few examples here:

- With the Commerce Commission's support, the government is examining potential reforms to the payments industry merchant and interchange fees for card transactions. That work could ideally look broader, to whether future-proofing changes could help ensure that merchants and retailers can accept (if they so choose) cryptocurrencies from their customers, and in turn, use those cryptocurrencies to bring down the costs of transacting through the banking system, and the payment network operators that the banking system owns. This could also reduce de-banking risk to those shops, small businesses, and merchants threatened that they might lose access to their bank accounts if they wish to accept cryptocurrencies from customers.

- Digital identity workstreams, led by the DIA, can and should extend to the benefits and corroboration offered by blockchain and cryptocurrency solutions. Identification of customers, transactions and verification/reconciliation processes are inherent in the design of most blockchain solutions.

- As a result of the FATF Mutual Evaluation Report on New Zealand earlier this year, the industry discusses matters as part of this AML/CFT Act review. A possible issue identified by FATF is the need for more precise licensing roles, including for money remitters and potentially new payments providers and VASPs. Those international hints also reinforce the local industry's desire to have clear licensing frameworks introduced.

6. De-risking

Can the AML/CFT regime do more to mitigate its potential unintended consequences? If so, what could be done?

Unintended consequences of the Act involve risk aversion strategies employed by some financial institutions in their onboarding process. Risk assessment and control matrices that have to be created by any reporting entity to cover the risks are challenging for any business, especially when new technology or legislation comes into practice. Some companies select the path of least resistance, and decline to start business relationships with clients if the risk exceeds their tolerance. Two different risks are stipulated in the risk assessment guidelines – inherent risk (where no controls are implemented) and residual risk (after controls are implemented). Residual risk should be considered when assessing the customer's total risk score, not inherent risk. We think it is essential to recognise these two definitions because it aligns with the spirit of the AML/CFT regime. It is not to avoid or hide the problem but to highlight and manage it. By implementing controls (prevention and detection), reporting entities can safely onboard higher-risk customers and potentially uncover the deeper connections with the criminal structures that may be hidden during the initial interaction. The opportunity to collect important data is missed by blanket de-risking of customers. Let's not forget that there is a human life behind every verification. Syrian or Iranian citizens living in New Zealand sending money to their families should not suffer because of the country's risk assessment. Targeted measures should be put in place to address the risk and conclude on the nature and purpose of the business relationship.

Many VASPs are doing a great job of educating their staff and preventing scams/fraud daily. New technology, such as digital money, would undoubtedly catch the attention of the criminal minds (same as any other developing industry does). It is not the reason to decline a VASP's account at the financial institution, it is the reason to educate and develop the optimal routes for capturing harmful transactions. The best way to adapt to criminal advancement is to get ahead of it. If vulnerable people will still be targeted as scam victims or money mules, better that they talk to adequately trained staff who can identify this, rather than an unregulated peer-to-peer exchange that will process any transaction (regardless of the risk).

We need to reconsider the idea of the "risk" and approach it with courage and readiness to create new innovative measures. New technologies, such as analytics, biometrics, IP address authentication, and open banking, are good steps toward the risk-embracing future. Criminals are moving at a fast pace; they do not have to comply with regulation - we need to become equally flexible and adaptive (or even more so). The better network we create, the better the solutions and information sharing we have to protect our society.

7. Code of Practice

Current NZ VASPs are largely open to a code of practice, and in fact, welcome the idea. We need improved EDD guidance, suspicious transactions guidance, high-risk entities verification and use cases. Codes of practice from the NZ Police would be beneficial for identifying red flags, grounds for suspicion and guidelines on how to deal with the customer while avoiding tipping them off.

8. Types of VASPs

Definitions provided by the FATF in the recent "Updated guidance: A risk-based approach to VASPs" are based on the activity that VASPs conducts. It is a much more useful approach than the one the DIA selected in the VASP Guidance issued in March 2020, where the types of VASPs were listed. The types of VASPs provided did not cover all the relationships between cryptocurrency and fiat currency and what the business operations can capture. For example, cryptocurrency retailing and peer-to-peer transacting were missed.

Types of activities should be clearly defined and captured under the legislation. It will provide more clarity to the reporting VASPs and avoid existing ambiguity. It can be either done by including the definitions in the Act, or issuing a Code of Practice specific for the VASPs.

9. EDD

Enhanced Due Diligence requirements are not precise under the existing legislation in some areas. We list the following as problematic areas of EDD regulations:

- EDD for high-risk customers, especially for customers under suspicion. Customers have broad networks, and if one was asked for a source of wealth and another one wasn't, it would be a clear tip-off for the higher-risk customer.

- Documents certification requirement. It is unclear when to apply it and what value it adds. It is also unclear how to verify an agent that can serve as a customer's agent – are they a registered CA/lawyer? Do they act in the best interests of the AML/CFT Act and/or the customer?

- Types of documents that can serve as proof of wealth documents and the level of their verifiability. Do they have to have a customer's full name/address on it? Do they have to be current? Can we accept screenshots? Some guidance is needed in this respect.

- The balance between the amount of wealth we verify and the transactional limit that customers are given is sometimes hard to figure out. Do we verify SOW (source of wealth) once and permanently leave the higher limit for the customer?

- EDD for an ordinary family trust is excessive. It is becoming a burden for both the compliance department and the customers. We had cases where the customer chose to verify his individual account vs trust account solely because the requirements seemed overwhelming.

- Some support must be provided by the regulators/FIU in extremely complicated cases. We find it *very* hard to conduct EDD for some customers in areas with no guidance from supervisors (e.g cryptocurrency gaming industry, cryptocurrency purchases by the businesses for payments, cryptocurrency loans, etc). We would appreciate practical advice from the regulators, not just a reference from the guidance/the Act.

- EDD verification of customers from high-risk countries should be considered separately as the documents might be unreliable even if they are certified by a foreign JP. There is no standard on how you check/verify an international JP.

10. IVCOP

Do you encounter any challenges with using IVCOP? If so, what are they, and how could they be resolved?

Biometric verification is becoming more common for online-based businesses and those affected by COVID-19. BitPrime believes that the reference or an indication that biometric verification is acceptable at the same level as the face-to-face verification should be made in the Act. A legitimacy status should be added to electronic verification to raise it to the same level as a face-to-face verification.

Standards should be applied to the technology providers that guarantee the quality and the results.

MOJ should consider the problem of electronic verification of international customers where government data sources are not available. Alternative checks should be considered for the purposes of identity verification.

Currently, "Explanatory Note: Electronic Identity Verification Guideline" is vague about the cases where the EIV providers do not verify identity information against an underlying source (such as a government database). It should be clarified what additional data sources (apart from the government) can be used to verify a customer's identity.

Even for NZ or AU based customers, guidance states, "Supervisors expect that the primary electronic source used to verify name and DOB of an individual that is in NZ is either the DIA or NZTA". It is not understood how strong this expectation is and if it is prescribed or just recommended.

It is unclear what the DIA means by "otherwise" in saying that the customer can be linked to their claimed identity biometrically or otherwise. There are additional methods that the DIA suggests, such as verifying the payment via one of the NZ banks, but BitPrime understands that it is not what is meant above.

Immigration NZ data source should be available for providers to connect to, as it is a valuable government source to verify the name and DOB of the NZ visa holders.

11. Tipping-off

Tipping off is a significant concern when the compliance team has a reason to believe it deals with the perpetrator rather than a victim. Every word and step we take should be considered to extract valuable information that the NZ Police can use during the investigation.

More guidance on tipping-off provision is necessary, mainly to understand how far the business should go in getting the information from the suspected fraudster. Exclusions should be included in the guidance where the requirements for EDD or other questions may put a person on guard. It is sometimes a thin line, and to keep the lead open, it can be essential to restrain random questions. BitPrime is of the opinion that the line of communication should be kept open in case the Police want to pursue the questioning. In extremely rare cases, it can be considered the suspicion is evident to any reasonable person.

12. VASPs specific issues

Are there any obligations we need to tailor for virtual asset service providers? Is there any further support that we should provide to assist them with complying with their obligations?

Currently, BitPrime's main issues touch the following areas:

- goAML reporting is not customised to report cryptocurrency transactions. The quality of the reports suffer significantly, and the provided intelligence is not at its best. We understand that this issue does not directly relate to the AML/CFT Act. Still, as the regulators state on more than one occasion, the sole purpose of the regime is to report those suspicious transactions, so we conclude it is directly relevant to this review. The same goes with PTRs and bulk reporting – it is not apparent if we can connect to the goAML portal to send our PTRs as a bulk until it is adjusted to suit VASP's parameters (API connection will require time, and costs are involved).

- VASPs definitions are not clearly defined in the VASP guidance.

- Wired transfers provisions are not defined to suit VASPs businesses. We understand that the current definitions of wired transfers roles classify BitPrime as an "intermediary" exempt from the reporting requirement. Though we report our PTRs, it is unclear if it is our obligation or not. Declaring all virtual asset transfers as cross-border wire transfers requires thorough consideration as the mechanism of complying with the provisions of such a decision is complicated. It is not technically correct to name all crypto transfers "cross-border transfers" as some are clearly domestic (wallet to wallet transfer within one country). Our concern is that by calling all crypto transfers "cross-border," we remove the ability to classify the assets and assign a different level of risk to different types of activities. Domestic risks are clearly different to the risks of transferring funds to a FATF grey country. The argument for classifying them all as "cross-border" transfers is substantial in relation to international compliance.

- New Zealand should analyse the experience of bringing the wire transfer rules into legislation from other jurisdictions and learn all aspects of implementing the "travel rule". It is not obvious if integrating the travel rule into a virtual assets ecosystem brings more benefits or complications.

- Once the travel rule is implemented in many countries, the requirement to call all virtual asset transfers "cross-border" transfers will be mandatory if NZ VASPs continue to operate on the international market. The NZ FIU needs to build capabilities to accept VASP-specific PTRs before introducing a "cross-border" definition.

- Scams are very common amongst cryptocurrency customers. Often victims are not initially cryptocurrency users. They are induced to use crypto as part of the scam due to its immutability. BitPrime (and any other VASP) come across scams/fraud daily, and the rate and sophistication of the crimes are growing and developing. It is vitally essential for the whole AML community to pay attention to these crimes. They are considered unimportant and often go undetected as victims do not report them due to being ashamed and/or genuinely convinced that the scam is in fact entirely legitimate. We encourage MOJ and the NZ Police to consider greater possibilities of uncovering fraud/scam schemes by using new technologies, particularly cryptocurrency.

13. PTRs

PTR requirements are not currently precise for VASPs. When a VASP serves as an intermediary institution between the originator and beneficiary, no obligation to report the transaction exists. In our case, both originator and beneficiary can be a private wallet, and the transfer will not be captured by any other means if we don't report it. BitPrime selects to report it based on the customer's information about the destination of their transfers.

If all crypto transactions are classified as "cross-border" transfers, and the definitions are clarified, all VASPs will have to send reports to the FIU daily. The arrangements to facilitate this information sharing should be made.

As with many other provisions of the Act, the nature of cryptocurrency transactions differs from fiat currency transactions. Recognition of this fact and particular steps must be made to facilitate visual asset transfers and fulfil reporting requirements.

14. SARs

How can we improve the quality of reports received by the FIU and avoid low-quality, defensive reporting?

SARs are a significant part of our compliance work. It is the purpose and the result of the routine work we do to monitor customers' information and behaviour.

It is a time-consuming process to report a quality SAR - a reporting agent has to investigate red flags, communicate to the customer (carefully, to avoid tipping-off!), collect all necessary information, and then decide if there are enough grounds for suspicion to report the case. At BitPrime, it is a rare day when we don't have to report a SAR or investigate ongoing cases. Apart from the difficulties involved in confirming a suspicion, lots of work has to be done to fulfil the data collection requirements for a quality SAR. For an ordinary VASP, it includes information from the data analytics, blockchain, and general KYC information. Sometimes, the investigations take a significant time when we come across a chain of linked customers or transactions. To produce a high-quality SAR complying with all requirements is complicated and time-consuming work.

Factors that make the process extremely difficult for us are summarised below:

- The absence of customised VAs transaction reporting interface in goAML
- Ambiguity in defining suspicion
- Significant delays in communications with the FIU staff
- Lack of typologies for NZ-specific VA red flags
- Inability to share the information with other VASPs
- Lack of visibility of VASP reporting stats in the total reports submitted to the FIU
- Lack of feedback/guidance from the FIU regarding the quality of the SARs/PTRs

- Lack of communication between the FIU and regulators. We often encounter situations where one source sends us to another to clarify our questions.

- Technical capabilities of the goAML portal are deficient: platform loading time delays, loss of data due to platform restarts, unsupported document formats, etc

- Lack of training on how to extract necessary details from the customer and avoid tipping-off

- The unnecessarily complicated existing interface of the reports ("your client", "not your client", multiple transaction types)

- Lack of tech/crypto-related indicators in goAML system (IP address concerns, darknet, suspicious internet activities, etc)

Other

How can we ensure the AML/CFT system is resilient to long- and short-term challenges?

- Leave legislation as risk-based

- Industry led working groups/agencies

- Information sharing between reporting entities

- Technological improvements of the regulators, law enforcement systems

- Education of general public of the purpose and the requirements of the AML regime

- Embracing new technologies instead of avoiding them