BitMEX

Travel Rule
Data Storage Principles

Intro 1

1. Overview 2

2. The Data Storage Principles 4

2.1 Access Management 4

2.2 Travel Rule Data Security 4

2.3 Information Protection 5

2.4 Logging & Monitoring 6

2.5 Incident Management 6

2.6 Privacy 6

2.7 Additional Principles 7

Intro

"We are proud to provide this as an open-source, non-copyrighted resource for Virtual Asset Services Providers, compliance and security professionals, policymakers, and the rapidly growing community of those who are using virtual assets. We invite you to build upon this work. We hope it sparks discussion between regulators, industry, and users. As we iterate on these principles, we hope the final product will help to safeguard the privacy of the billions of people the Travel Rule will ultimately affect. "

Malcolm Wright

Chief Compliance Officer at 100x Group

1. Overview

In June 2019, the Financial Action Task Force (FATF) updated its Recommendations[1] to include activities provided by Virtual Asset Service Providers, or VASPs[2]. The Interpretive Note to Recommendation 15 required that:

"...originating VASPs obtain and hold required and accurate originator information and required beneficiary information on virtual asset transfers, submit this information to beneficiary VASP or financial institution (if any) immediately and securely

...beneficiary VASPs obtain and hold required originator information and required and accurate beneficiary information..."

This requirement has colloquially become known as the **'Travel Rule'**.

Jurisdictions around the globe are now implementing this requirement into local legislation that will require VASPs to comply. Further, even where a VASP may not yet have governing legislation in the jurisdiction from which it operates, the impact of the FATF Recommendations may still be felt where a VASP interacts with counterparty VASPs in other jurisdictions where they are required to comply.

Since June 2019, several Technology Service Providers, or TSPs, have been working hard to build out solutions that provide for the immediate and secure transmission of originator and beneficiary information. However, little focus has been given to the data once it is stored. This data is highly sensitive; VASPs will be transmitting their customer information to third party VASPs with little understanding of how that data will be stored upon receipt.

[1] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

[2] https://www.fatf-gafi.org/glossary/u-z/

Therefore, the purpose of this document is to suggest some guiding principles for VASPs on good data storage practices that will aid in building confidence amongst VASPs when Travel Rule data is sent. VASPs may use these principles in building their own Travel Rule data storage solutions as well as assessing counterparty VASP storage arrangements prior to the exchange of data.

To aid with understanding these principles it is helpful to understand the purpose for the collection and retention of this data which is to:

- Enable law enforcement to make a request to a VASP for counterparty details on both sides of a transaction
- Enable a VASP to screen originator and beneficiary names against relevant sanctions lists
- Enable a VASP to utilise the data in transaction monitoring in order to detect suspicious activity

2. The Travel Rule Data Storage Principles

2.1 Access Management

- **Deny All by Default** - The VASP should deny all access to the travel rule data store by default.
- **Principle of Least Privilege and Need to Know** - Access to travel rule data at the VASP should be granted based on the principle of least privilege and on a need to know basis. Just in Time (JIT) access tokens can be utilised for granting short term access for special purposes or in case of an emergency.
- **Multi Factor Authentication (MFA)** - The VASP should use MFA to grant access to the travel rule data store.
- **User Access Management** - User access to the travel rule data store should be managed by having well defined processes of user provisioning, user deprovisioning and user attestation.
- **Personal Device Usage** - Usage of personal devices to access the travel rule data store at the VASP should be prohibited.
- **Physical Access** - Physical access to travel rule data storage infrastructure should be managed and protected.
- **Admin** - Admin access should be restricted.

2.2 Travel Rule Data Security

- **Encryption at Rest** - The VASP should use AES 256 or higher for encrypting travel rule data at rest.
- **Encryption Key Management -** Encryption keys should be stored in an appropriate location, such as a FIPS certified HSM, Hashicorp Vault, or similar solution.
- **Data Storage** - Travel rule Data should be stored securely according to state of the art principles, using certified or approved storage environments. The VASP should prohibit the usage of removable media or storage.
- **Data Separation** - Travel rule data at the VASP should be logically separated from other organisational customer data.

- **Prevent Data Leakage** - Measures like Data Leak Prevention (DLP) tools should be utilised, in line with applicable laws, to prevent accidental and malicious data leakage of the travel rule data.
- **Data Integrity** - The integrity of travel rule data should be maintained by the VASP.
- **Data Backup** - Backup copies of travel rule data should be collected at frequent, planned intervals, stored in a secure location and tested periodically to verify the backup process is operating correctly.
- **Data Reproduction** - The VASP should not reproduce travel rule data for any use other than for law enforcement, screening, and transaction monitoring purposes as discussed above.
- **Data Sharing** - The VASP should not share any travel rule data with third parties other than when required to do so by law. As such, third party access to the travel rule data store should be prohibited.
- **Data Retention** - The VASP should retain travel rule data only for so long as legally required or as required to effectively carry out the VASP's AML compliance program.
- **Data Disposal** - Travel rule data should be securely disposed by the VASP when the applicable retention period has expired.

2.3 Information Protection

- **Secure Baseline -** A secure baseline configuration (golden image or similar standardised configuration) should be designed and maintained for travel rule data storage infrastructure.
- **Secure System Development Lifecycle -** The VASP should implement secure design and testing controls throughout the system development lifecycle and require the use of secure coding practices.
- **Change Control -** Changes to travel rule data storage at the VASP should be reviewed and approved according to the authorised change control processes.
- **Vulnerability Management -** Procedures to manage vulnerabilities (e.g., scanning, patching, remediating and deploying compensating safeguards) should be documented and followed.

2.4 Logging & Monitoring

- **Security Event Logging -** Important events (e.g. data access, configuration changes, failures or privileged activity) with potential security implications should be defined and recorded in logs.
- **Alerting -** Detected security events should be promptly escalated and responded to in accordance with a defined incident management process.
- **Event Detection Communication -** The beneficiary VASP should, as applicable, provide an event notification to the originating VASP as per an SLA upon detection of a security event.

2.5 Incident Management

- **Incident Response Plan -** An incident response plan that outlines formal reporting, that may include reporting to law enforcement, data privacy regulators, and / or financial regulatory authorities. Response procedures should be established, documented and followed when responding to security incidents.
- **Recovery Plan -** The VASP should pre-establish a recovery plan to restore the travel rule data store by rebuilding systems, restoring data backups, closing of the information security incident, and restoring security controls (i.e. firewall rules, removing emergency user accounts) after an incident has taken place.

2.6 Privacy

- **Data Use** - The VASP should use the travel rule data only for the purposes of fulfilling legislative requirements based upon the FATF Recommendations and the collection, processing, and sharing of such data, as applicable, should be done in full compliance with applicable laws.
- **Data Use Restrictions** - The VASP should not target users from the received travel rule data to provide additional services or to enhance their products. Re-use of travel rule data should be limited.
- **Data Commingling** - Where possible, the VASP should prevent commingling of travel rule data received from different counterparty VASPs.

2.7 Additional Principles

- **Accountability** - The VASP should have in place internal mechanisms and control systems that ensure compliance and provide evidence – such as audit reports – to demonstrate compliance to external stakeholders, including supervisory authorities.
- **Local Laws** - The VASP should give due consideration to the cybersecurity, data compliance and privacy laws to which it is subject.
- **Security Awareness Training** - All authorised users of the travel rule data store should be trained for security awareness on an annual basis at least.