Wizz Networks, LLC

Anti-Money Laundering Policy
Compliance Program

Last Updated – July 7, 2019

BSA Compliance Officer: Jessica Murphy
Phone : 407-883-1674
E-mail: jessica@genesiscompliance.com

Table of Contents:

WIZZ NETWORKS COMPLIANCE POLICY:

This document is the Wizz Networks, LLC's ("Wizz Networks") Anti-Money Laundering Policy (the "Policy").

Wizz Networks is a blockchain dapp with many services including a decentralized exchange. Wizz Networks was founded with the mission of reaching a global crypto economy and social network.

Because Wizz Networks is in the business of exchanging various cryptocurrencies, it is required to register as a Money Service Business ("MSB") with the Financial Crimes Enforcement Network ("FinCEN"). Wizz Networks is registered under the MSB Category of Money Transmitter, its registration number is 27118533. As an MSB, Wizz Networks must adhere to a strict culture of compliance in order to assist the government in its battle against money laundering and terrorist financing. The penalties for non-compliance can be severe, and Wizz Networks has taken great care to meet all of its obligations on this front. One of the main requirements is the preparation of an effective anti-money laundering ("AML") compliance program. The program must describe how the Company will monitor transactions, report suspicious activity, provide employees with appropriate training and conduct annual independent audits of its compliance program.

Wizz Networks has selected **Jessica Murphy** as its Bank Secrecy Act Compliance Officer (the "BSA Compliance Officer") who will, along with other Senior Management of Wizz Networks, ensure this Compliance Program is enforced across the Company. If any personnel and business partners are found to have intentionally violated this Compliance Program, they are subject to immediate termination. This Policy will be reviewed and audited annually, and any deficiencies found in the Compliance Program will be addressed and implemented immediately. The BSA Compliance Officer keeps a copy of the Bank Secrecy Act Quick Reference Guide for Money Services Businesses printed and easily accessible by his desk.[i]

I. LAWS AND REGULATIONS APPLICABLE TO MONEY TRANSMITTERS

A. Anti-Money Laundering and Anti-Terrorist Financing

Money Laundering is the process of concealing the source of illegal proceeds so that the money can be used without detection of its criminal source. The United States has passed many laws to combat money laundering and terrorist financing. The Bank Secrecy Act ("BSA") was established in 1970 and implemented regulations that require financial institutions ("FIs") to assist the government by creating a paper trail for currency transactions over $10,000. Additionally, this Act introduced the requirement for FI's to verify the identity of customers and keep certain records of customer transactions. Noncompliance with these requirements carry both civil and criminal penalties.

As a FinCEN Registered MSB, Wizz Networks must adhere to the following BSA requirements (More details are included in later parts of this Policy):

1. *Registration.* As part of the registration rule, each business that meets the definition of an MSB must register with the Financial Crimes Enforcement Network ("FinCEN"). Wizz Networks is an MSB because it is engaged in the business of transferring cryptocurrency as a Money Transmitter.[ii]

2. *Agent List.* Each registered MSB must prepare and maintain a list of its agents including the agent's name, address, phone number, the type of service the agent provides, the gross transaction amount the agent processed in the preceding 12 months (this must be current within the past 45 days), the year the individual became an Agent of the MSB, and any branches or subagents. If requested, the MSB must make its list of agents available to FinCEN or the Internal Revenue Service ("IRS").[iii]

3. *Suspicious Activity Report ("SAR").* An MSB is required to file SAR when any type of suspicious transaction has occurred for an amount greater than $2,000. In order to be considered suspicious, the transaction must cause the MSB to know or reasonably suspect that the transaction (or a pattern of transactions of which the transaction is a part):

    a. **Involves funds derived from illegal activity** or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or is

    b. **Designed to evade the requirements of the Bank Secrecy Act**, whether through structuring or other means, or

    c. **Serves no business or apparent lawful purpose**, and the reporting business knows of no reasonable explanation for the transaction after examining all available facts.

The SAR must be filed using a SAR MSB form, and must be filed within 30 days of the MSB becoming aware of the suspicious transaction. The MSB must retain a copy of the filed form and supporting documentation for a period of five years from the date of filing. The MSB must ensure the SAR is not disclosed to anyone involved in the transaction. Civil and criminal penalties may be imposed for willful violation of the SAR requirement.[iv]

4. *Anti-Money Laundering ("AML") Compliance Program.* All MSBs are required to develop and implement an AML compliance program as required by section 352 of the USA PATRIOT Act and implemented by regulation at 31 CFR 1022.210.

5. *Currency Transaction Report ("CTR"*). MSBs must file CTRs on transactions involving more than $10,000, in either cash-in or cash-out, conducted by, though, or to the MSB on any one day by or on behalf of the same person. MSBs must also be aware of "Aggregation" where multiple transactions conducted by or on behalf of the same person on the same day must be treated as a single transaction for CTR purposes. The CTR must be filed within 15 days and copies must be retained for five years.[v]

6. *Funds Transfer Rule*. Any time a $3,000 transfer of funds occurs, the MSBs must maintain certain information:

    a. The name of the transmitter (the transmitter is the person wanting to do the transaction);

    b. The account number of the transmitter;

    c. The address of the transmitter;

    d. The identity of the transmitter's financial institution;

    e. The amount of the transmittal order;

    f. The execution date of the transmittal order; and

    g. The identity of the recipient's financial institution.

7. *Record Retention.* All of these records must be retained for five years and must be accessible within a reasonable period of time.

Bitcoin & the BSA:

On May 9, 2019, FinCEN addressed the status of digital currencies under the Bank Secrecy Act. For further details, *see* Application of FINCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, FIN-2019-G001 (the "Guidance").[vi]

The Guidance described how FinCEN regulations relating to money services businesses apply to business models involving transmission denominated in value that substitutes for currency, specifically, convertible virtual currencies. The Guidance stated that FinCEN does not distinguish between government backed currencies or virtual currencies, the same rules apply to both. Whether a person is a money transmitter depends on the facts and circumstances of a given case.

B. Office of Foreign Assets Control

The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.

OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. OFAC sanctions can either be comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. Prohibited transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. Because each program is based on different foreign policy and national security goals, prohibitions may vary between programs.

There is no single compliance program suitable for every financial institution. OFAC is not itself a bank regulator; its basic requirement is that financial institutions not violate the laws that it administers.[vii]

C. Privacy

The Gramm-Leach-Bliley Act (the "GLBA") is also known as the Financial Modernization Act of 1999. It is a United States federal law, enforced by the Federal Trade Commission ("FTC") that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

D. State Licensing

To operate legally, money transmitters may be required to obtain a license from certain states where they will service or solicit customers. At this time, there is no uniformity with respect to virtual currencies and state regulations. Each state has different rules, and it is a perplexing task to interpret how each of the 50 United States views the transmission of virtual currency. While some states have issued guidance, opinion letters, or other information defining their definition of money, many have yet to take action. As of the time of this writing, the following require licenses for the type of business of which Wizz Networks is operating Alabama, Hawaii, New Mexico, New York, Vermont, Virginia, and Washington. There are also states with laws that could be interpreted to require a license, it is best to send them a No Action Letter. At the time of this writing, since the No Action requests have not yet been made, Wizz Networks should wait to conduct business in: Alaska, Connecticut, and North Carolina.

E. BSA Penalties

Violations of the BSA carry criminal and civil penalties may result in criminal and civil penalties. Under the civil penalties, there is a difference between negligent and willful misconduct.

- Negligent misconduct can result in up to $500 fine, or, if there is a pattern of negligent violations, a fine of $50,000. *See* 31 USC 5321(a)(6)(A); 31 CFR 1010.820(h)

- Any person willfully violating, or willfully causing any violation of 31 USC 5314 can result in a fine for the greater of: (a) the amount (no to exceed $100,000) equal to the balance in the account at the time of the violation, or $25,000. *See* 31 CFR 1010.82(g)(2).

A separate violation is can be counted for each day the violation continues and at each location where the violation takes place. Failing to file reports or making material misstatements or omissions in the reports can result in additional penalties.

Criminal penalties can be assessed for willful BSA regulation violations. Any individual, including a credit union employee, found guilty of this is subject to criminal fines of up to $250,000 or five years in prison, or both. If the individual commits a willful BSA violation while breaking another law or committing other criminal activity, he or she is subject to a fine of up to $500,000 or ten years in prison, or both. Violations of certain BSA provisions or special measures can make an institution subject to a criminal money penalty up to the greater of $1million or twice the value of the transaction.[viii]

The most recent fines assessed against MSBs were:

- April 19, 2019*: In the Matter of Eric Powers* – charged with willfully violating the BSA's registration requirements and reporting program. Powers acted as a virtual currency exchanger without registering as an MSB, creating a written compliance policy, maintaining records, or filing SARs. Powers was assessed a $35,000 fine and agreed to an industry bar that would prohibit him from providing money transmission services or engaging in any other activity that would make him a "money services business" for purposes of FinCEN regulations.[ix]

- July 27, 2018: In the Matter of BTC-E a/k/a Canton Business Corporation) and Alexander Vinnik – charged with money laundering, conspiracy to commit money laundering, engaging in unlawful monetary transactions, and the operation of an unlicensed money transmitting business. The Company was an exchanger of convertible virtual currency and attempted to conceal the fact that it serviced U.S. based customers. It was determined that the Company and its Compliance Officer willfully violated MSB registration requirements, failed to implement an AML policy, failed to detect or report suspicious activity, and failed to keep adequate records. FinCEN assessed a fine of $110 Million on the Company and 12 Million on Alexander Vinnik.

<u>The fines for OFAC violations</u>:

Criminal and civil penalties exist and can be levied against the institution as well as the

individuals involved. Criminal penalties include a fine of up to $1 million and/or up to 20 years in prison for each violation. Civil penalties include a fine of up to $55,000 for each violation. Other penalties for violations of OFAC regulations include seizure/forfeiture of the goods involved.[x]

II. MONEY LAUNDERING AND TERRORIST FINANCING

A. Money Laundering

The conversion or transfer of property, the concealment or disguising of the nature of the proceeds, the acquisition, possession or use of property, knowing that these are derived from criminal activity and participate or assist the movement of funds to make the proceeds appear legitimate, is money laundering.

Money obtained from certain crimes, such as extortion, insider trading, drug trafficking, and illegal gambling is "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods which vary in complexity and sophistication.

Money laundering involves three steps:

1. **Placement** involves introducing cash into the financial system by some means;
2. **Layering** involves carrying out complex financial transactions to camouflage the illegal source of the cash; and
3. **Integration** is acquiring wealth generated from the transactions of the illicit funds ("integration").[xi]

In the United States, money laundering can also take place when funds are transferred with the intent to promote or engage in an unlawful activity such as financing terrorist activity.

Handling money knowing that the funds came from an illegal source is a serious crime. "Knowing" also includes ignoring signs that a reasonable person would pick up on that point to the fact the funds could be derived from illegal activities, also known as "willful blindness."

B. Structuring

Structuring is the breaking up of transactions for the purpose of evading the Bank Secrecy Act reporting and recordkeeping requirements, and if it is appropriate, should be reported with a SAR. Structuring can take two basic forms. First, a customer might deposit currency on multiple days in amounts under $10,000 (e.g., $9,900.00) for the intended purpose of circumventing a financial institution's obligation to report any cash deposit over $10,000 on a CTR.

Customers may also engage in multiple transactions for one day or over a period of several days or more in a manner intended to circumvent either the currency transaction reporting requirement, or some other Bank Secrecy Act requirement, such as the recordkeeping requirements for funds transfers of $3,000.

Structuring may be indicative of underlying illegal activity; further, structuring itself is unlawful under the Bank Secrecy Act. An effective anti-money laundering program should be designed to

detect and report both categories of structuring to guard against use of the institution for money laundering and ensure the institution is compliant with the suspicious activity reporting requirements of the Bank Secrecy Act.[xii]

Wizz Networks staff that directly interact with customers have an amplified responsibility to ensuring they do not willingly or unknowingly assist in structuring a transaction. Primarily, staff must not advise customers to reduce the amount they send in order to avoid reporting requirements.

C. Terrorist Financing

Terrorist financing provides funds for terrorist activity. Terrorists must develop sources of funding and a way to obfuscate any link between their source of funds and their terrorist activity. An MSB needs to screen its customers through official lists of known terrorist individuals and organizations.

D. HIFCA: High Intensity Financial Crime Area

High Intensity Financial Crime Areas ("HIFCA") were introduced in 1999 as a means of focusing law enforcement efforts in certain geographic zones. Wizz Networks has the potential to service users that may be located in HIFCA zone. Below is the HIFCA jurisdictional map as identified by FINCEN:

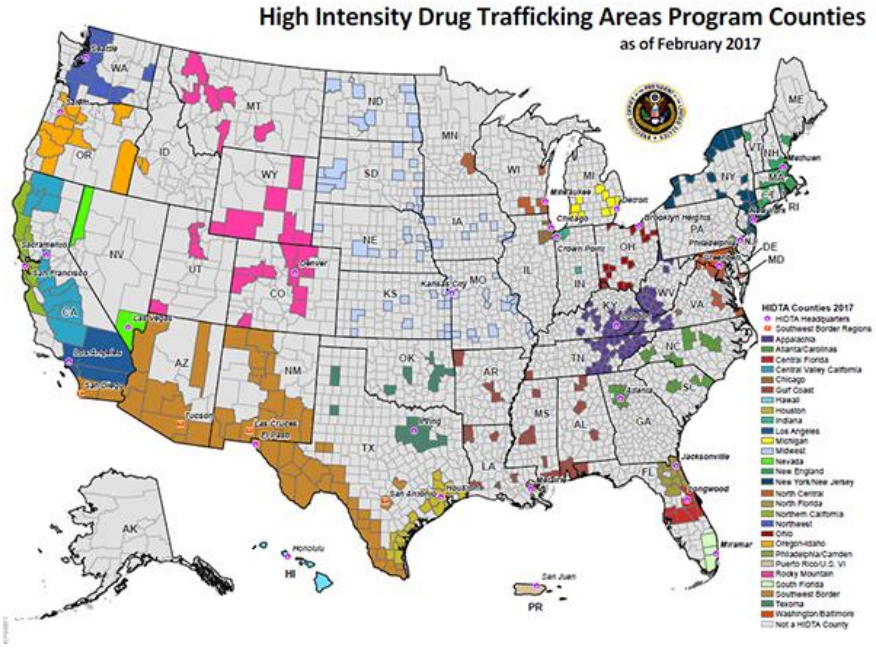
HIFCA Regional Map

California Northern District	Monterey, Humboldt, Mendocino, Lake, Sonoma, Napa, Marin, Contra Costa, San Francisco, San Mateo, Alameda, Santa Cruz, San Benito, Monterey, Del Norte
California Southern District	Los Angeles, Orange, Riverside, San Bernardino, San Luis Obispo, Santa Barbara, Ventura
Southwest Border	Arizona - All Counties Texas - Counties Bordering, and adjacent to those bordering, the US and Mexico Boundary
Chicago	Cook, McHenry, Dupage, Lake, Will, Kane
New York	New York - All Counties New Jersey - All Counties
Puerto Rico	Puerto Rico - All Areas U.S. Virgin Isles - All Areas

South Florida	Broward, Miami-Dade, Indian River, Martin, Monroe, Okeechobee, Palm Beach and St Lucie

E. High Intensity Drug Trafficking Areas (HIDTA)

The High Intensity Drug Trafficking Areas ("HIDTA") program has determined 28 critical drug-trafficking regions, located in 46 states, as well as Puerto Rico, the U.S. Virgin Islands and the District of Columbia. Wizz Networks may have customers located in HIDTA's, and needs to be vigilant about its culture of compliance. Below is the HIDTA map of the United States:



Wizz Networks performs Enhanced Due Diligence ("EDD") for high risk customers in these geographic locations. This due diligence process includes an analysis of the customer's source of funds, and screening of any listed beneficiaries of the IRA account.

WIZZ NETWORKS 'S COMPLIANCE PROGRAM

The elements of Wizz Networks 's Compliance Program are:

- A BSA Compliance Officer
- A Written Compliance Program
- An updated Agent List
- An internal program for reviewing and reporting suspicious transactions and currency transactions
- An internal training program for all staff
- An annual Independent Compliance Audit

A. BSA Compliance Officer and Department

Wizz Networks has selected **Jessica Murphy** as the BSA Compliance Officer, whose duty is to ensure the Company follows this Compliance Policy including AML/BSA and OFAC compliance, including:

Policies and procedures:

- Developing and revising all policies and procedures for record keeping under the BSA and other laws applicable to MSBs;
- Developing and revising all policies and procedures for handling SAR and CTR reporting, responding to official requests for information, and independent audit reviews;
- Engaging external professionals to correct any compliance deficiencies or adapt to any regulatory changes and ensuring any recommendations are promptly implemented;
- Monitoring all transactions and inspecting any unusual activity;
- Reviewing SARs and other reports for precision prior to filing them with authorities; and
- Observing staff and partner activity for compliance with this Policy.

Reporting and Record-Keeping

- Using a secure records management procedure for storage and retrieval of certain transaction reports, customer identity information, and other documents and logs.
- Ensuring accurate and timely reporting in order to maintain compliance with all requirements of an MSB.
- Keeping this Compliance Policy and the accompanying training material up-to-date.
- Maintaining all SAR and CTR reports and accompanying records for 5 years.
- Maintaining an up-to-date agent list.

Training:

- Overseeing Wizz Network's Compliance Training Program to ensure that staff and partners are properly trained on all FinCEN requirements of an MSB, what to look for as unusual activity, the importance of record keeping, the prohibition against telling customers about reporting requirements, how to look for signs of placement, structuring, or lawyering, what OFAC requirements are necessary, the penalties for non-compliance, and the overall importance of this Policy.
- Delivering additional training each time this Policy is updated, regulations change, a compliance deficiency is found, or at a minimum, annually as a refresher.

Wizz Network's BSA Compliance Officer is also charged with speaking on behalf of the company to any regulatory agencies who may inquire. The BSA Compliance Officer may work closely with the Company's General Counsel or Outside Counsel, or other professional consultants and risk management specialists who help the BSA Compliance Officer in his execution of his duties.

B. Compliance Training

Wizz Networks trains all staff members or contracted third parties who have contact with customers or see customer transaction activity to ensure:

- They are aware of the laws relating to money laundering and counter-terrorist financing, and the requirements Wizz Networks has as a FinCEN registered MSB;

- They understand how to recognize and deal with transactions and other activities that may be related to money laundering or terrorist financing.

Wizz Networks trains new staff at the time they are hired and gives refresher training to existing staff any time: (1) the regulations change, (2) deficiencies in current compliance policies are identified, or (3) at a minimum, once per year. All training events are documented with their date, the person who facilitated the training, the materials that were taught, and the individuals who attended. Training includes:

1. The facilitator of the training will go through this manual with each employee;

2. Case Studies of recent FinCEN or OFAC enforcement actions;

3. Explanation of the rules applicable to Wizz Networks; and

4. Consequences for failure to comply with Wizz Network's Compliance Policy (ex: criminal, civil fines, immediate termination, etc.).

C. Independent Compliance Auditing Function

The Bank Secrecy Act requires money services businesses to establish anti-money laundering programs that include an independent audit function to test programs. An officer or employee of Wizz Networks may conduct the review so long as they are not the BSA Compliance Officer. The primary purpose of the independent review is to monitor the adequacy of the Company's anti-money laundering program. The review should determine whether the business is operating in compliance with the requirements of the BSA and the Company's own policies and procedures outlined in this Compliance Policy. Each MSB should identify and assess the money laundering risks that may be associated with its unique products, services, customers, and geographic locations.[xiii]

Wizz Networks will engage an independent auditor to test its compliance program each year. The final report will be reviewed by the BSA Compliance Officer, and any suggested changes will be implemented accordingly.

D. Transaction Analysis Function

Wizz Networks' clients (the "Clients") are known to the Company because the Company collects their identity information at the time they register. Wizz Networks also analyzes each of its client's transaction patterns to assess whether or not any transactions or patterns of transactions are suspicious or unusual. Wizz Networks performs the following precautions:

- Initial and ongoing checks of the customer against the OFAC SDN List and Non-SDN lists.
- Opening cases for investigation where needed.
- Filling out and sending SAR and CTR reports if needed.
- Documenting all customer and transactional data and preserving all records electronically, backed up periodically, for five years.
    - Record keeping must be done in a way to accomplish future retrieval if necessary.
    - Records should be stored using a logical sorting criterion based on dates written as yyyy-mm-dd.
    - Any incoming and outgoing mail should be scanned and stored according to its date. Outgoing mail should be sent certified or registered, with tracking numbers.
    - All records of incoming and outgoing communications with clients, partners, vendors, or independent contractors concerning transactions should be stored in chronological order, sorted by their date.

E. Federal Registration and Reporting

The BSA requires MSBs to file reports that can be used by FinCEN or the IRS for regulatory investigations. To file any mandatory reports, Wizz Networks has registered as a BSA E-Filer on http://bsaefiling.FinCEN.treas.gov/main.html.

Wizz Networks is required to renew its registration every two years by December 31 of the two-calendar year period following its initial registration. Wizz Networks filed its initial FINCEN registration on 11/20/2018 its MSB Registration Number is 31000136599927. Renewal needs to be completed by 12/31/2020.

i. Agent List

As a registered MSB, Wizz Network's must create a list of each agent that has been authorized to sell or distribute its MSB services. For Wizz Networks, the term "MSB Services" refers to the purchase or sale of virtual currencies.[xiv] The Agent List must be updated by January 1st of each year and must be made available to FinCEN upon request.

The agent list must include:

1. Agent's legal name.

2. Agent's address.

3. Description of the Services the Agent provides on behalf of the Wizz Networks.

4. Gross Transaction Amount: A listing of the previous 12 months in which the agent purchased or sold greater than $100,000 worth of virtual currency (excluding commissions and fees). Information about the agent volume must be current within 45 days of the due date of the agent list.

5. Depository Institution. The name and address of any depository institution at which the agent maintains a transaction account for all, or part of the funds received in or for the services the agent provides on behalf of Wizz Networks.

6. Year Became Agent. The year the Agent became an Agent for Wizz Networks.

7. Branches: The number of Branches and Sub-Agents the Agent has, if any.

ii. Only One Official Reporter

Wizz Networks' BSA Compliance Officer is responsible for all federal reporting. No other Wizz Networks personnel are to engage in any official reporting.

iii. Suspicious Activity

Suspicious activity is any observed behavior that could indicate money laundering, terrorism or terror-related crimes. Whether a particular transaction requires reporting must be decided by the MSB based on all of the facts and circumstances relating to the transaction or pattern of transactions in question.

Reportable transactions: The threshold for Wizz Networks is $2,000 and reportable transactions include:

- Transactions involving funds derived from illegal activity or intended or conducted in order to hide or disguise funds or assets derived from illegal activity;

- Transactions designed, whether through structuring or other means, to evade the requirements of the BSA; and

- Transactions that appear to serve no business or apparent lawful purpose.

When to file a SAR: Wizz Networks will file a SAR if a customer admits or makes some kind of statement involving criminal activities, attempts to convince an employee not to complete any documentation required for the transaction, makes inquiries that indicate a desire to avoid reporting, provides inaccurate or counterfeited documentation, or refuses to produce the required

documentation. Wizz Networks will also be on the lookout for activity that is inconsistent with what would be expected from the customer's declared business, transactions that appear unnecessarily complex for its stated purpose, or are not economically viable for the customer.

Wizz Networks will monitor transactions for dollar volume and frequency by each customer and will investigate deviations in the customer's transaction history.

Timeline for filing a SAR: MSBs are given 30 days after becoming aware of a suspicious transaction to complete a SAR and electronically file it with FinCEN. In situations involving violations that require immediate attention, such as ongoing money laundering schemes, the appropriate MSB should to notify the appropriate law enforcement authority immediately, by telephone, in addition to filing the required form.

Supporting documentation relating to each SAR is to be collected and maintained review as needed by law enforcement and regulatory agencies. The rule incorporates the statutory provision (called a "safe harbor") that provides broad protection from liability to customers of financial institutions that report suspicious transactions. In addition, the rule specifically prohibits persons filing suspicious transaction reports from disclosing, except to law enforcement and regulatory agencies, that a report has been filed or from providing any information that would disclose that a report has been prepared or filed.[xv]

Mandatory SAR reporting of cyber-events: If Wizz Networks knows, suspects, or has reason to suspect that a cyber-event was intended, in whole or in part, to conduct, facilitate, or affect a transaction or a series of transactions, it should be reported as suspicious transaction.

iv. Funds Transfer Records (The Travel Rule)

Any time a $3,000 transfer of funds takes place, the Travel Rule procedures of in 31 C.F.R. § 1010.410(e) must be followed. The financial institution initiating the transmission greater than $3,000 needs to send the receiving financial institution the following information:

1. The name of the transmittor;
2. The account number of the transmittor;
3. The address of the transmittor;
4. The identity of the transmittor's financial institution;
5. The amount of the transmittal order;
6. The execution date of the transmittal order; and
7. The identity of the recipient's financial institution.

If there's an intermediary in the transaction, it is required to pass on everything it receives from the transmitter's financial institution but has no general duty to collect more than it receives.

v. Currency Transaction Reports (CTRs)

Wizz Networks must file a Currency Transaction Report (CTR) within 15 days whenever a transaction or series of transactions in currency (or virtual currency such as bitcoin):

1. Involves more than $10,000 in either cash-in or cash-out, and
2. Is conducted by, or on behalf of, the same person, and
3. Is conducted on the same business day.

Multiple cash transactions are considered to be one transaction on which a CTR must be filed if the MSB has knowledge that:

1. They are by or on behalf of the same customer during one business day, and
2. They are conducted at one or more branches or agents of the same MSB, and
3. They total more than $10,000 in either cash-in or cash-out.

The CTR must be filed electronically. Wizz Networks' BSA Compliance Officer must be registered on the FinCEN e-filer system as a "Supervisory User" and subscribed to the role of "FinCEN CTR Filer."

Electronic filing instructions can be found under "User Quick Links" of the BSA E-Filing System homepage (http://bsaefiling.fincen.treas.gov/main.html) or on the "Forms" page of the FinCEN Web site (http://www.fincen.gov/forms/bsa_forms/).

The filing name should be "Wizz Networks, LLC" and that name should be used consistently for any FinCEN filings.

Wizz Networks must follow these steps when completing a FinCEN CTR:

1. Complete the report in its entirety with all requested or required data known to the filer.
2. Click "Validate" to ensure proper formatting and that all required fields are completed.
3. Click "Sign with PIN" – Enter the personal identification number (PIN) the BSA E-Filing System has assigned to your user ID. If you do not know your PIN, please click on the "Manage PIN" link in the left navigation menu for your PIN to be displayed.
4. Click "Save" – Filers may also "Print" a paper copy for their records. The "Save" button will allow you to select the location to save your filing.
5. Click "Submit" – After clicking "Submit," the submission process will begin.

Amending a CTR: If Wizz Networks needs to amend or correct a CTR, this can be accomplished by checking "Correct/amend prior report" and enter the previous Document Control Number

(DCN)/BSA Identifier (ID) in the appropriate field. The filer should complete the FinCEN CTR in its entirety, including the corrected/amended information, save (and keep a copy for its records). The corrected/amended FinCEN CTR will be assigned a new BSA ID.

Saving the CTR: The BSA E-Filing System is not a record keeping program; consequently, filers are not able to access or view previously filed reports. The BSA E-Filing System does provide tracking information on past report submissions and acknowledgements for accepted BSA reports. Users of the BSA E-Filing System must save and can print a copy of the FinCEN CTR prior to submitting it. FinCEN does not provide copies of filed reports to filers. After submitting a report via the BSA E-Filing System, filers are required to save a printed or electronic copy of the report in accordance with applicable record retention policies and procedures and must keep copies of their filing for five years.

Recording Multiple Transactions on a CTR: A CTR would be completed indicating those entities on whose behalf the transaction(s) were conducted and those individual(s) conducting the transaction(s). Each entity and individual would be listed in a respective Part I.[xvi]

Questions about CTR: FinCEN is very receptive to questions and can be contacted at:

- 1-800-767-2825 or (703) 905-3591 or by emailing your inquiry to FRC@fincen.gov.

vi. Report of Foreign Bank and Financial Accounts (FBAR)

While Wizz Networks will likely never encounter the need to file an FBAR, if the Company takes on a financial interest in, or signature authority over, a foreign financial account that has an aggregate value exceeding $10,000 at any time during the calendar year, the BSA Compliance Officer must file an FBAR by June 30th of the following year.[xvii]

vii. Information Sharing and Response to Official Requests

Under the Open Government Directive, FinCEN is required to take immediate, specific steps to promote transparency, participation, and collaboration with other Federal Agencies. Nothing in the Open Government policies or memoranda is inconsistent with, or lessens in any way, FinCEN's obligations to protect classified and other sensitive information, including, for example, FinCEN data and personally identifiable information.[xviii]

A law enforcement agency investigating terrorist activity or money laundering may request that FinCEN solicit, on the investigating agency's behalf, certain information from Wizz Networks. When making this request to FinCEN, the law enforcement agency would have to provide a written request that states:

- Each individual, entity, or organization about which the law enforcement agency is seeking information;

- What terrorist or money laundering activity the individual, entity, or organization is

suspected to be engaged in;

- The request must include enough specific identifiers, such as date of birth, address, and social security number, that would permit a financial institution to differentiate between common or similar names; and

- Identify one person at the federal agency to field any questions relating to its request.

Upon receiving the requisite certification from the requesting law enforcement agency, FinCEN may require any MSB to search its records to determine whether it has maintained accounts for, or has engaged in transactions with, any specified individual, entity, or organization.

If FinCEN makes such an information request of Wizz Networks, Wizz Networks must expeditiously search its records to determine whether it maintains or has ever maintained any account for, or has engaged in any transaction with, each individual, entity, or organization named in FinCEN's request.

Except as otherwise provided in the information request, Wizz Networks shall only be required to search its records for:

A. Any current account maintained for a named suspect;

B. Any account maintained for a named suspect during the preceding twelve months; and

C. Any transaction, as defined by § 1010.505(d)[xix], conducted by or on behalf of a named suspect, or any transmittal of funds conducted in which a named suspect was either the transmittor or the recipient, during the preceding six months that is required under law or regulation to be recorded by the financial institution or is recorded and maintained electronically by the institution.

If a transaction is identified for any individual, entity, or organization named in a request from FinCEN, Wizz Networks must provide FinCEN with the following information:

A. The name of such individual, entity, or organization;

B. The number of each such account, or in the case of a transaction, the date and type of each such transaction; and

C. Any Social Security number, taxpayer identification number, passport number, date of birth, address, or other similar identifying information provided by the individual, entity, or organization when each such account was opened, or each such transaction was conducted.

Upon receiving an information request under this section, Wizz Networks' BSA Compliance Officer is the only point of contact. When requested by FinCEN, Wizz Networks shall provide FinCEN with the name, title, mailing address, e-mail address, telephone number, and facsimile number of Jessica Murphy, in such manner as FinCEN may prescribe. Any changes to such contact information must be updated promptly.

This information may not be used for any other purpose than:

1. Reporting to FinCEN as provided in this section;

2. Determining whether to establish or maintain an account, or to engage in a transaction; or

3. Assisting the financial institution in complying with any other FinCEN requirements.[xx]

It is very important that Wizz Networks does not alert the individual, entity, or organization that FinCEN has made any information requests. The adequate procedures for safeguarding this confidentiality are outlined in Section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801).[xxi] Wizz Networks maintains this confidentiality by securing such records with a secure password protected file storage that is accessible only to Jessica Murphy and Gus Demos.

Receiving an information request from FinCEN does not mean that Wizz Networks should close the account or refuse to process transactions on behalf of the individual, entity, or organization under investigation unless it is directed to do so by FinCEN.

viii. Voluntary Information Sharing

USA PATRIOT Act Section 314(b) encourages financial institutions, upon providing notice to the United States Department of the Treasury, to share information with one another in order to identify and report to the federal government activities that may involve money laundering or terrorist activity.

While information sharing under the 314(b) program is voluntary, it can help financial institutions enhance compliance with their anti-money laundering/counter-terrorist financing (AML/CFT) requirements, most notably with respect to:

- Gathering additional information on customers or transactions potentially related to money laundering or terrorist financing, including previously unknown accounts, activities, and/or associated entities or individuals.

- Shedding more light upon overall financial trails, especially if they are complex and appear to be layered amongst numerous financial institutions, entities, and jurisdictions.

- Building a more comprehensive and accurate picture of a customer's activities where potential money laundering or terrorist financing is suspected, allowing for more precise decision-making in due diligence and transaction monitoring.

- Alerting other participating financial institutions to customers whose suspicious activities it may not have been previously aware.

- Facilitating the filing of more comprehensive SARs than would otherwise be filed in the absence of 314(b) information sharing.

- Identifying and aiding in the detection of money laundering and terrorist financing methods and schemes.

- Facilitating efficient SAR reporting decisions - for example, when a financial institution obtains a more complete picture of activity through the voluntary information sharing process and determines that no SAR is required for transactions that may have initially appeared suspicious.[xxii]

In cases where a financial institution files a SAR that has benefited from 314(b) information sharing, FinCEN encourages financial institutions to note this in the narrative in order for FinCEN to identify and communicate specific examples of the benefits of the 314(b) program. Please note, however, that while information may be shared related to possible terrorist financing or money laundering that resulted in, or may result in, the filing of a SAR, Section 314(b) does not authorize a participating financial institution to share a SAR itself or to disclose the existence of a SAR.

Financial institutions wanting to do so may register here: https://www.fincen.gov/314b/Register.

Should Wizz Networks decide to voluntarily opt in, its BSA Compliance Officer would be the primary point of contact for receiving and providing information under 314(b). Before honoring a request for information under section 314(b), Wizz Networks will need to verify that the other financial institution or association of financial institutions with which it intends to share information has also submitted the required notice to FINCEN. It will do so by consulting FINCEN's list of participating financial institutions and their related contact information.

F. Customer Due Diligence ("CDD")

FinCEN's CDD Rule, which amends the Bank Secrecy Act, has four core requirements. It requires covered financial institutions to establish and maintain written policies and procedures that are reasonably designed to:

1. Identify and verify the identity of customers;

2. Identify and verify the identity of the beneficial owners of companies opening accounts;

3. Understand the nature and purpose of customer relationships to develop customer risk profiles; and

4. Conduct ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[xxiii]

In order to carry out its intended business of offering tax-advantaged Individual Retirement Accounts, Wizz Networks is required to collect detailed information on each of its clients, which comply with all of FinCEN's KYC guidelines. Wizz Networks collects the following from each customer:

1. Full Name,

2. Former Aliases,
3. Address,
4. Type of ID provided, ID #or Alien ID #,
5. Social Security Number,
6. Mobile phone number,
7. Email address,
8. Date of Birth,
9. Place of Birth, and
10. Nationality.

If the customer is an institution, Wizz Networks collects the following information prior to opening an account:

1. Institution legal name,
2. Employer Identification Number ("EIN") or any comparable identification number issued by the government,
3. Full legal name (of all account signatories and beneficial owners),
4. Email address (of all account signatories),
5. Mobile phone number (of all account signatories),
6. Address (principal place of business and/or other physical location),
7. Proof of legal existence (e.g., state certified articles of incorporation or certificate of formation),
8. Unexpired government-issued business license, trust instrument or other comparable legal documents as applicable,
9. Contract information of owners/principals/executive management (as applicable),
10. Proof of identity (e.g., driver's license, passport or government-issued ID) for each individual,
11. Beneficial owner that owns 10% or more, as well as all account signatories, and
12. Identifying information for each entity beneficial owner that owns 10% or more (see individual customer information collected above for more details).

i. Identity Screening

Wizz Networks has implemented procedures for comparing the customer's information against third-party public records databases to verify that the customer's information indicates the customer is a real person. The photograph of the customer is compared to the photograph on the customer's government identification to confirm it is the same individual.

Wizz Networks also screens each customer against the OFAC SDN list. If a customer matches a name on the OFAC SDN List, Wizz Networks proceeds to check the full name against all records it has of this individual including address, nationality, passport, SSN, Tax ID, place of birth, date of birth, former names and aliases. If the match appears concrete, Wizz Networks calls the OFAC hotline: 1-800-540-6322.[xxiv]

ii. Know Your Employee

It is also critical for Wizz Networks to be aware of the company's staff members and independent contracts and screen them before hiring or contracting with them and collects the following information:

1. Full Name,
2. Former Aliases,
3. Address,
4. Type of ID provided, ID #or Alien ID #,
5. Social Security Number,
6. Telephone Number,
7. Date of Birth,
8. Place of Birth, and
9. Nationality.

All employees must read this manual and sign an affirmation that they have read, understand and commit to abide by its provisions.

iii. Know Your Vendor

Wizz Networks also collects detailed information on its vendors and screens them against the OFAC SDN list.

Wizz Networks' BSA Compliance Officer must subject each potential vendor to the following questionnaire and receive and review certain documents that the vendor supplies.

1. Certificate of Good Standing,

2. Evidence of vendor's MSB Registration,

3. List of shareholders with 10% or higher stake, if company is privately owned. If publicly owned, most recent annual corporate reports (or internet address).

4. The vendor's written AML policies and procedures,

5. The vendor's latest independent audit of its AML program including management response (if applicable and available).

6. The vendor's organizational chart showing name of key officers, directors and employees.

7. Name and contact information of the vendor's BSA Compliance Officer.

iv. Vendor Monitoring Procedures

Wizz Networks conducts ongoing monitoring of the activity and behavior of each vendor, including periodic OFAC re-screening.

v. Termination for Compliance Reasons

If Wizz Networks deems it necessary, the BSA Compliance Officer may terminate any vendor relationship that is perceived as an unacceptable high risk.

G. OFAC Compliance

OFAC administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Prohibited transactions are trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute.

OFAC requires prohibited transactions to be blocked. In this case, title to the blocked property remains with the target, but the exercise of powers and privileges normally associated with ownership is prohibited without authorization from OFAC. Blocking immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.[xxv]

Wizz Networks and its Senior Management promotes a "culture of compliance" throughout the organization and understand that OFAC compliance is a critical factor in determining this Policy's effectiveness against money laundering and terrorist financing.

Senior Management ensures that its compliance program has delegated sufficient authority and autonomy to deploy its policies and procedures in a manner that effectively controls the organization's OFAC risk. Senior management has taken, and will continue to take, steps to

ensure that the organization's compliance unit(s) receive adequate resources—including in the form of human capital, expertise, information technology, and other resources, as appropriate—that are relative to the organization's breadth of operations, target and secondary markets, and other factors affecting its overall risk profile.

Wizz Networks has appointed Jessica Murphy as the dedicated OFAC sanctions compliance officer and ensured he has the technical knowledge and expertise with respect to OFAC's regulations, processes, and actions and has the. Ability to identify OFAC-related issues, risks and. Prohibited. Activities.[xxvi]

Wizz Networks screens its customers and vendors against the OFAC SDN list, and also conducts periodic screening to ensure continued compliance. In the event of a positive match, the OFAC Compliance Officer, the BSA Compliance Officer may consult legal counsel and determine whether the customer or vendor's account must. Be. Terminated and/or whether the funds must be blocked.

In the event that funds are blocked, Wizz Networks will place them into an account on Wizz Networks' books from which only OFAC-authorized debits may be made. The blocking also must be reported to OFAC Compliance within 10 business days, and annually by September 30 of each year the assets are blocked.

As required by law, Wizz Networks will report all OFAC-related blockings within 10 business days of the occurrence and annually, by September 30, it will send a report to OFAC concerning the assets blocked in the last twelve months, if any. The annual report must be made in the Annual Report of Blocked Property by filling out Treasury Form TD F 90-22.50.[xxvii]

In order to test its OFAC Screening system, Wizz Networks will attempt to onboard an individual on the OFAC list. Wizz Networks will then document the positive identification and alert. If the signup does not result in a positive identification and alert, this will be investigated and documented, and sign-up procedures will be immediately enhanced before any additional customers can be on-boarded.

H. Privacy

Wizz Networks is required to protect the privacy of Consumer Financial Information according to the Privacy Rule of the Gramm-Leach-Bliley Act (the "GLBA"). The Privacy Rule protects a consumer's "nonpublic personal information" ("NPI"). NPI is any "personally identifiable financial information" that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise publicly available.[xxviii]

Wizz Networks will provide each customer an initial privacy notice by clearly and conspicuously posting the notice on its website. Wizz Networks has taken steps to secure its customers' data and personal non-public information and will only share this information with law enforcement when required by law.

All of Wizz Networks' confidential documents and files are stored electronically in manner that

is reasonably protected against destruction and physical damage. Access is limited by secure passwords only available to senior management. Secure backups are also kept. When the information is no longer required to be stored, it is deleted in a secure fashion.

I. FCPA Compliance

Wizz Networks is committed to compliance with the US Foreign Corrupt Practices Act (the "FCPA") of 1977 and prohibits bribery payments to foreign officials.

While Wizz Networks does not foresee any situations where it would encounter foreign officials seeking bribery, all Wizz Networks staff agree to the following guidelines:

- No payments of anything of value are made to anyone for the purpose of obtaining an improper advantage.
- No payment intermediaries are used to channel payments that would violate the FCPA.
- All vendors also agree to follow the FCPA.
- No gratuity, gifts, or other payments are made to anyone for the purpose of expediting an administrative action.
- No company funds are donated to foreign political parties or campaigns.
- No payments to third parties are authorized that are unreasonable for the work performed.

J. Blocking Customers

Wizz Networks may close the accounts of customers who violate Wizz Networks' Terms of Service or Customer Agreement or is found to be engaged in suspicious activity. A list of all customers whose accounts have been closed will be maintained and checked when new customers attempt to register for an account.

References:

[i] https://www.fincen.gov/sites/default/files/shared/bsa_quickrefguide.pdf

[ii] https://www.fincen.gov/money-services-business-definition

[iii] https://www.fincen.gov/money-services-business-msb-agent-list

[iv] https://www.fincen.gov/money-services-business-msb-suspicious-activity-reporting

[v] http://moneyservicesbusiness.com/reporting/ctrs/

[vi] https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf

[vii] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#start

[viii] https://www.nafcu.org/compliance-blog/bsaaml-violations-can-cost-you

[ix] https://www.fincen.gov/news-room/enforcement-actions

[x] https://cws.auburn.edu/vpr/ConMan/ConMan_FileDownload.aspx?filename=violations.pdf

[xi] https://www.fincen.gov/history-anti-money-laundering-laws

[xii] https://www.fincen.gov/resources/statutes-regulations/administrative-rulings/suspicious-activity-reporting-structuring

[xiii] https://www.fincen.gov/sites/default/files/shared/Guidance_MSB_Independent_Audits9-21.pdf

[xiv] https://www.fincen.gov/each-agent

[xv] https://www.fincen.gov/sites/default/files/shared/msbsarfs.pdf

[xvi] https://www.fincen.gov/frequently-asked-questions-regarding-fincen-currency-transaction-report-ctr

[xvii] https://www.fincen.gov/report-foreign-bank-and-financial-accounts

[xviii] https://www.fincen.gov/fincens-commitment-open-government

[xix] Except as provided in paragraph (bbb)(2) of this section, transaction means a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition, and with respect to a financial institution includes a deposit, withdrawal, transfer between accounts, exchange of currency, loan, extension of credit, purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument, security, contract of sale of a commodity for future delivery, option on any contract of sale of a commodity for future delivery, option on a commodity, purchase or redemption of any money order, payment or order for any money remittance or transfer, purchase or redemption of casino chips or tokens, or other gaming instruments or any other payment, transfer, or delivery by, though, or to a financial institution, by whatever means effected. For purposes of §§ 1010.311, 1010.313, 1020.315, 1021.311, 1021.313, and other provisions of this chapter relating solely to the report required by those sections, the term "transaction in currency" shall mean a transaction involving the physical transfer of currency from one person to another. A transaction which is a transfer of funds by means of bank check, bank draft, wire transfer, or other written order, and which does not include the physical transfer of currency, is not a transaction in currency for this purpose.

[xx] https://www.law.cornell.edu/cfr/text/31/1010.520

[xxi] https://www.law.cornell.edu/uscode/text/15/6801

[xxii] https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

[xxiii] https://www.fincen.gov/news/news-releases/fincen-reminds-financial-institutions-cdd-rule-becomes-effective-today

[xxiv] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/pg5.aspx

[xxv] https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_general.aspx

[xxvi] https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

[xxvii] https://www.treasury.gov/resource-center/sanctions/Documents/td902250.pdf

[xxviii] https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm