Anti-Money Laundering Policy

Version: October 30, 2023

1. Introduction

Casa Systems, Inc. (together with its subsidiaries and affiliates, the "Company") is committed to observing the highest standards of ethical conduct in its operations throughout the world. The Company shall comply with laws that prohibit money laundering or terrorist financing that are applicable to Casa Systems, Inc. or any subsidiary or affiliate thereof, including in any jurisdiction in which it operates or otherwise undertakes business ("Anti-Money Laundering Laws"). The Company does not condone, facilitate or support money laundering or terrorist financing. This Anti-Money Laundering Policy (the "Policy") applies to and is intended to help ensure that the Company and its employees, directors, officers, agents and controlled affiliates understand and comply with the Anti-Money Laundering Laws.

This Policy refers to a Compliance Manager. The Compliance Manager for purposes of this Policy as of August 15, 2023, is Thomas Billbrough (thomas.billbrough@casa-systems.com).

2. Definition of Money Laundering and Terrorist Financing

Money laundering is the process by which those involved in criminal activities conceal the source of and disguise the nature of illicit funds by making them appear legitimate. The process generally involves three stages:

- **Placement** – the placement of illicit funds into the financial system by converting those funds into some other financial instrument or medium;
- **Layering** – the separation of illicit funds from their source by involving those funds in a series of legitimate transactions; and
- **Integration** – the involving of illicit funds in a series of transactions intended to make it appear that the funds have been derived from a legitimate source.

Terrorist financing may or may not involve the proceeds of criminal conduct, but may nonetheless involve an attempt to conceal either the origin of funds or their intended use, which could be for criminal purposes. Although the motivation may differ between traditional money launderers and those engaged in terrorist financing, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorism does not always require large sums of money, and the associated transactions may not be complex.

3. Red Flags for Trade Based Money Laundering

Money launderers may engage in so-called trade-based money laundering ("TBML"), which is defined as the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimize their illicit origin. Red flags for TBML include but are not limited to:

- Customer/Counterparty is incorporated or has substantial operations in a jurisdiction with weak anti-money laundering ("AML") or counter-terrorist financing ("CTF") legal infrastructure (e.g., a jurisdiction identified by the Financial Action Task Force ("FATF") as being "high risk" and "subject to a call for action" or a jurisdiction identified by FATF as being subject to "increased monitoring"). FATF has identified high risk and other monitored jurisdictions here: High-risk and other monitored jurisdictions (fatf-gafi.org).
- Customer/Counterparty has an unnecessarily complex corporate or organizational structure involving multiple shell entities without an obvious business purpose.
- Customer/Counterparty is unwilling or unable to provide a physical address (e.g., an address other than a Post Office Box) where its business is located, or the address provided does not appear to be appropriate for the Customer's/Counterparty's business activities (e.g., Customer/Counterparty purports to be engaged in a manufacturing business but provides a residential address without adequate explanation).
- Customer/Counterparty lacks an online or public presence or online or its public presence is not consistent with its stated or known business activities.
- Customer/Counterparty has experienced unexplained dormancy in its business.
- There is negative news relating to the Customer/Counterparty or its owners (e.g., reports of money laundering, fraud, tax evasion, public corruption, other criminal activity or prior or ongoing investigation of such activity).
- Existence of Customer/Counterparty cannot be confirmed through a public record search (e.g., search of Secretary of State database or company register).
- Customer/Counterparty payments originate from a jurisdiction other than the jurisdiction where the Customer/Counterparty's business operations are primarily located, and Customer/Counterparty is not able to offer an adequate explanation.
- Customer/Counterparty payments are made by a person that appears to be unrelated to Customer/Counterparty, and Customer/Counterparty is not able to offer an adequate explanation.
- Customer/Counterparty requests "over" or "under" invoicing of goods/services (e.g., misrepresenting the value of the goods or services provides), false invoices and/or multiple invoices for the same goods or services, often in combination with a request or understanding that a "refund" will be provided.
- Customer/Counterparty makes a payment originating from a particular account or jurisdiction and requests a refund or payment to another account or an account in a different jurisdiction without adequate explanation.

If an employee identifies or becomes aware of a red flag, he or she shall escalate such red flag to the Compliance Manager through a manager or division head.

4. Risk Assessment

The Company believes that its business presents a low risk of inadvertently facilitating money laundering or terrorist financing because its business involves providing physical, virtual and cloud-native 5G infrastructure and customer premise networking equipment solutions to communications service providers and does not involve the provision of financial services. The Company does not accept cash payments and only receives payments for the sale of goods and services through transactions intermediated through regulated financial institutions.

5. Policy

The Company is not a financial institution required to maintain a formal anti-money laundering policy. However, the Company's policy is not to facilitate money laundering or terrorist financing. Although the Company does not conduct special diligence to determine the identity of its customers or counterparties or the source of funds of its customers or counterparties, the Company shall not do business with or conduct a transaction with any person if the Company believes that such person presents a money laundering risk or is engaged in terrorist financing. In particular, the Company shall refuse to conduct business with a person or entity that the Company believes to be engaged in money laundering, terrorist financing or other illegal activity, including any person engaged in conduct that may indicate a risk of TBML or other forms of money laundering. The Company's policy is to refuse requests to facilitate TBML or other forms of money laundering or terrorist financing.

In the event the Company is required to process a refund, it is the Company's policy to refund the amount due to the same person that made the payment and to the same account or payment method by which the original payment was made unless the Company receives a satisfactory explanation. The Company's policy is to make payments to third parties only (a) in exchange for legitimate goods, services and/or property provided to the Company having a value equivalent to the amount paid, (b) in satisfaction of the Company's legal obligations, or (c) in connection with distributions to the Company's shareholders.

6. Training

The Company will provide and employees are required to receive training regarding this Policy based on the knowledge and skills required to perform their duties. At a minimum, Company personnel with responsibilities for onboarding new customers and new hires will be trained to recognize and mitigate potential money laundering and terrorist financing issues within 30 days of being hired and not less frequently than once during every 18-month period thereafter. The Company will create and maintain records of attendance at required trainings, training materials, and audit compliance with training requirements.

7. Violation

A violation of the Anti-Money Laundering Laws can potentially expose the Company and the employees involved to significant civil or criminal liability. Accordingly, any employee, director, officer or agent who violates this Policy by engaging in or facilitating the conduct of money laundering or terrorist financing, including by the Company or a customer or counterparty of the Company, may be subject to disciplinary action up to and including termination of employment and/or referral to governmental authorities.

8. Administration of Policy

The Compliance Manager is responsible for maintaining, implementing and updating this Policy, including at least annually reviewing the effectiveness of the Policy against the Company's risk profile to determine whether revisions or updates to the Policy are necessary.

The Compliance Manager is further responsible for investigating red flags reported to him or her and determining whether the Company should continue its relationship with the identified customer or counterparty under the Policy or whether other action by the Company is warranted in light of such reported red flag. The Compliance Manager will create a record of any instance in which activity constituting a red flag is escalated to the Compliance Manager and the manner in which such red flag was resolved or handled.

The Chief Financial Officer of the Company and his or her designees is responsible for reviewing anonymously reported violations of the Policy and reporting such alleged violations to the Compliance Manager. The Compliance Manager will ensure that the Company maintains any records created in accordance with this Policy for at least five years from the date each such record is created.

Document History:

- *Adopted: August 15, 2023*
- *Amended and restated: October 30, 2023*