ANTI MONEY LAUNDERING POLICY

It is the policy of the Era Swap Technologies (“Company”) to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable requirements of prevailing anti-money laundering statutes and implementing regulations.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages. Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions. At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs

between traditional money launderers and terrorist financiers, 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 terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Our AML policies, procedures and internal controls are designed to ensure compliance with all applicable regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

2. AML Compliance Person Designation and Duties

The Company has designated its Directors as its Anti-Money Laundering Policy Compliance officer, with full responsibility for the Company's AML policy (hereinafter referred as AML Compliance Party or designated Director). The duties of the AML Compliance designated Director, will include monitoring the Company's compliance with AML obligations, overseeing communication and training for employees. The Designated Director will also ensure that the Company keeps and maintains all of the required AML records, if any. The Designated Director is vested with full responsibility and authority to enforce the Company's AML policy.

3. Giving AML Information to Law Enforcement Agencies and Other Financial Institutions

We will respond to all law enforcement requests concerning accounts and transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction

with, each individual, entity or organization named in the request. Our policy is to respond to such inquiries within 14 days, unless otherwise specified. If the AML Compliance Party searches our records and does not find a matching account or transaction, then the AML Compliance Party will not reply to the request. We will maintain documentation that we have performed the required search.

We will respond to the request of law enforcement when we find a matching account or transaction. We will disclose to the party or parties of the subject account or transaction that law enforcement has requested or obtained information from us, except to the extent necessary to comply with the information request. The AML Compliance Party will review, maintain and implement procedures to protect the security and confidentiality of requests regarding the protection of customers' nonpublic information. We will direct any responses we receive to the requesting law enforcement agency as designated in the request. Unless otherwise stated in the law enforcement request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the periodic required as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

We understand that the receipt of a grand jury subpoena concerning a customer does not in itself require that we file a response. When we receive a grand jury subpoena, we will conduct a risk assessment of the customer subject to the subpoena as well as review the customer's account activity. If we uncover suspicious activity during our risk assessment and review, we will elevate that customer's risk assessment and may response to the subpoena. We understand that none of our officers, employees or agents may directly or indirectly disclose

to the person who is the subject of the subpoena its existence, its contents or the information we used to respond to it. To maintain the confidentiality of any grand jury subpoena we receive, we will process and maintain the subpoena by theAML Compliance Party.

We will share information with other financial institutions regarding individuals, entities, organizations and countries for purposes of identifying and, where appropriate, reporting activities that we suspect may involve possible terrorist activity or money laundering. We understand that this requirement applies even to financial institutions with which we are affiliated, and that we will obtain the requisite notices from affiliates and follow all required procedures.

We will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the Company's other books and records.

We also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities;

- determining whether to establish or maintain an account, or to engage in a transaction; or

- assisting the financial institution in complying with performing such activities.

4. Checking & Control Listings

Before opening an account, and on an ongoing basis, the AML Compliance Party will check to ensure that a customer does not appear on the Specially Designated Nationals and Blocked Persons List (“SDN”) or is not engaging in transactions that are prohibited by the economic sanctions and embargoes.

If we determine that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes, we will reject the transaction and/or block the customer's assets.

5.Customer Identification Policy

a. Required Customer Information

Prior to opening an account, should it become applicable, AML Compliance Party will collect the following information for all accounts, if applicable, for any person, entity or organization that is opening a new account and whose name is on the account:

- (1) the name;
- (2) date of birth (for an individual);
- (3) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or

a principal place of business, local office, or other physical location (for a person other than an individual); and

- (4) an identification number, which will be a taxpayer identification, or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard.

  When opening an account for a foreign business or enterprise that does not have an identification number, we will request alternative government-issued documentation certifying the existence of the business or enterprise.

b. Customers Who Refuse to Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, our Company will not open a new account and, after considering the risks involved, consider closing any existing account.

c. Verifying Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. AML Compliance Party will analyze the information we obtain to determine whether the information is sufficient to form a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

We will verify customer identity through documentary means, non-documentary means or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. We may also use non-documentary means, if we are still uncertain about whether we know the true identity of the customer. In verifying the information, we will consider whether the identifying information that we receive, such as the customer's name, street address, zip code, telephone number (if provided), date of birth and tax identification number, allow us to determine that we have a reasonable belief that we know the true identity of the customer (e.g., whether the information is logical or contains inconsistencies).

Appropriate documents for verifying the identity of customers include the following:

- For an individual, an unexpired government-issued identification evidencing nationality or residence and bearing a photograph or similar safeguard, such as a driver's license or passport; an

- For a person other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as

verification of a customer's identity. If, however, we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We will use the following non-documentary methods of verifying identity:

- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database or other source;

- Checking references with other financial institutions; or

- Obtaining a financial statement.

We will use non-documentary methods of verification when: (1) the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard; (2) the Company is unfamiliar with the documents the customer presents for identification verification; (3) the customer and Company do not have face-to-face contact; and (4) there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before or after the account is opened. Depending on the nature of the account and requested transactions, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification,

restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering, terrorist financing activity, or other suspicious activity, we may, after internal consultation with the Company's AML Compliance Party, elect to not open such account.

We recognize that the risk that we may not know the customer’s true identity may be heightened for certain types of accounts, such as an account opened in the name of a corporation, partnership or trust that is created or conducts substantial business in a jurisdiction that has been designated by the United States as a primary money laundering jurisdiction, a terrorist concern, or has been designated as a non-cooperative country or territory. We will identify customers that pose a heightened risk of not being properly identified. We will also take the following additional measures that may be used to obtain information about the identity of the individuals associated with the customer when standard documentary methods prove to be insufficient.

d. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following: (1) not open an account; (2) impose terms under which a customer may conduct transactions while we attempt to verify the customer’s identity; or (3) close an account after attempts to verify customer’s identity fail

e. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancies identified in the verification process. We will keep records

containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will also keep records containing a description of the resolution of each substantive discrepancy discovered when verifying the identifying information obtained. We will retain records of all identification information for five years after the account has been closed; we will retain records made about verification of the customer's identity for five years after the record is made.

f. Comparison with Government-Provided Lists of Terrorists

At such time as we receive notice that a federal government agency has issued a list of known or suspected terrorists and identified the list as a list for CIP purposes, we will, within a reasonable period of time after an account is opened (or earlier, if required by another federal law or regulation or federal directive issued in connection with an applicable list), determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any federal government agency and designated as such by Treasury in consultation with the federal functional regulators. We will follow all federal directives issued in connection with such lists.

We will continue to comply separately with OFAC rules prohibiting transactions with certain foreign countries or their nationals.

g. Notice to Customers >

We will provide notice to customers that the Company is requesting information from them to verify their identities, where required by law

Important Information About Procedures for Opening a New Account
What this means for you: When you open an account, we will ask for your name, address, date of birth and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

6.General Customer Due Diligence

It is important to our AML policy that we obtain sufficient information about each customer to allow us to evaluate the risk presented by that customer and to detect and report suspicious activity. When we open an account for a customer, the due diligence we perform may be in addition to customer information obtained for purposes of our CIP.

We will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. Such information should include

- the customer's business
- the customer's anticipated account activity (both volume and type);
- the source of the customer's funds.

For accounts that we have deemed to be higher risk, we will obtain the following information:

- the purpose of the account;
- the source of funds and wealth;
- the beneficial owners of the accounts;
- the customer’s (or beneficial owner’s) occupation or type of business;
- financial statements;
- banking references;
- domicile (where the customer’s business is organized);
- description of customer’s primary trade area and whether international transactions are expected to be routine;
- description of the business operations and anticipated volume of trading;
- explanations for any changes in account activity.

7.Due Diligence and Enhanced Due Diligence Requirements for Private Banking Accounts/Senior Foreign Political Figures

We will review our accounts to determine whether we offer any private banking accounts and we will conduct due diligence on such accounts. This due diligence will include, at least, (1) ascertaining the identity of all nominal holders and holders of any beneficial ownership interest in the account (including information

on those holders' lines of business and sources of wealth); (2) ascertaining the source of funds deposited into the account; (3) ascertaining whether any such holder may be a senior foreign political figure; and (4) detecting and reporting, in accordance with applicable laws and regulations, any known or suspected money laundering, or use of the proceeds of foreign corruption.

We will review public information, including information available in Internet databases, to determine whether any private banking account holders are senior foreign political figures. If we discover information indicating that a particular private banking account holder may be a senior foreign political figure, and upon taking additional reasonable steps to confirm this information, we determine that the individual is, in fact, a senior foreign political figure, we will conduct additional enhanced due diligence to detect and report transactions that may involve money laundering or the proceeds of foreign corruption.

In so doing, we will consider the risks that the funds in the account may be the proceeds of foreign corruption by determining the purpose and use of the private banking account, location of the account holder(s), source of funds in the account, type of transactions conducted through the account and jurisdictions involved in such transactions. The degree of scrutiny we will apply will depend on various risk factors, including, but not limited to, whether the jurisdiction the senior foreign political figure is from is one in which current or former political figures have been implicated in corruption and the length of time that a former political figure was in office. Our enhanced due diligence might include, depending on the risk factors, probing the account holder's employment history, scrutinizing the account holder's source(s) of funds, and monitoring transactions to the extent necessary to detect and report proceeds of foreign corruption, and

reviewing monies coming from government, government controlled or government enterprise accounts (beyond salary amounts).

If we do not find information indicating that a private banking account holder is a senior foreign political figure, and the account holder states that he or she is not a senior foreign political figure, then we may make an assessment if a higher risk for money laundering, nevertheless, exists independent of the classification. If a higher risk is apparent, we will consider additional due diligence measures.

In either case, if due diligence (or the required enhanced due diligence, if the account holder is a senior foreign political figure) cannot be performed adequately, we will, after consultation with the Company's AML Compliance Party and, as appropriate, not open the account, suspend the transaction activity, or close the account.

8. Monitoring Accounts for Suspicious Activity

We will monitor account activity for unusual size, volume, pattern or type of transactions, taking into account risk factors and red flags that are appropriate to our business.Monitoring will be conducted through the automated monitoring.The AML Compliance Party or his or her designee will be responsible for this monitoring, will review any activity that our monitoring system detects, will determine whether any additional steps are required, will document when and how this monitoring is carried out, and will report suspicious activities to the appropriate authorities.

Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, we will immediately call an appropriate law enforcement authority.

Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers – Insufficient or Suspicious Information

- **Provides unusual or suspicious identification documents that cannot be readily verified.**

- **Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.**

- **Refuses to identify a legitimate source for funds or information is false, misleading or substantially incorrect.**

- **Background is questionable or differs from expectations based on business activities.**

- **Customer with no discernible reason for using the Company's service.**

Efforts to Avoid Reporting and Recordkeeping

- **Reluctant to provide information needed to file reports or fails to proceed with transaction.**

- **Tries to persuade an employee not to file required reports or not to maintain required records.**

- **“Structures” deposits, withdrawals or purchase of monetary instruments below a certain amount to avoid reporting or recordkeeping requirements.**

- **Unusual concern with the Company’s compliance with government reporting requirements and Company’s AML policies.**

Certain Funds Transfer Activities

- **Wire transfers to/from financial secrecy havens or high-risk geographic location without an apparent business reason.**

- **Many small, incoming wire transfers or deposits made using checks and money orders. Almost immediately withdrawn or wired out in manner inconsistent with customer’s business or history. May indicate a Ponzi scheme.**

- **Wire activity that is unexplained, repetitive, unusually large or shows unusual patterns or with no apparent business purpose.**

Certain Securities Transactions

- **Customer engages in prearranged or other non-competitive trading, including wash or cross trades of illiquid securities.**

- **Two or more accounts trade an illiquid stock suddenly and simultaneously.**

- **Customer journals securities between unrelated accounts for no apparent business reason.**

- **Customer has opened multiple accounts with the same beneficial owners or controlling parties for no apparent business reason.**

- **Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.**

- **Customer's trading patterns suggest that he or she may have inside information.**

Activity Inconsistent With Business

- **Transactions patterns show a sudden change inconsistent with normal activities.**

- **Unusual transfers of funds or journal entries among accounts without any apparent business purpose.**

- **Maintains multiple accounts, or maintains accounts in the names of family members or corporate entities with no apparent business or other purpose.**

- **Appears to be acting as an agent for an undisclosed principal, but is reluctant to provide information.**

- **Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.**

Other Suspicious Customer Activity

- **Law enforcement subpoenas.**

- **Large numbers of securities transactions across a number of jurisdictions.**

- **Buying and selling securities with no purpose or in unusual circumstances (e.g., churning at customer's request).**

- **Payment by third-party check or money transfer without an apparent connection to the customer.**

- **Customer transactions include a pattern of receiving stock in physical form or the incoming transfer of shares, selling the position and wiring out proceeds.**

- **Payments to third-party without apparent connection to customer.**

- **No concern regarding the cost of transactions or fees (i.e., surrender fees, higher than necessary commissions, etc.).**

9.Responding to Red Flags and Suspicious Activity

When an employee of the Company detects any red flag, or other activity that may be suspicious, he or she will notify the AML Compliance Party.

Under the direction of the AML Compliance Party, the Company will determine whether or not and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account and/or closing the account.

AML Recordkeeping

Our AML Compliance Party and its designee will be responsible for ensuring that AML records are maintained properly. In addition, as part of our AML policy, our Company will create and maintain relevant documentation on customer identity and verification and funds transmittals. We will maintain such documentation for at least five years. We will hold such documentation confidential. We will not inform any third party about the existence of such documentation

10. Clearing/Introducing Company Relationships

We will work closely with our third party partners to detect money laundering, if required. We will exchange information, records, data and exception reports as necessary to comply with AML laws.

11. Training Policies

We will develop ongoing employee training under the leadership of the AML Compliance Party and senior management. Our training will occur on at least an annual basis. It will be based on our Company's size, its customer base, and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) what to do once the risk is identified; (3) what employees' roles are in the Company's compliance efforts and how to perform them; and (4) the Company's record retention policy.

We will review our operations to see if certain employees, such as those in compliance, margin and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

12. Monitoring Employee Conduct and Accounts

We will subject employee accounts to the same AML procedures as customer accounts, under the supervision of the AML Compliance Party. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Party's accounts will be reviewed by the AML Compliance Person.

13. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the Company's AML compliance policy to the AML Compliance Party, unless the violations implicate the AML Compliance Party, in which case the employee shall report to the AML Compliance Party. Such reports will be confidential, and the employee will suffer no retaliation for making them.

14. Additional Risk Areas

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above.

15. Senior Manager Approval

Senior management has approved this AML compliance policy in writing as reasonably designed to achieve and monitor our Company's ongoing compliance with the requirements of prevailing law.