Terms & Conditions

INFORMATION SHARING AND CUSTOMER PRIVACY POLICIES

INFORMATION SHARING WITH OTHER FINANCIAL INSTITUTIONS

Section 314(b) permits financial institutions, including MSBs, to transmit, receive, or otherwise share information with other financial institutions regarding individuals, entities, organizations, and countries for the purpose of identifying and, where appropriate, reporting activities that the financial institution or association suspects may involve possible terrorist activity or money laundering.

If the business intends to share information, the business must submit to FinCEN a notice as described on FinCEN's website, www.FinCEN.gov. The notice is effective for a period of one year beginning on the date of the notice. To continue sharing information after the one year, the business must submit a new notice. Prior to sharing information, the business must take reasonable steps to verify that the other financial institution with which it intends to share information has submitted to FinCEN the required notice.

The information received using this regulation may not be used for any other purpose other than:

- Identifying and, where appropriate, reporting on money laundering or terrorist activities;
- Determining whether to engage in a transaction, or to establish or maintain on account; or
- Assisting the financial institution in complying with any requirement of this part. The business must maintain adequate procedures to protect the security and confidentiality of such information. The regulation also provides a safe harbor provision for the business if it adheres to the procedures in the regulation. If the business has a reason to suspect an individual, entity, or organization is involved in terrorist activity or money laundering, The business will file a SAR and notify law enforcement when necessary.

SHARING PROCEDURES

Our Company is not currently registered and therefore does not currently participate in Section 314(b) information sharing with other financial institutions. It is unlikely that Tawakal will need to participate in the 314(b) information sharing program. However, in the event that the business' bank requests our participation or the volume and risk of transaction activity warrants participation, the BSA Officer will evaluate the program requirements, establish appropriate procedures and register if determined appropriate.

CUSTOMER PRIVACY PROTECTION POLICIES

It is our Company's central policy to protect customer's private information that have been entrusted to us. The following policies have been instituted:

- Customer data is only accessed by authorized personnel and agents who have been vetted and trained in protecting customer information. Data is only entered and stored in our online database system that is only accessible to authorized staff only.
- All customer documents given to us by our customers must be locked in secured file cabinets that are accessed by authorized personnel. The documents include ID cards, social security information, addresses and other biographic information, and financial records such as checks, bank statements, pay slips etc.
- All information pertaining to customer transactions and information must be sent through our secured database system only. All online database system is well secured with adequate firewall protection against hacking.
- All information and documents containing customer information that needs to be destroyed must be done in accordance with our Company's documents destruction policies. The Compliance officer provides training on how to destroy using the approved shredding machines per our Company's requirements.

IDENTITY THEFT PROTECTION

We have implemented identity theft protection program and included policies for detecting, preventing, and mitigating identity theft. These policies requires us to:

- identify relevant patterns, practices and specific forms of activity that are "red flags" signaling possible identity theft.
- detect red flags that have been incorporated into the internal control program.
- respond appropriately to any red flags that are detected to prevent and mitigate identity theft, and
- ensure the program is updated periodically to reflect changes in risks from identity theft.