Private and Confidential

REFINITIV – END CUSTOMER TERMS & CONDITIONS

Refinitiv terms to be flown down by Partner in its Customer Agreement:

1. USGAGE PERMISSIONS AND RESTRICTIONS

1.1. Permissions. During the term set out in the Order Form, Partner permits its Customers to: (i) only use Refinitiv Content for Customer Permitted Purposes (as defined below) and for no other purpose(s) (including any external commercial purposes).

1.2. Restrictions**.** Customer shall not transfer or access, any Refinitiv Content outside of the Territory without Partner's prior written consent, provided Partner obtains Refinitiv's prior written consent. Customer shall comply with the restrictions on use of Refinitiv Content under the Customer Agreement. Customer shall ensure that no Customer Users allow any other person to use his or her credentials to access the Authorised Product and the Refinitiv Content for any purpose, including to exercise any of the access and/or usage rights granted in the Customer Agreement.

1.3. Customer shall immediately notify the Partner if it becomes aware of any applicable legal or regulatory requirements that may impact the performance of the obligations and the exercise of the rights of Customer, Partner or Refinitiv under the Customer Agreement. Following receipt of such notice, Partner may at its discretion suspend the performance of any of its obligations under the Agreement if it reasonably believes that continued performance of such obligations may result in a breach of applicable legal or regulatory requirements by Partner. Any such suspension may continue until Partner is satisfied that the reason for the suspension is resolved in full. Partner will have no liability for not performing its suspended obligations during the period of suspension.

2. USE OF PERSONALLY IDENTIFIABLE INFORMATION

2.1. Customer will at all times comply with Data Protection Legislation in respect of its processing of Personally Identifiable Information.

2.2. Customer is a separate and distinct data controller of any Personally Identifiable Information it processes that originates from, or is derived from, the Refinitiv Content. In particular, Customer is responsible for giving appropriate transparency notices, obtaining any required consents or approvals (if any), responding to subject rights requests (other than as set out in Clause 2.4 below), carrying out any privacy by design, impact or other assessments required, and ensuring that any use of Personally Identifiable Information complies with Data Protection Legislation.

2.3. If the Refinitiv Content includes Personally Identifiable Information, the Customer shall provide a link or other form of signposting to the relevant Refinitiv privacy notice for that Refinitiv Content to affected individuals being screened in accordance with relevant laws. Link to Refinitiv World-Check Privacy Statement: https://www.refinitiv.com/en/products/world-check-kyc-screening/privacy-statement.

2.4. Refinitiv shall be responsible for dealing with any subject requests under Data Protection Legislation that relate solely to Personally Identifiable Information contained within World Check. In particular, Customer shall not provide subjects with raw copies of Refinitiv Content without Refinitiv's approval (such approval not to be unreasonably withheld).

2.5. Customer shall ensure that Customer Users receive privacy training and guidance in accordance with good industry practice.

2.6. Customer will provide reasonable assistance to enable Partner to understand how Personally Identifiable Information within Refinitiv Content is being processed from time to time (including so as to enable Refinitiv to complete its statutory records of data processing and any due diligence Refinitiv reasonably deems necessary to satisfy its obligations under applicable laws).

2.7. Customer will maintain and will require all third-party data processors it engages to maintain appropriate physical, technical and organisational measures to protect the Personally Identifiable Information within the Refinitiv Content against accidental, unauthorised or

unlawful destruction, loss, alteration, disclosure or access in accordance with good industry practice. Customer shall use all reasonable endeavours not to use the Refinitiv Content in such a way as to knowingly or negligently cause Refinitiv to breach its obligations under Data Protection Legislation.

2.8. [Not used]

2.9. Customer Users that are provided access to Refinitiv Content may redistribute Refinitiv Content to a government or regulatory authority solely to the extent specifically permitted by applicable law and if requested by such government or regulatory authority for the purposes of investigating the Customer's compliance with laws and regulations. Customer Users may redistribute Refinitiv Content to Customer's client's in accordance with Customer's Permitted Purpose.

3. SECURITY

3.1. Customer shall implement and maintain appropriate physical, technical and organisational measures designed to prevent security incidents that affect Refinitiv Content, including Personally Identifiable Information ("**Security Incidents**"). Such measures shall include: a) strict controls on access to Refinitiv Content by Customer's staff (including third party data processors) and on Customer's physical infrastructure; b) regular scanning and penetration testing to identify potential security vulnerabilities; and c) use of encryption (where appropriate).

3.2. Customer shall notify the Partner without undue delay (and in any event within 24 hours) of any actual or suspected Security Incident affecting Refinitiv Content. As part of that notification, Customer shall provide: (i) a description of the nature of the Security Incident, including the volume and type of Refinitiv Content affected and, if relevant, the categories and approximate number of individuals concerned; (ii) the likely consequences of the Security Incident; and (iii) a description of the measures taken or proposed to be taken to address the Security Incident including, where appropriate, measures to mitigate its possible adverse effects.

3.3. In the event of a Security Incident, Customer shall provide all reasonable assistance requested by the Partner and Refinitiv in relation to investigating, responding to, or mitigating the effects of the Security Incident, including in relation to making notifications to regulators and/or individuals.

3.4. Partner shall be entitled to conduct a security assurance exercise: (i) annually; and (ii) in connection with any Security Incident, to check that the Customer is and has been using Refinitiv Content in accordance with the Customer Agreement. This will not ordinarily necessitate Partner entering Customer premises. Customer will complete each such security assurance exercise promptly, honestly and in good faith and provide Partner with any further information and/or confirmations it may reasonably request to confirm that Customer is using the Refinitiv Content in accordance with the Customer Agreement. Security assurance exercises do not require Partner to see personally identifiable information and Partner shall comply with any reasonable security measures. If Customer fails to comply with this Clause 3.4, or Partner concludes (acting reasonably) from the information provided to it pursuant to this Clause 3.4 that Customer is not using the Refinitiv Content in accordance with this Schedule as incorporated in the Customer Agreement, this shall constitute a material breach of the Customer Agreement by Customer which permits Partner to terminate the Customer Agreement without cost upon 30 days' written notice.

3.5. Partner shall have the right to suspend Customer's access to Refinitiv Content immediately in the event of suspected misuse of Refinitiv Content or to prevent or mitigate the effects of a Security Incident or to identify or investigate a reasonably suspected Security Incident.

4. DISCLAIMERS

4.1. The Customer acknowledges and agree that:

a. the Refinitiv Content cannot be an exhaustive source of information and Customer should not rely solely upon the Refinitiv Content when making any decision to deal with any person or entity and that before making any such decision Customer should make independent checks of such person or entity to supplement and verify the information contained in the Refinitiv Content and/or the Authorised Product and their resulting suitability as a commercial counterparty;

b. Refinitiv Content cannot be incorporated into any product, service, tool, software or other mechanism designed to make automated decisions about an individual or that individual's personal or professional interests;

c. Refinitiv provides Refinitiv Content without giving any opinion or recommendation about any individual or entity named in same;

d. Refinitiv may include information in Refinitiv Content that relates to an entity or individual that bears the same name as other unconnected persons;

e. if the Refinitiv Content contains negative allegations about any person or entity, it should be assumed that such allegations are denied by them;

f. information in the Refinitiv Content is necessarily in summary form and should be read and used by Customers in context of the full details available in the underlying sources included in the Refinitiv Content;

g. the inclusion or exclusion of any person or entity in or from the Refinitiv Content should not solely be taken to draw any particular inference (negative or otherwise) about that person or entity, including as the result of the linking of that person or entity to any other person or entity identified in the Refinitiv Content. Customers should not assume that any person or entity identified in the Refinitiv Content has breached any law or sanction, and the parties agree that Refinitiv is not in a position to make such determinations. Refinitiv has no responsibility for the Refinitiv Content provided by third party databases or extracts. The Refinitiv Content or a Report may include or mention the following without limitation:

   (1) The "Iran Economic Interest" or "IEI" database, which contains content on persons or entities that have been reported in the public domain as having some direct or indirect economic interest in Iran or with Iran or a person connected to Iran;

   (2) The US SAM Exclusions Extract, which contains information on individuals and entities that are restricted or prohibited from engaging in contracts with the US Federal Government, as determined by the US Government in accordance with their own criteria and guidelines; and

   (3) Country Risk Ranking and Country Risk Ranking Reports which are provided as a guide to assist with determinations of jurisdictional risk in relation to the country in question. Any risk rankings and bandings generated using the Country Risk Ranking predefined or default weight sets represent Refinitiv's assessment of risk associated with that country based on available public domain information (which may be inaccurate), an underlying algorithm and Refinitiv's perception of risk and may not be appropriate for Customer's use. Customer must satisfy themselves that they understand Refinitiv's default settings and risk criteria and that such settings are appropriate and applicable for their level of risk appetite. Country Risk Ranking and Country Risk Ranking Reports do not in any way seek to assign a level of risk to individuals identified in Refinitiv Content and Customer may not use the Country Risk Ranking and Country Risk Ranking Reports to do this;

h. many persons are included in the Refinitiv Content solely because they hold or held prominent political or other positions or are connected to such individuals and no particular inference (negative or otherwise) should be drawn about such persons based on any such position;

i. while significant time and effort is invested by Refinitiv to ensure that the Refinitiv Content is kept up to date, Refinitiv cannot guarantee that information contained in them will remain up to date or will always be free of error (including inaccuracies);

j. Refinitiv makes no warranty or representation about, and disclaims all liability for, the accuracy, completeness or currency of any information from third party providers that forms part of the Refinitiv Content; and

k. Customers must make their own assessment of the relevance and applicability of any classification of individuals contained in the Refinitiv Content.

5. AUDIT

5.1 Customer shall allow Refinitiv the right to audit the Customer's compliance with the Customer Agreement in the event of an actual or suspected security breach that Refinitiv (acting reasonably) suspects is linked to the Customer's acts or omissions in connection with Refinitiv Content.

5.2 If Customer is accessing and using the Deployed Datafile, it shall also allow Refinitiv (without limiting Refinitiv's rights in clause 5.1) the right to audit the Customer's compliance with the Customer Agreement for any reason. Refinitiv will not audit more than once every 12 months pursuant to this clause 5.2 unless Refinitiv has cause to suspect, or an audit reveals, that Customer is non-compliant.

5.3 Refinitiv shall, when carrying out any audit, comply with Customer's reasonable security, health and safety, and confidentiality procedures that are provided to Refinitiv in advance in writing.

5.4 Customer authorises the Partner to provide a copy of the Customer Agreement to Refinitiv (with any pricing redacted) for Refinitiv to verify such agreement imposes appropriate restrictions on use and security of the Refinitiv Content.

6. TERMINATION AND DELETION OF REFINITIV CONTENT

6.1. Upon termination or expiry of the Customer Agreement, Customer shall (i) cease all use of the Refinitiv Content; (ii) promptly delete all Refinitiv Content (including any copies of the Deployed Datafile), however Customer is permitted to retain copies of its screening records containing Refinitiv Content to extent required by, and used only to comply with, law or regulation (iii) certify to Partner, in writing, that it has fully complied with this Clause 6.1.

DEFINITIONS

Authorised Product – a Partner product (which may be a tool, report or other item provided by Partner to Customers) which includes Refinitiv Content.

Customer – any customer of the Partner that receives Refinitiv Content under Customer Agreement.

Customer Agreement – the agreement between the Partner and Customer setting out the terms and conditions applicable to the Customer's access and use of Authorised Product.

Country Risk Ranking - a summary measure of a range of constituent information that might be considered to be associated with operational and locational risk.

Country Risk Ranking Report - an objective and customizable geopolitical risk index that models country risk for 247 countries and territories.

Customer Permitted Purposes –use of an Authorised Product by Customer Users for Customer as part of supporting the Customer's clients' compliance processes (as opposed to use for any external commercial purpose) to conduct due diligence and other screening activities that are necessary for reasons of substantial public interest on the basis of, or as authorised by applicable law."

Customer Users – individuals employed by a Customer who are permitted to access the Authorised Product in accordance with the relevant Customer Agreement.

Data Protection Legislation – legislation relating to an individual's right to privacy with respect to the processing of Personally Identifiable Information which is applicable to a Party from time to time.

Deployed Datafile – the Refinitiv Content where: (i) the Refinitiv Product is World-Check Datafile; and (ii) a deployed instance of the Authorised Product is held in the Customer's environment.

Partner – FRANKIE FINANCIAL PTY LTD (this shall include references to "Frankie Financial")

Personally Identifiable Information – any information that, alone or in combination with other information, can be used to identify, locate or contact an individual, including, without limitation, information constituting "personal data" as defined in the European Union's General Data Protection Regulation (2016/679).

Refinitiv – Refinitiv Limited, the provider of World Check

Refinitiv Content – the content in any Refinitiv Product that is made accessible to Customer under the Customer Agreement via the Authorised Product.

Refinitiv Product – any database, functionality, software or other product made available by Refinitiv to Partner pursuant to the agreement executed by Partner and Refinitiv for the provision of Refinitiv Content

Territory – APAC