KAJIMA PHILIPPINES INC.

KOA Group Invoice Fraud Prevention Measures
Established March 12, 2018

PURPOSE OF THE KOA GROUP INVOICE FRAUD PREVENTION MEASURES

This Invoice Fraud Prevention Measures for Kajima Overseas Asia Pte. Ltd. ("KOA") and its subsidiaries and affiliates which KOA can exercise significant and important influence onto is implemented pursuant to section (1)(8) of the KOA Group's Corporate Code of Conduct and section 10 of KOA Group's Code of Conduct for Information Security, and sets out the framework for protocols and measures to be established by each company within the KOA Group (each a "Company") and complied with by all employees.

I. MEASURES TO BE COMPLIED WITH BY A GROUP COMPANY AND EMPLOYEES

1. Creation of Profile for ongoing Suppliers and Vendors (for both cheque and bank transfer payments)

   (1) Creation of Vendor Profile (for new Vendors) and Due diligence on Vendor:

   (i) Prior to commencing any transaction with a supplier or vendor (each a "Vendor"), a Vendor's legal existence and credibility shall be verified via information obtained from the original registration application form provided by the Company, to be completed by the Vendor (the "Vendor Registration Form"), together with other information and data on the Vendor [to be furnished together with the Vendor Registration Form], such as but not limited to its tax identification number, other publicly registered and disclosed information, company profile (searches at public government agencies), financial reports, bank guarantees, credit check information, etc.

   (ii) Once a Vendor is approved via the above review procedure, a secure record of the relevant information and profile of the Vendor, such as but not limited to its company name, representative name, bank account, etc. (the "Vendor Profile") shall be maintained by the Company. No changes or amendments shall be made to a Vendor Profile save in accordance with section 1.(2) below.

   (iii) The above review procedure and approvals given thereunder shall be done by more than one person, which shall in any event include the person in charge of financials and administration of the company (such person referred to as the "CFO", and together with all persons appointed hereunder to undertake the approval process, the "Authorized Persons").

   (iv) All employees shall abide at all times with any further detailed procedures, instructions and measures that the Company may issue, implement or notify employees of from time to time, in connection with the above.

(2) Change or Amendment to Existing Vendor Profile:

(i) In the event a Vendor requests any change or amendment to its Vendor Profile, such Vendor shall always be required to submit the original registration change application provided by the Company (a "Vendor Registration Change Form"), together with the original or copies of all supporting information and documents (such as but not limited to publicly registered information, bank account statements, etc.), to be reviewed in the same manner as set out in section (1)(i) above.

(ii) No person may approve or accept any change or amendment to the Vendor Profile based on requests given by such Vendor over the phone, e-mail or any other electronic communication.

(iii) The above review procedure and approval given thereunder shall also be done by more than one person, which shall in any event include the Authorized Persons and the CFO.

2. Payment Approval Procedures and Guidelines

(1) Procedure

(i) The Company shall commence payment approval procedures only after receipt of the original invoice and payment request from the Vendor. Invoices sent by e-mail, fax or other electronic methods shall not be accepted.

(ii) After receipt of the original invoice, the invoice must be checked against the payment terms under the applicable agreement or contract with the relevant Vendor (each a "Vendor Contract"), and in the event the invoice is not payable thereunder in accordance with the stipulated timeframe set out in the Vendor Contract within a reasonable time frame, the Company shall not commence the payment approval procedures.

(iii) In the event any information set out in the original invoice differs from the Vendor Profile (e.g. bank account details), or if any other changes to standard contents thereunder are detected, the Vendor shall be requested to submit supporting documents to substantiate such differences and changes made, to the satisfaction of the Company.

(iv) Payment approval procedures shall be done by more than one people, which shall in any event include both the person in charge of the Company (the "MD") and CFO.

(v) In the event of absence of or inability to perform the above approval procedures by any of the appointed approvers, those approvers shall each designate another person to perform such duty to approve on behalf of them, to satisfy requirement of number of approvers for this payment approval procedure.

(2) Variation to Payment Approval Procedure

Any payments not in accordance with the payment schedule in the applicable Vendor Contract shall still be subject to the same payment approval procedures in section (2)(a) above, and shall be processed based on the original invoice and payment request from the relevant Vendor. However, in the event such off-scheduled payment is deemed to be requested under unavoidable circumstance from a reasonable point of view, and subject to the CFO confirming directly the background of the payment requestee and such unavoidable circumstance with a representative of the Vendor of appropriate seniority (for example only, such representative being the project manager, director, etc.), the Company may commence the payment approval procedure prior to receipt of the original payment request and invoice, however only after receipt of a pdf copy of the payment request and invoice via e-mail.

(3) Blanket Prohibition

Transfer of monies to a bank account in any country other than to a bank account in the country where the Vendor is incorporated or established and undertakes its business is, in principal, prohibited.

3. Reporting Requirements

(1) The Company shall forthwith report the occurrence of any incident (including those attempted) constituting an “Applicable Event” to the International Division of KC, notwithstanding the amount involved therein.

Please refer to the Schedule (Reporting Requirements) to the KOA Group Invoice Fraud Prevention Measures for what constitutes an “Applicable Event”.

II. ISSUES FOR THE COMPANY TO CONSIDER WHEN IMPLEMENTING THE KOA GROUP INVOICE FRAUD PREVENTION MEASURES

1. Establishment of robust system with appropriate checks and balances

   (1) The Company shall create and establish a system that contain the accurate details of the Vendor after completing the due diligence process in Section (I)(1)(a), which should include designated account numbers, name of account holders (which should in most cases be the name of the Vendor or one of the companies in its group) and/or name of cheque payees from the Vendor Profile. The Company shall maintain and confirm operation of such system periodically.

   (2) With respect to import/export transactions undertaken by the Company, to consider instituting regulations requiring payment by letter of credits (L/C) in lieu of bank transfers or cheque payments.

   (3) Appoint more than one people, which shall in any event include both the MD and CFO, as persons who hold the final approval and execution right for transferring money online or who hold signatory rights to sign-off on cheques. However, the person who actually executes the final step to transfer money online or signs the cheque may be, from time to time, a single person, due to the fact and understanding that such payment has been approved by more than one persons based on the established payment approval procedure.

   (4) Rules and regulations on accounting system access and approval rights shall be established, and such rights be given to more than one person (which shall include the CFO at all times other than the accounting system access rights).

   (5) Rules and regulation on access and approval rights with respect to online money transfers shall be established, and such rights be given to more than one people (which shall include the CFO and MD at all times).

2. Education and training

   (1) The following codes and group measures shall respectively and collectively be explained to newly hired employees concerned, and any amendments, changes or updates thereto shall be disseminated to all employees and posted on the company intranet: KOA Group's Corporate Code of Conduct; Code of Conduct for Information Security; and KOA Group's Invoice Fraud Prevention Measures.

(2) The Company should consider requiring all employees concerned to sign a compliance confirmation, acknowledging, and accepting, and confirming ongoing compliance with the codes of conduct listed in paragraph (i) above, on an annual basis.

(3) The company shall conduct timely alerts conduct periodic training for and educate all its employees on the risks of potential fraud involving payment approvals online.

3. Measures against internet infrastructure risks

(1) The Company shall establish, implement and maintain rules and regulation to manage company provided e-mail accounts.

(2) The Company should consider introducing security software or other methods which automatically warns and alerts recipients when receiving e-mails from free e-mail accounts/domains. Accounting staff in particular shall have their e-mail software (such as Outlook) set-up, so that they receive warnings and alerts in the event and when they receive e- mails from or send e-mails to free e-mail accounts/domains. Such set-up is also recommended for staffs in other departments/divisions, so as far as it does not interfere with or decrease efficiency of their scope of work.

(3) With respect to transferring and exchanging electronic files, each employee shall password protect such file at all times if being transferred or sent via e-mail, and for alternative methods to send or saving such file, use servers or cloud services which allow control over user access rights, and also provide an acceptable level of security.