Bottomline Hosted Services Master Customer Agreement: Mandatory Terms

These Mandatory Terms shall apply and supplement the Terms and Conditions as further described below. Unless otherwise defined below, capitalised terms used in these Mandatory Terms shall have the same meanings as the (i) Terms and Conditions, (ii) Product Schedules, and (iii) Annexes.

Bottomline reserves the right to amend these Mandatory Terms from time-to-time as may be required due to changes in its contracts with PNPs, suppliers and subcontractors by posting the amended Mandatory Terms on www.bottomline.com/uk/product-terms-conditions/swiss-mandatory-terms (the "**Mandatory Amendments**"). The Mandatory Amendments shall be deemed accepted by the Customer through the Customer's continued use of Bottomline Solutions after the Mandatory Amendments have been posted.

1. SWIFT

Insofar as any Bottomline Solutions provided to the Customer includes connectivity to the SWIFT network, this Clause 1 shall apply.

1.1 The Customer agrees:

(a) to have in place a current agreement between SWIFT and the Customer during the term of the Agreement (for the avoidance of doubt failure to maintain such an agreement will be deemed a material breach of the Agreement);

(b) be responsible and liable for all applicable SWIFT membership charges and SWIFT traffic fees in accordance with its SWIFT user agreement;

(c) to comply with the policies stipulated by SWIFT for SWIFT users whether contained in SWIFT terms and conditions published from time to time or otherwise, and shall notify Bottomline and SWIFT of any non-compliance with such rules and regulations and/or breach of any such conditions; and

(d) to treat as confidential, any information relating to Bottomline Solutions or SWIFT operations (including but not limited to the contents of messages passing through the Subscription Services), SWIFT technical documentation, SWIFT security tokens and SWIFT network information.

1.2 The Customer undertakes to ensure that the Customer, its employees or any authorised third party shall not abuse or make any fraudulent use of the SWIFT messaging service, which may include without limitation:

(a) any illegal or unlawful activity;

(b) the collection, development or distribution of malicious code;

(c) hacking or cracking activities;

(d) the circumvention of copy-protection mechanisms; and

(e) assisting or allowing any third person to do any of the foregoing.

1.3 The Customer acknowledges and accepts that SWIFT periodically amends its operational requirements applicable to service bureaux providing shared infrastructure services pursuant to the SWIFT Shared Infrastructure Programme or any successor thereto ("**SIP Requirements**"), and that such amendments may include without limitation certain provisions to be inserted into the service bureau's client contracts. Accordingly, in order to facilitate compliance with SWIFT's requirements, the parties hereby agree that Bottomline shall document and publish such provisions in an addendum to the Agreement, which shall be deemed to be incorporated automatically into the Agreement with effect from the date of publication on Bottomline's client portal or, if present, the date expressly stated in the applicable addendum, and that each new version of the said addendum shall replace all of its previous versions with effect from that date. Bottomline may only include in the said addendum such provisions as are required to comply with the SIP Requirements, which do not materially degrade the service levels, and which do not impose additional charges on the Customer. Bottomline reserves the right to introduce additional charges for new functional or operational requirements imposed by SWIFT to the extent these are outside the scope of the then current Bottomline Solutions, and these shall be handled via the Order Form mechanism as for other changes with commercial impact.

1.4 With regard to SWIFT security functions:

(a) the Customer's own personnel shall continue to be the SWIFT registered Security Officers ("**SO**"). The Customer shall notify Bottomline of its designated Security Officers with full contact details;

(b) the Customer shall delegate the control and operation of the Customer's SO private PKI keys to Bottomline for the purpose of managing the Customer's certificates and for providing connectivity to the Subscription Services;

(c) the Customer's private PKI keys and certificates will be held securely on the Bottomline Infrastructure in accordance with SWIFT best practice;

(d) the Customer's private PKI keys and certificates will be accessible only to authorised Bottomline personnel. The Customer may request, at any time, a list of the Bottomline authorised personnel that can access the Customer's private PKI keys and certificates;

(e) any disabling, revoking, creation, or usage of the Customer's private PKI keys and certificates; and changes in the user profile (defined in the context of Role Based Access Control (RBAC) by Bottomline) will be performed according to strict procedures defined in Bottomline's SWIFT Bureau Cryptographic Key Management Procedure ("**SBCKMP**");

(f) the initiation, modification, and termination of cryptographic secrets and arrangements by Bottomline will be performed according to strict procedures defined in the SBCKMP; and

(g) The Customer may request an audit trail of all actions carried out by Bottomline in relation to the Customer's private PKI keys and certificates.