RISK SERVICE ACCEPTABLE USE POLICY (AUP)

This Risk Service AUP applies to the Customer's use of the Risk Services, and these obligations apply in addition to any obligations set out in the PPS Agreement (the "**Agreement**"). Any capitalized terms herein shall have the meaning set out in the Risk Service Contract Addendum (Telesign EULA). In this AUP, "Client" and "Customer" shall have the same meaning. PLEASE NOTE THAT THIS RISK SERVICE AUP COMPRISES TELESIGN FLOWDOWN TERMS AND AS SUCH IS NON-NEGOTIABLE VIS-A-VIS CUSTOMER AND PCI PAL.

You agree to comply with the terms and conditions set out in this Risk Service AUP as follows:

1. **Content Standards**: Any content stored or sent via the Risk Services shall comply with the following standards:
    a. All content must include identification of the Customer including but not limited to Customer name, brand name, company, or brand identity.
    b. No promotional or marketing content may be sent unless the end user has consented to receive such content via specific opt-in acknowledgment.
    c. All promotional and marketing content must contain a specific opt-out mechanism in compliance with Applicable Laws.
    d. All content must comply with Applicable Laws and any requirements set out in any applicable industry or relevant telecommunications operators and/or carrier's ("**Carrier**") code of conduct, guidelines or similar requirement. Such industry guidelines may include but not limited to the Mobile Marketing Association's Code of Conduct, the Consumer Best Practices Guideline, the CTIA Short Code Monitoring Handbook, the then-current requirements of the US Common Short Code Administrator and other similar guidelines and standards established for mobile marketing and messaging in applicable countries such as CWTA (Canada) and Phone pay plus (United Kingdom).
    e. Content must not be defamatory, slanderous or libelous.
    f. Content must not contain any information that would require PCI Pal to comply with any financial regulations or the Payment Card Industry Data Security Standards.
    g. Content must not contain any personal health information as defined in the Health Insurance Portability and Accountability Act of 1996, including any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.
    h. Content must not violate any system or network security of PCI Pal, an end user or third party.
    i. Content must not be illegal, unauthorized, prohibited, fraudulent, deceptive, inaccurate or misleading (including, without limitation, by using a false identity or forged address or telephone number).
    j. Content must not contain pornography, nudity, sexual activity or similar adult-themed materials.
    k. Content must not contain information in which the failure or delay of Risk Services could lead to death, personal injury, physical property damage or environmental damage.
    l. Content must not contain any viruses, worms, trap doors, back doors, timers, clocks, counter or other limiting routines, instructions or designs, or contain any unauthorized code.

m. The Customer shall be liable to pay any fines or penalties levied by a Carrier, and to fulfil any indemnification obligation owed by PCI Pal or any subcontractor to any Carrier, as a result of Customer's noncompliance with the Content Standards set forth herein.

2. **SPAM Policy:**

a. Client must not use the Risk Services to send any message without the prior express consent of the recipient, or any message sent after the recipient has expressly withdrawn its consent to receive such message, or otherwise for fraudulent purposes ("SPAM"). SPAM may include (but is not limited to) the sending of bulk SMS and RCS messages to a list of telephone numbers without prior consent from the holders of such telephone numbers, or the sending of marketing messages to end users that have not expressly consented to receive such messages. Telesign's decision as to whether Client is using the Risk Services to send SPAM shall be final.

b. Client must comply with all anti-SPAM laws and regulations, including, but not limited to, the CAN-SPAM Act of 2003, the Telephone Consumer Protection Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the Children's Online Privacy Protection Act and the Do-Not-Call Implementation Act (or any similar or analogous anti-spam, data protection, or privacy statutes or regulations in any other jurisdiction).

c. If PCI Pal suspects the Customer's account is being used to send SPAM:

i. PCI Pal may without prior notice immediately suspend some or all of the Risk Services.

ii. upon notice from PCI Pal, the Customer must immediately take all necessary action to cease such SPAM, including suspending or terminating any end user's account.

iii. PCI Pal and the Customer shall cooperate to cease the sending of SPAM, including sharing end user details where necessary to identify the sender of SPAM.

iv. PCI Pal may, without prior notice to the Customer, notify Carriers or other required-to-be-informed third parties.

d. If the Customer suspects that its account is being used to send SPAM, the Customer must immediately take all necessary action to cease such SPAM, including suspending or terminating any end user account, and cooperate with PCI Pal to cease such SPAM.

e. The Customer is responsible for obtaining all necessary consent to enable lawful sending of messages to end users. PCI Pal may delay or suspend the delivery of any messages suspected to be SPAM until the Customer has provided PCI Pal with evidence, reasonably satisfactory to PCI Pal, that all necessary consent has been obtained.

f. Client shall be liable to pay any fines or penalties levied by a government or regulatory body, and to fulfil any indemnification obligation owed by PCI Pal or any subcontractor to any Carrier, as a result of SPAM being sent via the Risk Services.

3**. Generally applicable use restrictions:** The Customer shall:

a. not use the Risk Services or the Licensed Data, in part or in whole, for any purpose, or in any way prohibited by any Applicable Laws, or in any manner that may disable, impair, damage or interfere with any of PCI Pal or its subcontractors hardware, software applications, system or network security, intellectual property rights, the Risk Services, or any other clients or users of the Risk Services;

b. not copy, reverse engineer, modify, create derivative works of, distribute, sell, resell, assign, pledge, sublicense, lease, loan, rent, share, timeshare, grant a security interest, deliver, or otherwise transfer, directly or indirectly, any portion of or rights in the Risk Services, Licensed Data, or any of PCI Pal or its

subcontractor's software (including source code thereto), computer systems or networks, or otherwise make available the Licensed Data (or any portion thereof) to third parties (except to the extent expressly set forth in this Contract Addendum);

c. maintain the confidentiality of the Customer's username and password (if any is provided) utilized to access the Risk Services and to keep secure PCI Pal or its subcontractor's API key. The Customer bears the sole responsibility for any requests sent from its account and/or via the PCI Pal API and any and all usage of the Risk Services via its account and any password and/or via the PCI Pal API by the Customer, any end user or any third party, whether with or without the Customer's permission (unless such usage results from any negligence of PCI Pal or its subcontractor). Any such usage shall be deemed to be the Customer's use of the Risk Services. The Customer must notify PCI Pal immediately upon any disclosure of the Customer's password or any unauthorized use of the Customer's account or if the PCI Pal API key have been compromised;

d. not use the Risk Services or the Licensed Data for the purpose(s) of solely automated decision-making producing legal effects or similarly affecting the end users, such as:

    i. cancellation of a contract;

    ii. entitlement to or denial of a particular social benefit granted by law, such as child or housing benefit;

    iii. refused admission to a country or denial of citizenship;

    iv. decisions that affect someone's financial circumstances, such as their eligibility to credit (i.e.: assessing creditworthiness);

    v. decisions that affect end users' access to health services;

    vi. decisions that deny end users' an employment opportunity;

    vii. decisions that affect end users' access to education, for example university admissions;

    viii. decisions that affect end users' access to housing;

    ix. decisions that affect end users' access to insurance;

    x. decisions that affect end users' access to criminal justice; or

    xi. decisions that affect end users' access to basic necessities, or essential goods or services;

g. provide all end users' with any disclosure, notice, or explanation required by Applicable Laws and/or providers concerning the Customer's use of the Risk Services, and obtain, maintain and secure any necessary consent and authorizations from end users' that may be required by Applicable Laws and/or providers in order to authorize PCI Pal and its subcontractor's provision of the Risk Services, or otherwise ensure a lawful basis for PCI Pal and its subcontractor's provision of the Risk Services and processing of Risk Services Customer Data. If requested by PCI Pal, provide satisfactory evidence of its collection and continued receipt of end user consent for the provision of the Risk Services. Immediately provide any updates to notices, consents and authorizations to PCI Pal. Any records required to be kept to meet these obligations shall be retained by the Customer for at least 12 months or such other period as may be indicated in the applicable agreement;

h. provide any information relating to the Customer's use of the Risk Services reasonably requested by PCI Pal;

i. comply with the Fair Credit Reporting Act ("**FCRA**"), to the extent it is applicable, including without limitation, if information provided by PCI Pal will be used for employment decisions, certify to PCI Pal inwriting, that the Customer: (1) notified the applicant or employee and got their permission to get a consumer report; (2) complied with all of the FCRA requirements;

and (3) will not discriminate against the applicant or employee or otherwise misuse the information, as provided by any applicable federal or state equal opportunity laws or regulations; and

j. comply with the Gramm-Leach-Bliley Act, to the extent it is applicable.

4. **Licensed Data:** In relation to Risk Services in which PCI Pal provides Licensed Data, the Customer shall:

    a. only use Licensed Data for purposes in respect of which the end user to whom such Licensed Data relates has expressly consented;

    b. not use the Risk Services to collect or process information about any end user without such end user's prior consent;

    c. use the Licensed Data for one-time use only, and shall not cache the Licensed Data for the purpose of reuse by the Customer;

    d. not use the Licensed Data, in part or in whole, in conjunction with any data mining or to create or store in any form an archive of the Licensed Data, or to construct products or services that may compete with the Risk Services; and

    e. delete all Licensed Data within 30 days of delivery by PCI Pal, or immediately on termination of the PPS Agreement or the Contract Addendum or on request from PCI Pal;

    f. not store Licensed Data received from Austria, Spain, or France outside of the EU; and

    g. when using Risk Services in China and Singapore, expressly ask for end user consent.