1. The Issuing Solution(s)

1.1. The Customer will:

1.1.1. regularly monitor the Account(s) to ensure no unauthorized Payment Transactions have occurred and to validate that the Account(s) is active or otherwise, should have been terminated for inactivity in accordance with the Issuing Agreement;

1.1.2. ensure that the Customer's systems are compatible, suitable and in good working order for the use with the Issuing Solution(s);

1.1.3. secure any equipment or telecommunications lines and connections that may be necessary for Customer to use or connect to the Issuing Solution(s);

1.1.4. not interfere with, disrupt, or cause any damage to other users of Outpayce's services, including but not limited to, the Issuing Solution(s);

1.1.5. update Customer's information technology, software and equipment in order to access the Issuing Solution(s);

1.1.6. access the Issuing Solution(s) using the authentication procedures mandated by Outpayce, as required from time to time;

1.1.7. not access all or part of the Issuing Solution(s) to build a product or service which competes with the Issuing Solution(s);

1.1.8. not access the Issuing Solution(s) via third party products (e.g., robotic tools) that are not expressly authorized by Outpayce in writing;

1.1.9. not directly, indirectly, manually or through robotic devices access or use (or allow any third party to access or use) the Issuing Solution(s) for (i) making Payment Transactions which are speculative, fictitious, duplicative, improper or fraudulent, or made solely to achieve minimum targets, minimum usage requirements or to otherwise obtain improper economic advantages; (ii) whether knowingly or not, transmitting or disseminating any virus, trojan or other malicious, harmful or disabling data, work, code or program; or (iii) interfering with, disrupting or attempting to gain unauthorized access to any computer, system or network; and

1.1.10. not use any automatic device, software, application, program, browser plugins, algorithm, whether integrated in a browser or otherwise, or methodology having similar processes or functionality, or any manual process, to monitor, perform any Payment Transactions, frame, modify, add content or copy any part of the Issuing Solution(s).

2. Authorized Users

2.1. The Customer will:

2.1.1. license, transfer, assign, distribute, display, disclose or otherwise make the Issuing Solution(s) available to any third party except Authorized Users or as expressly permitted under the Issuing Agreement or Applicable Law(s);

2.1.2. provide Outpayce with unique and non-transferable corporate e-mail addresses for each Authorized User and acknowledge that the security and use of the Customer's login credentials and passwords for the Issuing Solution(s) remain the Customer's sole responsibility;

2.1.3. establish robust, personalized security credentials for each Issuing Solution(s), ensuring that access credentials are not shared among multiple individuals and that the same password is not reused across different products or tools;

2.1.4. always store such security credentials safely and securely and implement and maintain appropriate administrative procedures to ensure that such access credentials are accessible only to the Authorized User;

2.1.5. ensure that all Authorized Users access the Issuing Solution(s) using strong authentication protocols, including mandatory two-factor authentication, in accordance with Industry Standards and security requirements under Applicable Law(s) and Guidelines;

2.1.6. employ all physical, administrative and technical controls, screening and security procedures and other safeguards necessary to securely administer the distribution and use of all access credentials and prevent any unauthorized access to, or use of, the Issuing Solution(s);

2.1.7. inform Outpayce, without undue delay, if the accesses granted to each Authorized User are insufficient to perform their function or do not reflect the actual usage; and

2.1.8. inform Outpayce, without undue delay, if the access to the Issuing Solution(s) of any Authorized User should be disabled (e.g., if an Authorized User leaves the company).

3. Reporting to Outpayce

3.1. The Customer will immediately cease the use of the Issuing Solution(s) and contact Outpayce, within twenty-four (24) hours of becoming aware, by email (b2bpayments.support@outpayce.com) or through any available channel, as may be updated from time to time. Full incident details will be provided to Outpayce within forty-eight (48) hours of the initial report. Reportable events include:

3.1.1. unauthorized use of, or access to, the Issuing Solution(s) or any suspicion thereof;

3.1.2. theft, lost or compromise of the Card(s) (or Card(s)'s details), or of the personalized security credentials, or any suspicion thereof;

3.1.3. unauthorized Payment Transactions or any suspicion thereof; and/or

3.1.4. incorrect or defective Payment Transactions and any non-agreed charges levied upon the Customer as a result, and/or any other security concerns regarding the Issuing Solution(s).

4. Data security and PCI DSS

4.1. Each Party will maintain standard environmental, safety and facility procedures, data security and back-up procedures and other safeguards, in accordance with generally accepted industry standards, against the destruction, loss, unauthorized use or alteration of (i) with respect to Outpayce, Outpayce Data; or (ii) with respect to the Customer, the Customer Data.

4.2. The Customer acknowledges and agrees that the environment in which the Issuing Solution(s) are used must be secure. Accordingly, the Customer must (and must ensure that any subcontractor or other Third Party Providers providing information technology services on its behalf):

4.2.1. implement and maintain active firewalls to limit and control incoming and outgoing traffic on the Customer's client computer systems;

4.2.2. implement and maintain active and regularly updated anti-virus and anti-malware tools on all computers;

4.2.3. only use supported, up-to-date and patched versions of application software, operating systems and infrastructure components, ensuring that all security updates are applied promptly; and

4.2.4. conduct security awareness training sessions for all Authorized Users in accordance with industry best practices and PCI DSS. At a minimum, these training courses will cover:

(i) identification and prevention of phishing, social engineering, and other common cyber threats;

(ii) proper handling and protection of access credentials, cardholder data, and other sensitive information; and

(iii) procedures for promptly reporting suspected security incidents or breaches.

Such training courses will be conducted during onboarding and at least annually thereafter, or more frequently as required by changes in Applicable Law(s), PCI DSS, Industry Mandates or Guidelines. The Customer will maintain verifiable records of the training courses and provide Outpayce with evidence of completion upon request.

4.3. In no event will Outpayce be liable for any loss or damage to Customer resulting from or relating to Cyber-Crimes affecting the Issuing Solution(s), networks or the internet, illegal hacking, (distributed) denial of service attacks, unauthorized use to or interference with data, identity theft, phishing, software and media piracy, website vandalism, release of viruses and worms, invasion of privacy and cyber-spying.

4.4. Outpayce reserves the right, upon reasonable notice, to request documentation or other evidence of the Customer's compliance with its security obligations under the Issuing Agreement, including but not limited to, controls implemented by any Third Party Providers. The Customer will provide such information in a timely manner and cooperate in good faith with any related inquiries.

4.5. Outpayce and the Customer are each responsible for the security of cardholder data that are stored or processed on or transmitted through their respective systems and agree to collaborate to maintain such security to enable Outpayce and its Affiliates to certify annually to the Payment Card Industry Data Security Standards, as published and mandated by the PCI Security Standards Council at the time of certification, with respect to the storage, transmission or processing of cardholder data.