**Service Level Agreement – PTX® Hosted Services**

This service level agreement ("SLA") applies to the PTX Subscription Services hosted by Service Provider (Bottomline) ("Hosted Services"). By subscribing to the Hosted Services, through an Order Agreement, or otherwise using such services, Customer agrees to be bound by the terms of the reference contract stated in the applicable Order Agreement ("Agreement"), this SLA, and the applicable Order Agreement(s).

Capitalised terms not defined in this SLA have the meaning given to them in the Agreement. This SLA applies only to services to which Customer has subscribed.

1. **Third Party Providers**. Service Provider may contract with third party providers to deliver the Hosted Services, or a portion thereof. Customer acknowledges and agrees that Service Provider's websites, dashboards, or portals may contain references (e.g., name, logo or brand) to such third-party service providers, which references may be required by law or contract. Service Provider third-party providers have no logical access to any Customer data.

2. **Datacentres.** Hosted Services use two third party datacentres - a Production datacentre and a Disaster Recovery datacentre. Service Provider reserves the right to relocate its data centre locations upon written notification to Customer. The Production and Disaster Recovery datacentres are always separately located and kilometres apart.

3. **Operating Environments.** Service Provider is responsible for the operation, control and maintenance of the Hosted Services environments, including the hardware and software equipment under the responsibility of and managed by Service Provider. The infrastructure includes access to three separate environments: Production environment, Disaster Recovery environment and Test environment. Service Provider commits to service levels for the Production and Disaster Recovery environments only. Test environments are out of scope for the service levels described in this document.

4. **Infrastructure.** Customer is fully responsible for the entirety of its own infrastructure in use at Customer's site. Service Provider takes full responsibility for the entirety of the Hosted Services infrastructure within its perimeter of control, except any Customer component (e.g. VPN tunnel, customer internet connectivity, customer router etc.). Service Provider reserves the right to upgrade, at its sole discretion, the Hosted Services infrastructure, environments and processes to ensure service efficiency and data protection in line with capacity management, compliance regulations and good industry practice.

5. **Security.** Service Provider has a Chief Information Security (CISO) team dedicated to the security of Service Provider services and solutions and the Hosted Services are operated exclusively in accordance with Service Provider IT security policies.

   **Security Controls.** The Hosted Services environment is protected using a combination of security controls such as boundary protection, use of certified and supported software, a security Incident policy (including ownership, process, communication, escalation and tracking), penetration testing, vulnerability scanning, intrusion detection and malware protection. Data flows between Customer and the Hosted Services are secured using recognised industry standard encryption algorithms. The Hosted Services implements logical separation of customer data so that each Customer only has access to its own information.

   **Secure Use.** Customer undertakes to take all appropriate technical and organisational security measures in accordance with good industry practice to protect against any abuse or fraudulent use of the Hosted Services, including but not limited to any illegal or unlawful activity; the collection, development or distribution of malicious code; hacking or cracking activities; the circumvention of copy-protection mechanisms; assisting or allowing any third person to do any of the foregoing.

   **Secure Access**. Service Provider manages employee logical and physical access to the Hosted Services to ensure that access is restricted to authorised personnel only in accordance with their role and that access is monitored and controlled. Customer is responsible for its own user administration for the Hosted Services (unless an applicable Order Agreement states that Customer has delegated this responsibility to Service Provider) which includes controlling Customer's end user access and authorisation. Service Provider employee access to the Hosted Services requires a mandatory secondary authentication (multi-factor authentication) after password control; and Customer end user access to Hosted Services may require a mandatory secondary authentication (multi-factor authentication) after password control for some elements of the Hosted Services. Customer remains fully responsible for employing the password requirements defined by the Hosted Services (such as controls on password length, character content, character repetition, sequence repetition, frequency of password change and number of allowed unsuccessful login attempts) and multi-factor authentication (mandatory secondary authentication after password control) to ensure secure access to the Hosted Services.

   **Personnel Vetting and Training.** Service Provider maintains a screening policy regarding Hosted Services employees, including systematic checks on criminal and financial records. Service Provider ensures that all Service Provider personnel follow a mandatory annual security awareness training programme.

6. **Hosted Services Availability**. The Company shall use all reasonable endeavours to make the Subscription Services available twenty-four (24) hours a day, seven (7) days a week exclusive of the following:

(i) in respect of planned system enhancements, upgrades, updates and preventative maintenance, which shall be notified in advance via in service messaging (UK time zone):

a. for PTX Connect and PTX Invoice Automation between 07:30 – 09:00 hours on Saturday, 00:00 – 08:00 hours on Sunday and 06:30 - 07:30 hours on Tuesday and Thursday; and

b. for all other PTX services between 00:00 – 08:00 hours on Saturday and Sunday and 04:00 – 07:30 hours on Tuesday and Thursday; and

(ii) in respect of unplanned system maintenance for essential or emergency work to maintain availability and/or security of the Subscription Services, which will be notified in advance wherever reasonably possible.

**Bacs Submission**. Where the Customer has acquired "PTX Bacs Indirect Submission" and/or "PTX FPS Indirect Submission" as specified in an Order Agreement, then related Transactions received from the Customer for same day submission to Bacs via the Subscription Services must be received by the Company no later than 21.55pm each weekday, excluding UK public holidays. Bacs Input reports that such Transactions have been received by Bacs should be available to be downloaded by Customer directly from the Bacs Payment Services website. The Customer is responsible for downloading and actioning any Bacs reports (including but not limited to: AWACS, ARUCS, ARUDD, ADDACS, DDIC, AUDDIS, Input, Withdrawal and Arrival reports) from the Bacs Payment Services website. The Company accepts no liability for the content or availability of such reports, or the Bacs network.

**Cancellation of a Transaction**. Where the Customer wishes to cancel a Transaction after submission to Bottomline, the Customer must give notice via the telephone number specified in clause 8 below, no later than 4pm on the day that the Transaction was submitted to Bottomline. Bottomline will then use all reasonable endeavours to cancel the transaction via the Customer's bank. To cancel a Transaction after 4pm the Customer must contact its sponsoring bank directly.

7. **Service Desk Support**. The Service Provider will use its reasonable endeavours to respond to Incidents in accordance with the prioritisation and timelines set out in clauses 11 and 12 below. All support for resolution of Incidents will be provided via the Customer Care Portal (or where this is not possible, by telephone). Resolution of Incidents will be confirmed via e-mail. Support provided within the Subscription Services fee does not include on-site services, change requests or training. These services are available at additional cost and should still be directed via the Support Centre. Bottomline shall provide support for the current and one prior version of the Software only.

8. **Contacts & Operating Times**

<table>
<tr><th>Contact Method</th><th>Subscription Service</th><th>Operating Hours</th><th>Time Zone</th></tr>
<tr><td rowspan="2">Customer Care Portal - http://www.bottomline.com/uk/support-services/contact-support; or<br><br>Phone: +44 (0)1189 258 250</td><td>PTX Bacs<br><br>PTX DDM<br><br>PTX FPS<br><br>PTX Pay Direct</td><td>08:00-22:30 Monday - Friday (excluding UK Public holidays)</td><td rowspan="3">UK</td></tr>
<tr><td>All other PTX</td><td>08:30-17:00 Monday - Friday (excluding UK Public holidays)</td></tr>
<tr><td>Phone: +44 (0)333 016 2175</td><td>All PTX - Priority 1 24/7 Incidents (where specified in an Order Agreement)</td><td>24 hours a day, 7 days a week</td></tr>
</table>

Customer will ensure that Customer personnel reporting Incidents are reasonably trained in and conversant with the Subscription Services.

9. **Incident Reporting.** All Incidents must be reported via the Customer Care Portal and only by phone where this is not possible. The Customer has the ability to prioritise the Incident based on the Incident Priority Criteria in accordance with section 12 below. Where an Incident has been incorrectly prioritised, the Company may acting reasonably amend the priority. Once the Incident has been submitted the Customer will be allocated an Incident reference number and the Incident is despatched to the Support Centre.

10. **Escalation Route.** All support Incidents should be raised and where necessary escalated through the Enterprise Self Service Portal.

11. **Incident Priority Criteria.** All Incidents will be classified upon receipt as one of the following Priority levels, dependent upon the impact and scope of the Incident on the Customer's business.

    (i) Priority 1 – Incidents that prevent live payments or debits being processed.

    (ii) Priority 2 - Incidents that prevent notification or updating of systems but do not prevent payments processing including returns data, fax notifications and email notifications of outgoing orders and remittances.

    (iii) Priority 3 – Incidents relating to non-production environments including Customer test environments, cosmetic failures and change requests, incorrect information appearing on documents and noncritical Equipment issues.

12. **Incident response times.** The Incident response times specified herein by Incident Priority level are guidelines only and commence from when an Incident is logged and an Incident reference number is given to the Customer.

    (i) For Priority 1 - Incidents placed into the Support queue will be acknowledged by the Support Team within 1 hour. Customer will be updated with a plan for resolution within 1 hour thereafter if the Incident has not already been resolved. Where Priority 1 24/7 Support is specified in an Order Agreement then Incidents placed into the Support queue via the telephone number shown in clause 3 above will be acknowledged by the Support Team within 15 minutes; and where an Incident is categorised as a Priority 1 Customer will be updated on an hourly basis until a work around or plan for resolution is achieved.

    (ii) For Priority 2 - Incidents placed into the Support queue will be acknowledged by the Support Team within 1 hour. Customer will be updated with a plan for resolution within 3 hours thereafter if the Incident has not already been resolved.

    (iii) For Priority 3 - Incidents placed into the Support queue will be acknowledged by the Support Team within 2 hours. Customer will be updated with a plan for resolution within 6 hours thereafter if the Incident has not already been resolved.

13. **Disaster Recovery.** A disaster constitutes an exceptional scenario which, when it occurs, results in the loss of services of the Service Provider for an extended period and critically affects Customer's business. Service Provider ensures that site and system resilience is in place so that services remain available for Customer in the event of a site disaster. Site and system resilience is achieved through a combination of local resilience on the Production site (where critical components and services are replicated or deployed in a cluster environment to ensure business continuity in case of hardware or software failure) and the provision of a Disaster Recovery site (which continues operations should a critical issue occur at the Production site). In the event of a disaster, Service Provider will use all reasonable efforts to switch to the Disaster Recovery site in accordance with the timeframes set forth in the table below where "H" is the time at which Service Provider's operational staff first becomes aware of the Disaster.

| SWITCH TO DR | Detection | Decision to switch | Invoke emergency procedures | Recovery Time Objective (RTO) | Recovery Point Objective (RPO) |
|---|---|---|---|---|---|
| Full loss of primary site | H+15 min | H + 2 hours | H + 3 hours | H + 4 hours | 15 mins |
| Major application Incident without data corruption | H+15 min | H + 2 hours | H + 3 hours | H + 4 hours | 15 mins |
| Major application Incident comprising unrecoverable data corruption | H+15 min | H + 2 hours | H + 4 hours | H + 4 hours | Up to 4 hours |

| | | | | | |
|---|---|---|---|---|---|
| Serious Connectivity issues at the primary site (inbound/outbound) | H+15 min | H + 2 hours | H + 3 hours | H + 3 hours | None |

Customers are notified as soon as possible upon a Disaster situation affecting services provided by Service Provider. Disaster scenarios and communication strategies are detailed in the Business Continuity Plan.

**Disaster Recovery Testing** or Disaster Recovery Role Swaps occur once annually at a minimum. Disaster Recovery Role Swaps are a form of testing where operations are run from the Disaster Recovery site instead of the Production site for a period of time to ensure business continuity in case of disaster. Customers are notified by Service Provider in advance of these tests.

14. **Monitoring.** Customer is the data controller and Service Provider is the data processor in relation to data flowing through the Hosted Services. Customer therefore is entirely responsible for monitoring its own business operations (monitoring transactions, payments, flows processed through the Hosted Services in line with what the Hosted Services to which Customer has subscribed can deliver). Service Provider is responsible for the technical monitoring of the Hosted Services within the perimeter of its control (connections, performance, processes, Incidents etc.).

15. **Service Status.** The Customer has the right to monitor the availability of the Subscription Services on an ongoing basis by means of the reports, status and availability data provided at: https://status.pt-x.com.

16. **Updates to this SLA.** Service Provider shall be entitled to amend this SLA to incorporate additional mandatory contractual provisions as required by Bacs and its other third-party providers from time to time in order to comply with its Shared Infrastructure Programme or any successor thereto.

    Service Provider may also amend this SLA from time to time as required to reflect changes in its operational processes, mandatory regulatory or legal requirements or evolution of the services provided, provided always that the amended version does not materially degrade the service levels enjoyed by Customer in the version being replaced.