Service Level Agreement – Hosted Services

This service level agreement ("SLA") applies to the financial messaging 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.

The Hosted Services include the services which are defined in the Agreement as "GlobalReach Services", "Bottomline Service Bureau" and "Financial Messaging Services", as applicable.

1. **Access Authorisation.** Subject to the terms and conditions of the Agreement and the applicable Order Agreement(s), Customer and its end users may access and use Hosted Services solely (i) for Customer's internal business operations, with no right to make such Hosted Services available to third parties, other than its own affiliates; and (ii) in accordance with the applicable documentation provided by Service Provider ("Documentation"). Customer's authorisation to use Hosted Services is non-exclusive, non-transferable, non-sublicensable, terminable and limited to any restrictions set forth in the documentation. Customer may make the Hosted Services available to use by its affiliates (within any applicable license parameters) providing that (i) it ensures that these affiliates comply with the applicable provisions of the Agreement and (ii) Customer is responsible for its affiliates' use of the Hosted Services and compliance with the Agreement as if the affiliates were Customer.

2. **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.

3. **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.

4. **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.

5. **Infrastructure.** Customer is fully responsible for the entirety of its own infrastructure except any Service Provider component (e.g. router) 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.

6. **Service Connectivity.** Customer is responsible for selecting the network solution to be used for connection to the Hosted Services; in particular Customer must ensure that the connectivity architecture selected meets its requirements in terms of security, availability, capacity, resilience and performance. The network architecture chosen by Customer can vary (examples include MPLS connectivity, customer leased line connectivity, and VPN over internet connectivity). The data flow between Customer and the Hosted Services is encrypted using industry standard encryption algorithms. Connectivity responsibilities are as follows:

Connectivity Method	Service Provider Responsibility	Customer Responsibility
MPLS Connectivity	Connectivity	Physical security and hosting of Service Provider router at Customer site
Customer Leased Line connectivity	Physical security and hosting of Customer router at the Hosted Services location	Connectivity
VPN over Internet Connectivity	Service Provider's internet connectivity (availability, bandwidth, quality of service) VPN tunnel joint responsibility with Customer for unmanaged VPN	Customer's Internet connectivity (availability, bandwidth, quality of service) VPN tunnel joint responsibility with Service Provider for unmanaged VPN
Internet Connectivity	Joint responsibility with Customer	Joint responsibility with Service Provider

7. **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. Amendments to the infrastructure are handled as set out in section 16 below, and Customer issues arising through the use of the Hosted Services are handled as set out in section 13.

   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 and Customer end user access to the Hosted Services requires a mandatory secondary authentication (multi-factor authentication) after password control. 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.

   Customer Scrutiny Right. Upon request from Customer, Service Provider provides the list of Service Provider employees who have logical or physical access rights to Customer data.

8. **Hosted Services Availability**. Service Provider will use all reasonable efforts to reach the targeted Availability Rate (calculated as set out below) of 99.8% per calendar quarter for Production environments. The Availability Rate is calculated as a percentage of total hours of availability for such quarter, excluding periods that the Services are unavailable due to Excluded Events. For the purposes of this section "availability" shall mean the ability to access and use the Hosted Services.

   Availability Rate is calculated by taking the sum of the hours of availability during Service Availability Hours (including Out-of-Hours support if applicable) and dividing it by the Total number of Service Availability Hours (including Out-of-Hours support if applicable) for a given period. Periods of less than an hour are expressed as a decimal fraction of an hour.

   Ta = *Number of hours service is unavailable per calendar quarter during Service Availability Hours*

   Tq = *Total number of service hours per calendar quarter during Service Availability Hours*

   Availability Rate [%] = $\left((1 - \frac{Ta}{Tq} \times 100\right)$

   An "Excluded Event " is one of the following events which results in services being unavailable: (a) network, Internet or telecommunications problems outside of Service Provider's control; (b) failure of Customer's hardware and/or software; (c) any scheduled, negotiated or emergency maintenance period; (d) problems with Customer's networks, including LANS, WANS, connectivity to the Hosted Services or any failure of such networks to conform to any capacity requirements; (e) Scheduled and Mandatory Maintenance (as defined below); or (f) network intrusions, denial of service attacks to the extent that these have not been caused by Service Provider's failure to implement technical and organisational measures against these risks in accordance with good industry practice, or any force majeure events; (g) service interruption linked to scheduled or unscheduled downtimes for Interbank Networks such as (this list is not exhaustive) BACS, SWIFT, SIC, euroSIC, SECOM, Telekurs; (h) service interruption linked to scheduled or unscheduled downtimes at the third party service providers (e.g. datacentres); (i) crisis events such as fire, flooding, pandemic as listed in the Business Continuity Plan; (j) Customer exceeds the authorised daily volume limits or the concurrent users limit, as defined in the Agreement.

   Service Availability Hours. The hours during which the Hosted Services are made available to Customer and supported according to the applicable Service Desk support level to which the Customer has subscribed, Standard, Gold or Platinum, excluding those Excluded Events as outlined under Hosted Services Availability – please see section 12 for more detail.

   Service Accessibility Hours. The hours during which the Hosted Services can be accessed. For periods outside the Service Availability Hours, Customer may access the services but incident management and availability service levels do not apply,

and Customer will not have access to Service Desk Support. Outside these hours, the Hosted Services are not available for use (services under maintenance for example).

The Hosted Services are accessible 24*7*365 except for internal maintenance windows (Hosted Services maintenance) and external maintenance windows (Interbank Network maintenance).

9. **Scheduled and Mandatory Maintenance**. Service Provider at its sole discretion, regularly conducts maintenance to perform routine software and hardware and other mandatory upgrades on the systems supporting the Hosted Services. Customer acknowledges and agrees that access to the Hosted Services may be degraded during scheduled maintenance. Customer involvement particularly for validation and non-regression testing may be required. Notification on scheduled or mandatory maintenance is as defined below unless otherwise defined by the recognised body mandating the change. Service Provider commits to provide and install new product versions rendered necessary by infrastructure changes (such as operating systems and hardware components) and product versions rendered necessary by Interbank Network enhancements where these enhancements do not involve a structural infrastructure or software change for Service Provider.

   Maintenance Notification. Service Provider provides 30 business days' notice at a minimum for changes relating to scheduled maintenance that are due to occur during Service Availability Hours. These changes include upgrades relating to operating systems, infrastructure components and Interbank Network enhancements. Service Provider will use commercially reasonable efforts to schedule maintenance at non-peak hours and limit its occurrence. Service Provider provides two (2) business days' notice at a minimum for mandatory maintenance which involves changes which Service Provider deems essential to be implemented before the next scheduled maintenance window. These include, without limitation, product releases, software and hardware upgrades, continuous improvement changes and configuration changes.

10. **Emergency Maintenance.** Emergency maintenance may be necessary to address emergency changes (fix deficiencies or address unexpected risks to the Hosted Services). An emergency change corresponding to a Critical Incident or High Incident and thus necessitating a rapid return to normal operations may also be required. Customer acknowledges and agrees that access to the Hosted Services may be degraded during emergency maintenance. Service Provider will notify customers upon event in this instance.

11. **Test Environment.** A test environment is made available to Customer. Customer is responsible for providing test cases and data and is also responsible for test implementation. Customer is also responsible for notifying Service Provider upon test completion. Test support is provided during Service Desk hours on a case by case basis only. Priority will always be given to production operations. If Customer wishes to procure test support, then it may initiate a Service Request for this purpose.

    Test Environment Accessibility Hours. The hours during which test environments can be accessed by Customer. There is no commitment on support service outside Service Desk hours unless provided for in accordance with a specific Order Agreement. Test environment accessibility is 24 * 7 * 365 excepting scheduled test environment maintenance and any crisis as outlined in the Business Continuity Plan.

    Test Environment Availability Hours. The hours during which the test environment is made available to Customer with service levels offered on a case by case basis only. Customers may utilise the test environment from 09:00 to 17:00 on normal business days during normal operations. Normal operations exclude all test environment maintenance windows and any crisis event affecting Business Continuity (pandemic, fire, flood..). Service Provider cannot guarantee test environment availability during maintenance windows.

    Test Environment Booking. If Customer wishes to ensure test environment availability (i.e. that no maintenance is underway), it must book a test environment slot under the following conditions: Customer to initiate a test slot request to Service Provider no earlier than twenty (20) calendar days in advance of the test slot required; Customer may utilise the booked test slot for a maximum of five (5) business days.

    Test Environment Monitoring. Gold and Platinum customers can request a Start of Business Day check on the availability of the test environment. Service Provider will communicate to affected customers in cases of unavailability.

12. **Service Desk Support**.

    Access. The Service Provider's Service Desk may be reached via the dedicated Service Desk Portal.

    Customers may contact the Service Desk by phone in the following specific circumstances only: (i) if the web portal is unavailable for any reason; (ii) to expedite handling of Critical Incidents (it is mandatory for Customer to contact the Service Desk by telephone in addition to opening the Incident on the Service Desk portal); and (iii) for Out-of-Hours support for Critical Incidents only.

    The contact information for the Service Desk can be found on the Service Provider's website based on region and type of products and services. Secure, password-protected access to Service Provider's customer support website is available 24 hours a day, 7 days a week, and 365 days a year.

Service Provider commits to providing support in English. Support in other languages may be provided if practicable for specific geographies.

Service Desk Hours. Hours during which the Service Desk is open and provides support to customers. The Service Desk Hours for Standard Customers are 07:00 to 18:00 business days for EMEA and North America time zones and 09:00 to 18:00 business days for the APAC time zone, unless noted otherwise on the contact support page on the Service Provider website. Outside these hours, Out-of-Hours support is provided, when agreed contractually for Critical Incidents only, as per the Support Levels below.

Support levels. Service Provider offers three support levels – Standard, Gold and Platinum. Service availability for Standard Customers is 07:00 to 18:00 business days for EMEA and North America time zones and 09:00 to 18:00 business days for the APAC time zone. Service availability for Gold Customers is 24*5. Service availability for Platinum Customers is 24*7.

13. **Incident Management**

For the purposes of this section, the term "Incident" shall mean a material defect in the Hosted Services, experienced by Customer, that prevents the Hosted Services from conforming in any material respect to the Documentation.

Customer raises an Incident through the Service Desk. Customer provides all supporting information and documentation required to investigate the Incident. If supporting documentation is missing – any defined response and resolution timelines are suspended. All Critical Incidents must be reported to Service Provider's Service Desk via telephone following Incident creation on the Service Desk portal.

Service Provider will determine, at its sole discretion, the applicable severity level of any reported Incident in accordance with the descriptions set forth in the table below. Service Provider formally acknowledges the Incident and then responds to the Incident in accordance with the target acknowledgement and response times set forth in the table below. Service Provider informs Customer about the status of the Incident and any actions taken to date. Where possible, Service Provider provides an estimated timeframe for issue resolution. Service Provider keeps Customer informed on the status of the Incident. Customer is responsible for providing any additional supporting information required for the investigation. If required supporting documentation is not provided, timelines are suspended and resolution could be delayed.

Service Provider targets to resolve Incidents in accordance with the target resolution times set forth in the table below:

Incident Severity	Standard	Gold	Platinum
Critical (P1) Incident – Inability to use the application for absolutely necessary business transactions. 100% users are impacted or An immediate solution is required as 50% of users are impacted or an entire group of users (with same role / same unit) is impacted	<u>Acknowledgement</u> Incidents will be acknowledged by the Service Desk tool within 15 minutes. <u>Response</u> Service Provider will coordinate a Critical Incident team and provide a response to Customer within 30 minutes. <u>Resolution</u> A work around or fix will be provided within 4 business hours.	<u>Acknowledgement</u> Incidents will be acknowledged by the Service Desk tool within 15 minutes. <u>Response</u> Service Provider will coordinate a Critical Incident team and provide a response to Customer within 30 minutes. <u>Resolution</u> A work around or fix will be provided within 4 business hours.	<u>Acknowledgement</u> Incidents will be acknowledged by the Service Desk tool within 15 minutes. <u>Response</u> Service Provider will coordinate a Critical Incident team and provide a response to Customer within 30 minutes. <u>Resolution</u> A work around or fix will be provided within 4 business hours.

High (P2) Incident – Limitations or restrictions to important functionality causing a specific part of the system to fail. Impact on a functional group. Solution required within 2 business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will coordinate an Incident team and provide a response to Customer within 2 business hours. Resolution A work around or fix will be provided within 2 business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will coordinate an Incident team and provide a response to Customer within 2 business hours. Resolution A work around or fix will be provided within 2 business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will coordinate an Incident team and provide a response to Customer within 1 business hour. Resolution A work around or fix will be provided within 1 business day.
Medium (P3) Incident – Inconvenience to perform business transactions; work around allows business processing to continue. Impacts few users. Solution required within several business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 8 business hours. Resolution A work around or fix will be provided for accepted Incidents within 5 business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 8 business hours. Resolution A work around or fix will be provided for accepted Incidents within 5 business days.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 8 business hours. Resolution A work around or fix will be provided for accepted Incidents within 5 business days.
Low (P4) Incident – Little or no effect on business functionality and no impact on business processing. Very few users impacted. No time constraint on solution delivery.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 2 business days. Target Resolution Resolution to be provided on a case by case basis.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 2 business days. Target Resolution Resolution to be provided on a case by case basis.	Acknowledgement Incidents will be acknowledged by the Service Desk tool within 15 minutes. Response Service Provider will provide a response to Customer within 2 business days. Target Resolution Resolution to be provided on a case by case basis.
	Targeted Achievement Rate of 90% for the above timeframes		

Customer is responsible for formally closing an Incident that has been resolved. However, Service Provider reserves the right to close a resolved Incident nine (9) days after resolution if no feedback has been provided by Customer.

Customer can escalate an Incident if it is dissatisfied with the way it is being handled. Customer may escalate Incidents using the Incident escalation process provided by Service Provider.

14. **Incident Notification.** Customer is notified within thirty (30) minutes of any Critical Incident (as defined under Incident Management) detected by Service Provider which impacts services.

15. **Service Requests.** Customer may make formal requests for the delivery of additional services or amendments to existing services ("Service Request"). In this case, a formal written request is required (email from official company email address or letter on customer branded paper) detailing the Service Request in full, and this must contain at least one signature from an authorised Customer representative.

    Service Request Acknowledgement. Service Provider will make an initial response to all Service Requests within two (2) business days during normal operations. Normal operations exclude any crisis event affecting Business Continuity (pandemic, fire, flood etc..). Positive responses may include a proposal or may be followed by a proposal. Negative responses include an explanation as to why the Service Request cannot be fulfilled.

    Service Request Acceptance. Customer must formally accept the positive Service Request response or proposal sent by Service Provider for the related work to commence.

    Service Request Support. For Gold Customers, Service Request support is provided for up to four (4) Service Requests a month where the Service Request effort is less than one (1) hour. For Platinum Customers, Service Request support is provided for all Service Requests where the Service Request effort is less than one (1) hour. Service Request support is applicable for a given month and cannot be carried forward. Service Request support does not include reporting.

16. **Change Management.** In the case the Service Request corresponds to a Customer change request or a Customer project related request, Service Provider deploys the change on the test environment within the agreed timeframe. Customer is responsible for test implementation by its users using its own test scenarios. Customer formally confirms that the change in the test environment meets its requirements and formally authorises Service Provider to deploy the change into production within the agreed timeframe. In the case of an internal change request issued by Service Provider, Customer is also responsible for test implementation. However, if no response or confirmation on test success is received from Customer within the specified timeframe, Service Provider can authorise deployment to the Production environment.

17. **Customer Administrators.** (Not applicable for APAC region). Customer formally nominates two (2) key representatives to (i) act as recipient for all formal Service Provider communications relating to the Hosted Services and (ii) act as administrator for Customer end user access to the Hosted Services and (iii) be authorised to make formal requests to Service Provider relating to the Hosted Services such as service requests, change requests and test slot registrations on behalf of Customer. Customer representatives' contact details (and any subsequent updates) must be communicated to Service Provider in writing, immediately following their nomination.

18. **Minimum System Requirements; Internet Connectivity and Browser Settings**. Customer acknowledges and agrees that use of the Hosted Services requires (i) maintenance of an Internet connection and browser on each authorised user's workstation with adequate bandwidth and the minimum system requirements as set forth in the Documentation, (ii) configuration of browsers to access the Hosted Services' websites, dashboards and portals, and (iii) verification that its firewalls and proxy servers allow access to the Hosted Services.

19. **Support Limitations**. In the case of any Incidents that are not reproducible by Service Provider Service Provider will restore the Hosted Services but may not be able to correct the underlying cause if the Incident is not reproducible. Service Provider is not responsible for correcting any Incidents that are (i) for services for which Customer does not have the appropriate subscription if such a subscription is required for the service (e.g. SWIFT); (ii) due to Customer lack of technical knowledge / training on the Hosted Services provided; or (iii) software errors related to any of the following: (A) changes to Customer's operating system or environment that adversely affect the Hosted Services; (B) use of the Hosted Services in a manner for which such Hosted Services were not designed or not otherwise in conformance with the Documentation; (C) Customer's negligence or misuse of the Hosted Services. In the event Service Provider is requested to provide support for any of the foregoing, Service Provider will use commercially reasonable efforts to assist Customer but reserves the right to charge for such assistance at its then applicable professional services rates.

20. **Business Continuity.** Service Provider maintains a Business Continuity plan which is reviewed annually. The Business Continuity plan details Service Provider's strategy for continuing business in case of major Incidents such as natural disasters, pandemics, technology outage, terrorist attack etc. A business Impact analysis exercise is conducted annually which is a systematic process to determine and evaluate the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

21. **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	Restart Services (RTO)	Maximum Loss of Data Target (RPO)
Full loss of primary site	H + 15 min	H + 2 hours	H + 4 hours	<= 15 minutes (no data corruption) <= 6 hours (data corruption)
Major application Incident without data corruption	H + 15 min	H + 2 hours	H + 4 hours	<= 15 minutes
Major application Incident comprising data corruption	H + 15 min	H + 2 hours	H + 4 hours	<= 6 hours
No connectivity to a banking network from the primary site	H + 15 min	H + 1hr 15 min	H + 4 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.

22. **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.).

23. **Reporting.** Service Provider provides the following reports to Customer:

    An Initial Critical Incident Status Report is sent to affected customers within five (5) business days of the Incident. This initial report is sent with information available at the point of issuing the report. Follow-up updates will be provided where applicable.

    A Service Availability Report listing service availability for the period and conformity with availability rate is provided to Customer during scheduled service reviews. Platinum customers receive this report monthly.

    A Daily Average Volume Report detailing volumes processed over the last twelve (12) months provided is provided to Customer during scheduled service reviews.

    A Disaster Recovery Test Report is provided to Customer annually upon request, provided the request is made within three (3) months of Disaster Recovery Test completion.

24. **Customer Data Retention.** Service Provider retains Customer data for twelve (12) rolling months as standard. Customer data may be retained in any combination of online data and archive files during this period. This retention period can be extended or reduced for certain specific Hosted Services based on Customer subscription in line with Customer requirements.

25. **Customer Data Archives.** Where there is an interbank network requirement for the service to which Customer has subscribed, Service Provider maintains an archive of Customer data. Customer data is made available by the Hosted Services either during or following Customer's Data Retention Period. Service Provider provides Customer with access to download its data archives through a secured channel. It is Customer's responsibility to ensure data archives have been downloaded and stored in its own infrastructure. Service Provider reserves the right to delete Customer archive files for the previous calendar year, following a minimum of three (3) reminder communications to Customer.

26. **Customer Data Confidentiality Policy**. Service Provider maintains a Privacy policy governing the confidentiality of privacy information and conducts a privacy risk assessment annually. Where required by FINMA regulations, Service Provider also maintains a Data Confidentiality policy and conducts a data confidentiality risk assessment annually. The Data Confidentiality policy includes an inventory of Client Identifying Data types managed by Service Provider. Each data type is listed with associated individuals access rights; logical and physical storage location; confidentiality level required; associated data lifecycle security mechanisms. The policy and associated monitoring reports can be made available to Customer on demand. Service Provider's Client Data Protection and Confidentiality policy incorporates a Mass Data Management policy which lists

Service Provider's employees with restricted access to confidential data and defines data access procedures and data locations (logical and physical).

27. **SWIFT Customers.** SWIFT customers must choose the Gold or Platinum support level to ensure services follow SWIFT regulations.

Customer Responsibilities. If Customer is using the Hosted Services to access SWIFT, it must have a valid membership agreement with SWIFT. Customer is responsible for paying all applicable SWIFT membership charges, SWIFT traffic fees and other fees levied by SWIFT, in accordance with its SWIFT user agreement. SWIFT customers must comply with the policies stipulated by SWIFT for SWIFT users and must notify Service Provider and SWIFT of any non-compliance with such rules and regulations and/or breach of any such conditions. SWIFT customers must treat as confidential, any information relating to the Hosted Services, or SWIFT operations (including but not limited to the contents of messages passing through the Services and Quoted Infrastructure), SWIFT technical documentation, SWIFT security tokens and SWIFT network information.

Customer Payload. Customer agrees that designated Service Provider operations staff may have access to Customer's message payload data for use only in appropriate operations / support tasks requiring such access. Access to Production platforms is restricted to these designated staff and change access to Production platforms is further restricted and subject to formal change authorisation. Service Provider user access is maintained at an appropriate number of individuals to carry out the support and operational activities in line with Service Provider's contractual commitments. User access is logged and reviewed and adjusted in line with employee roles twice annually at a minimum. Service Provider is not required to seek specific authorisation on each occasion when such access is required.

Delegated Operations. SWIFT customers may delegate certain operations to Service Provider and these delegated operations must be clearly identified in the Agreement. Customer's own personnel can act as SWIFT registered Security Officers (SOs) in which case Customer shall provide contact details for the designated Security Officers to Service Provider Alternatively Customer may nominate two or more Service Provider Security officers to act on its behalf. Customer delegates control and operation of its PKI certificates to two Security Officers (SO) at Service Provider. Customer's PKI keys are maintained securely by Service Provider according to SWIFT best practices and only accessible by authorised Service Provider personnel. Any changes to PKI keys are managed under related SWIFT procedures. Customer may request an audit trail of PKI operations. Customer may also request a list of authorised Service Provider personnel with access to the PKI keys.

Disaster Recovery Site and Tests. The Disaster Recovery site is capable of meeting SWIFT requirements in terms of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). SWIFT customers are required to participate in annual Disaster Recovery tests / Disaster Recovery Role Swaps.

SWIFT Upgrades. SWIFTNet upgrades are implemented by Service Provider at least one (1) month before the end of life of the current version; a SWIFT FIN standards release is provided by Service Provider for Customer testing at least six (6) weeks before the cutover date; SWIFT Quarterly security updates are applied by Service Provider in line with SWIFT requirements.

28. **SIC / EuroSIC / SECOM Customers.** These customers may delegate control of their RSA keys to two key contacts at Service Provider.

MINI-SIC. Customer provides Service Provider with the list of mini-SIC managers. Customer may delegate the physical transfer of the mini-SIC media to SIX to Service Provider. Customer is responsible for all communication with SIX. Service Provider is responsible for generating the encrypted outgoing dataset and its physical transfer to SIX. Service Provider is responsible for uploading the incoming dataset into the Hosted Services.

SECOM. During SECOM offline exercises, Customer is responsible for all communication with SIX and for providing the incoming data file to Service Provider. Service Provider is responsible for the encrypted file generation for outgoing data and the insertion of the incoming data file, provided by Customer, into the Hosted Services.

29. **Updates to this SLA.** Service Provider agrees to provide its services in compliance with the set of basic operational obligations as defined by SWIFT for Service Bureau Providers. Service Provider shall be entitled to amend this SLA to incorporate additional mandatory contractual provisions as required by SWIFT 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.

Customer may object to any such changes within thirty (30) days of being notified of them, in which case the parties shall meet to discuss in good faith to find a mutually agreeable solution. However, Customer understands and acknowledges that it is a condition of Service Provider's continued access to SWIFT that it must comply with SWIFT's mandatory provisions, which include the insertion of certain contractual clauses.

Where no unresolved objection exists after the thirty (30) day period allowed for objection, the new version of the SLA shall become part of the Agreement and shall replace the previous version in its entirety.

GLOSSARY

Business Day. Working days excluding weekends (Saturdays and Sundays in most geographic locations) and national holidays defined under Public Holiday.

Business Hours. Hours that fall during the Service Desk hours on a business day in the geography where the Hosted Services are based (and therefore excludes Out of Hours support).

Customer Administrator / Representative. Nominated Customer contact representative, acting as key point of contact for Service Provider Customer communication and authorised to make request to Service Provider for services such as access security measures, service and change Requests, test slot reservations, on behalf of Customer.

Disaster. An exceptional scenario which, when it occurs, results in the loss of services for an extended period and critically affects Customer's business.

Emergency Change. An emergency change is a change corresponding to a Critical Incident or High Incident and thus necessitates a rapid return to normal operations.

Incident. Any event resulting in a service interruption, a service slowdown or a loss of service quality.

Incident Acknowledgement. Automated email response sent to Customer with an Incident reference number once Customer logs an Incident in Service Provider's service desk tool.

Incident Priority. There are four Incident priorities as follows: Critical (P1), High (P2), Medium (P3), Low (P4).

Incident Resolution. A work around or fix provided by Service Provider to remedy an Incident.

Incident Response. The response provided to Customer by a Service Provider employee / team assigned to the Incident, following Incident acknowledgement and initial investigation.

Interbank Network. Networks that facilitate payment transfer between entities. Examples include (non-exhaustively) BACS, SWIFT, SIC, euroSIC, SECOM, and Telekurs.

Out of Hours support. Service provided by Service Provider outside the Service Desk hours. Corresponds to the additional support hours requested by Customer and agreed contractually with Service Provider to extend Service Desk Hours.

Production. Live business transaction processing which has effect outside a test environment.

Public Holiday. The following public holidays apply:
New Year's Day (Jan 1st); Good Friday; Labour Day (May 1st); Christmas Day (Dec 25th); Boxing Day (Dec 26th)
In addition, for EMEA Customers
Easter Monday;
In addition, for UK Customers
May Bank Holiday (early May); Spring Bank Holiday (May); Summer Bank Holiday
Note that if a bank holiday falls on a weekend, a 'substitute' weekday becomes a bank holiday, normally the following Monday.
In addition, for APAC Customers
Chinese New Year's Eve; Chinese New Year; Vesak Day; Hari Raya Puasa; Deepavali; New Year's Eve - 31st Dec

Recovery Point Objective. The Recovery Point Objective (RPO) is the targeted acceptable amount of data loss measured in time. It is the age of the files or data in backup storage required to resume normal operations if a computer system or network failure occurs.

Recovery Time Objective. The Recovery Time Objective (RTO) is the targeted duration of time within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Service Accessibility Hours. As set out in section 8.

Service Availability Hours. As set out in section 8.

Service Desk Hours. Hours during which Service Desk is open and providing support to customers.
Service Desk hours are defined on the Service Provider's website (www.bottomline.com/support) for each of Service Provider's regional Service Desks.

Service Request. A formal (written) Customer request for a service which is not Incident-related but results in the delivery of an additional service or an amendment to an existing service provided by Service Provider to Customer.

FM Hosted Services SLA Service Level Options-2.0

SERVICE AVAILABILITY		Standard	Gold	Platinum
Service Availability Rate Objective	99.8% per calendar quarter for Production environment.	■	■	■
Service Accessibility Hours *(Hours when Service may be accessed, including periods outside supported hours)*	24 * 7 * 365, except -scheduled and mandatory FM Hosted Services maintenance windows -applicable Banking network maintenance windows (such as SWIFT)	■	■	■
Service Availability Hours *(Basis for Service Availability Rate calculation, excluding Excluded Events)*	See Service Desk Hours	■		
	24*5		■	
	24*7			■
SERVICE DESK / SUPPORT		Standard	Gold	Platinum
Time zones supported	EMEA: GMT; GMT + 1; North America: EST / GMT – 4; APAC: SGT (GMT + 8)	■	■	■
Service Desk Portal	Unlimited access to Bottomline's Service Desk portal	■	■	■
Service Desk Hours	07:00 to 18:00, business days for all incidents (except APAC region) 09:00 - 18:00, business days (APAC region) * Business Days and ** Public Holidays defined below	■	■	■
Out of Hours Support	Out-of-Hours support for **critical incidents only** as follows:			
	• Upon request at additional fee and subject to on-call engineer availability	■		
	• 24 * 5		■	
	• 24 * 7			■
Incident Acknowledgement Timeframe	All incidents – within 15 minutes Automated email response to Customer – incident has been formally logged in Service Desk tool.	■	■	■

Incident Response Timeframe Target achievement rate of 90% for these timeframes	Critical – within 30 minutes Response provided to the Customer by a BT employee / team assigned to the incident	■	■	■
	High Priority - within 1 business hour			■
	High Priority - within 2 business hours	■	■	
	Medium Priority - within 8 business hours	■	■	■
	Low Priority - within 2 business days	■	■	■
Target Incident Resolution Timeframe Target achievement rate of 100% for Critical incidents and 90% for High, Medium and Low incidents	Critical - within 4 business hours	■	■	■
	High Priority - within 1 business day			■
	High Priority - within 2 business days	■	■	
	Medium Priority - within 5 business days (for accepted incidents)	■	■	■
	Low Priority – on a case by case basis	■	■	■
Crisis Incident Team	A critical incident team is appointed for all Critical Incidents with escalation contacts as required.	■	■	■
Service Request Acknowledgement	Within 2 business days at a maximum during normal operations. On a best effort basis for crisis scenarios as defined in our Business Continuity plan.	■	■	■
Service Request Support	Support included for all Service Requests a month where Service Request effort <= 1 hour.			■
	Support included for 4 Service Requests a month where Service Request effort <= 1 hour.		■	
Platform Incident Notification	Critical incidents are notified to customers within 30 minutes of detection by Bottomline.	■	■	■
Customer Data Retention	Bottomline retains customer data for 12 rolling months as standard. The Customer data may be retained as any combination of online data and archive files.	■	■	■
PLATFORM MAINTENANCE & TESTING		Standard	Gold	Platinum
Scheduled Maintenance Notification	BT provides 30 business days notice for scheduled maintenance during Service Availability hours. Scheduled maintenance includes changes such as upgrades relating to operating systems, infrastructure components and inter-banking network enhancements.	■	■	■
Mandatory Maintenance Notification	BT provides 2 business days notice for mandatory maintenance. Mandatory Maintenance involves changes that Bottomline deems necessary for implementation prior to the next scheduled maintenance window.	■	■	■
Emergency Maintenance Notification	Emergency changes are unplanned - notification is provided upon event.	■	■	■

Test Environment Accessibility	24 * 7 * 365, except -scheduled test environment maintenance windows -crises as defined in the Business Continuity Plan	■	■	■
Test Environment Availability	09:00 - 17:00 business days during normal operations. Bottomline cannot guarantee test environment availability during maintenance windows. If customers wish to ensure test environment availability (i.e. that no maintenance is underway), they must book a test environment slot under the following conditions: - Request for test slot not to be made more than 20 days in advance - Testing period is 5 business days maximum. Test Environment availability, even if pre-booked, is not guaranteed for any crisis outlined in the Business Continuity Plan.	■	■	■
Test Environment Monitoring	Start of business day check on availability of test environment and customer is notified upon unavailability.		■	■
SWIFT Upgrades	For SWIFT Customers -SWIFT FIN standards release provided for Customer testing 6 weeks before cutover date. -SWIFTNet upgrades implemented 1 month before end of life. -SWIFT Quarterly security updates applied in line with SWIFT requirements		■	■
REPORTING		Standard	Gold	Platinum
Critical Incident Report	Initial Critical Incident Report sent to affected Customers within a maximum of 5 business days of event. Initial report sent with available information. Follow-up updates will be provided where applicable.	■	■	■
Service Availability Report	Report listing service availability for period and conformity with availability rate provided monthly.			■
	Report listing service availability for period and conformity with availability rate provided during scheduled service reviews with customers.	■	■	■
Volumes Report	Report containing daily average volumes exchanged over last 12 months provided during scheduled service reviews with customers.	■	■	■
Disaster Recovery Report	Report detailing the annual Disaster Recovery Test / Role Swap to be provided on request.	■	■	■

BUSINESS CONTINUITY & DISASTER RECOVERY		Standard	Gold	Platinum
Business Continuity	A Business Continuity Plan (BCP) in place and is updated annually. A BCP business Impact analysis exercise is conducted annually.	■	■	■
Business Continuity Plan available	Copy of Business Continuity Plan available upon request.	■	■	■
Disaster Recovery Test Frequency	Disaster Recovery Test / Disaster Recovery Role Swap occurs once annually. Customers are notified in advance of this annual test.	■	■	■
Switch to DR Timeframes	In accordance with table below:	■	■	■

SWITCH TO DR	*DETECTION*	*DECISION TO SWITCH*	*RESTART SERVICES (RTO)*	*MAXIMUM LOSS OF DATA OBJECTIVE (RPO)*
Full loss of primary site	H + 15 min	H + 2 hours	H + 4 hours	<= 15 min (no data corruption) <= 6 hours (data corruption)
Major application Incident without data corruption	H + 15 min	H + 2 hours	H + 4 hours	<= 15 min
Major application Incident comprising data corruption	H + 15 min	H + 2 hours	H + 4 hours	<= 6 hours
No connectivity to a banking network from the primary site	H + 15 min	H + 1 hr 15 min	H + 4 hours	None

*Business Days: Working days excluding weekends (Saturdays and Sundays – unless otherwise specified) and national holidays defined under Public Holiday.

**Public Holidays: New Year's Day (Jan 1st); Good Friday; Labour Day (May 1st); Christmas Day (Dec 25th); Boxing Day (Dec 26th)

In addition, for EMEA Customers

Easter Monday;

In addition, for UK Customers

May Bank Holiday (early May); Spring Bank Holiday (May); Summer Bank Holiday

Note that if a bank holiday falls on a weekend, a 'substitute' weekday becomes a bank holiday, normally the following Monday.

In addition, for APAC Customers

Chinese New Year's Eve; Chinese New Year; Vesak Day; Hari Raya Puasa; Deepavali; New Year's Eve - 31st Dec