Service Order Attachment for
Message Security Services

Capitalized terms not defined in this Attachment will have the meanings set forth in the MSA.

Scope of Work

PatientLock intends to use SilverSky ("Host") installed products and services to provide a Security Operations Center-as-a-Service ("Service") designed to replace all of the necessary capital costs, licensed products and integration services normally required to establish a security program. The Host uses a secure and compliant cloud for ease of deployment and consumption by the healthcare industry, as well as others making the Service available at predictable and affordable rates. Under this Statement of Work for SilverSky's Message Security Services ("Message Security Services") PatientLock agrees to provide _____, ("Customer") with certain described services. It is understood by the Customer that PatientLock intends to retain the Service, in whole or in part, by SilverSky in connection with the Service under this Statement of Work. The Service focuses Cyber Threat Detection on network devices not covered by Message Security Services.

1. Message Security Services. Message Security Services will mean any of the message security services identified below including EPS Bundle - SPAM/AV, DLP, TAP, SEP, Encrypted Email (SKU# S-200-2884) and as may be further described in the *Service Order*. PatientLock will provide end users authorized by Customer to receive Message Security Services (each a "User") with access to the Message Security Services on the domain name(s) Customer specify to PatientLock, provided that Customer owns the domain name(s). PatientLock will provision Customer's specified domain names and Users on or before the date PatientLock first makes Message Security Services available to Customer ("Launch Date"). Additional domain names may be established thereafter.

2. Administrators. Prior to the Launch Date, Customer will appoint up to three administrators, each of whom will have the power to act as Customer's agent, with the authority to make decisions and give notices on Customer's behalf ("Administrators") and whose instructions and representations PatientLock may rely on. Administrators' authority includes, but is not limited to (i) controlling the creation and deletion of Users and domain names; (ii) managing changes to User information (such as changes to User name or password); (iii) serving as PatientLock's authorized technical contact for the Message Security Services; (iv) setting business rules/policies and/or filters on the Message Security Services that may filter and/or terminate emails sent to or by Users without delivering them; (v) requesting the restoration or disclosure of content by submitting an Authorization for Disclosure of Information form to PatientLock, and (vi) monitoring complaints against Users. At least one Administrator must attend a training session on the Message Security Services, which PatientLock will provide at no charge. Customer may replace Administrators at any time upon notice to PatientLock.

3. Technical Support. Customer will have sole responsibility for handling technical support inquiries from Customer's Users, unless Customer has purchased End User support from PatientLock. PatientLock will have responsibility for responding to inquiries from Customer's Administrators regarding Message Security Services. PatientLock will respond to inquiries from Customer's Administrators on a 24x7 basis; provided that inquiries (i) must be submitted via toll- free telephone or email in the English language, and (ii) such inquiries will be responded to in English.

4. Term And Termination. This Attachment will be in effect during the Initial Term set forth in the *Service Order* and will thereafter automatically renew for a period equal to the initial term as provided in the *Service Order*. The fee schedule listed in the *Service Order* will be subject to annual pricing adjustments. However, such pricing adjustments may not exceed 5%, on an annualized basis, during the Initial Term. Intention not to renew must be provided at least 60 days prior to the beginning of the renewal term. The sections related to Payment Terms, Limitation of Liability, Warranties, Indemnity, Confidentiality and Intellectual Property from the General Terms and Conditions, as provided in the referenced General Terms and Conditions document, will survive the expiration or termination of this Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, Customer must pay all undisputed fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

5. **Fees.** Customer will pay PatientLock the fees set forth in the *Service Order* for Message Security Services Customer purchase. PatientLock will invoice Customer for Message Security Services according to the Service and PatientLock's established billing cycle.

6. **Disclaimers.** PatientLock does not guarantee a continuous, uninterrupted, virus-free, malware-free, intrusion-free, or continuously secure Customer network or network environment, and PatientLock is not liable if Customer or Customer's end users are unable to access Customer's network at any specific time. Additionally, PatientLock does not guarantee that PatientLock will be able to replace any of Customer's information, content, or other data that may be lost, damaged, or stolen resulting from use of the Services.

Statement of Work for Message Security Services

PatientLock is committed to providing a scalable and highly available solution through the following Statement of Work.

1. **Service Level Availability Calculation**

$$\text{Availability} = \frac{\text{Total Monthly Minutes} - \text{Maintenance Minutes} - \text{Downtime Minutes}}{\text{Total Monthly Minutes} - \text{Maintenance Minutes}} \times 100\%$$

2. **Term of the Statement of Work.** This Statement of Work becomes applicable to the Services upon the later of (a) completion of a mutually agreed upon stabilization period (if applicable), or (b) 30 days from the Launch Date.

3. **Defined Terms.** For the purposes of this Statement of Work, the following terms shall have the following meanings:

   a. "Available" or "Availability" means that the Customer is able to access the Service via the specific access method for that Service subject to the exclusions defined in Downtime Minutes below.

   b. "Downtime Minutes" means the total number of minutes that Customer's end users cannot access the specific Service via the normal access method for that Service. The calculation of Downtime Minutes excludes time a Service is not Available due to any of the following: (i) the Maintenance Minutes; (ii) Customer's or Customer's end users' own Internet service provider; (iii) a Force Majeure event; (iv) any systemic Internet failures; (v) (vi) third party encrypted email Services; (vii) any failure in Customer's or Customer's end users' own hardware, software or Network connection, (viii) Customer's or Customer's end users' bandwidth restrictions, (ix) Customer's or any of Customer's end users' acts or omissions; (x) Customer configure Customer's email system to function as Open Relay; (xi) unavailability of Customer's primary email service; and (xii) and each Service-specific additional exclusion stated below.

   c. "Filter" means to detect and block or quarantine all email messages with viruses that (i) match against available/known virus signatures or (ii) identifiable by industry standard heuristics.

   d. "Mail Delivery Time" means the time elapsed between entry of an email to PatientLock's gateway and its exit.

   e. "Maintenance Minutes" means the time period during which the Services will not be Available (i) each month so that PatientLock can perform routine maintenance to maximize the performance of the Services, up to 240 minutes (4 hours) per Service per calendar month, and (ii) any emergency maintenance PatientLock deems necessary in PatientLock's sole discretion.

   f. "Maintenance Windows" means the scheduled time period during which PatientLock might perform routine maintenance each week. Current Maintenance Windows are Thursday from 10PM to Friday 5 AM Mountain Time. PatientLock may change Maintenance Window at any time. PatientLock will use reasonable efforts to notify Customer in advance of any changes to PatientLock's normal Maintenance Windows.

   g. "Network" means the network outside of PatientLock's border routers.

   h. "Open Relay" means an email server configured to receive email from an unknown or unauthorized third party and forward the email to one or more recipients who are not users of that email system. PatientLock reserves the right at any time during the supply of the Services to test whether the Customer's email systems function as an Open Relay. If at any time the Customer's email systems are found to function as an Open Relay, then PatientLock reserves the right to suspend all or part of the Services immediately and revoke SLA credit requests until the problem has been resolved.

   i. "Total Monthly Minutes" means the number of days in the month multiplied by 1,440 minutes per day.

   j. "Virus" means a known binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, or use inordinate system resources in the form of memory, disk space, or network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources.

4. **Maintenance Notices.** PatientLock will communicate the date and time that PatientLock intends to make Services unavailable through a global "welcome message" or an email sent to Customer's Administrator at least 24 hours in advance or longer, if practical. Customer understands and agree that there may be instances where PatientLock needs to interrupt the Services without notice in order to protect the integrity of the Services due to security issues, virus attacks, SPAM issues or other unforeseen circumstances.

5. **Measurement.** PatientLock uses a proprietary system to monitor and measure whether the Services have met the Service level metrics below and Customer agrees that this system will be the sole basis for resolution of any dispute that may arise between Customer and PatientLock regarding this Statement of Work. PatientLock's measurement system includes log files, database records and audit logs. PatientLock will make information PatientLock uses to validate Customer's claim available to Customer upon request.

6. **Service Level Metrics - Measured on A Calendar Month Basis.**
   a. **Availability**. The service level metric for availability is 99.99%.

   b. **Mail Delivery Time**. The service level metric for Mail Delivery Time is an average of 3 minutes or less, subject to the exclusions defined in Downtime Minutes above and the following:
      Exclusions:
      i. Delivery of email to quarantine.
      ii. Delay associated with third party software (e.g., Microsoft Office 365).
      iii. Customer configuration rules for SPAM/AV or DLP.
      iv. Initial 30 days immediately following deployment of PatientLock's Anti-Virus Service.

   c. **Inbound SPAM.** The Service level metric for inbound SPAM detection is 99.5%
      Exclusions:
      i. Not applicable to false negatives to invalid mailboxes.
      ii. Customer is using less than PatientLock's deployed default settings for SPAM and virus protection.

   d. **Anti-Virus Service.** The Service level metric for Anti-Virus Service is 100%.
      Exclusions:
      i. Cases of self-infection by the Customer.
      ii. Binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware).
      iii. Virus-infected email that is quarantined but is subsequently delivered to an end user or administrator by releasing the message.
      iv. Emails containing attachments that are password protected, encrypted or otherwise under an end users control.
      v. The infection was determined to originate from a source other than inbound corporate email.
      vi. Customer is not employing PatientLock's defined best practices at the time of infection.
      vii. Customer is not blocking or quarantining emails with encrypted compressed contents.
      viii. Customer is not blocking or quarantining known malicious files as defined by PatientLock.

7. **Amount of Service Level Credits.**
   Availability:
   Applies to Email Security, Email Content Filtering, Email DLP

Availability	Amount of Credit for Affected Users for Affected Month
< 99.99% but ≥ 99.00%	25%
> 97.00% but < 99.00%	50%
< 97.00%	100%

Mail Delivery Time:

Applies to Email Security, Email Content Filtering, Email DLP

Mail Delivery Time (Consecutive Minutes Per Test Seat)	Amount of Credit for Affected Users for Affected Month
≥3 minutes but <10 minutes	25%
≥10 minutes but <15 minutes	50%
≥15 minutes	100%

Inbound SPAM Detection:

Applies to Email Security, Email Content Filtering, Email DLP Detection

SPAM Detection	Amount of Credit for Affected Users for Affected Month
<99.5% but ≥ 98.00%	10%
>95.00% but <98.00%	50%
<95.00%	100%

If SPAM is included with the mailbox, then the credit for SPAM will be 10% of the per mailbox monthly charge based on the table above.

Anti-Virus Service:

Applies to Email Security, Email Content Filtering, DLP, Anti-Virus Service

Virus Filtering	Amount of Credit for Affected Users for Affected Month
<100%	35%

8. **Remedy and Procedure.** Customer's sole remedy and the procedure for obtaining Customer's remedy in the event that PatientLock fails to meet the service level metrics set forth above are as follows:

Customer must notify PatientLock in writing at supportdb@silversky.com of both the date the Downtime Minutes occurred and an estimate of the amount of actual Downtime Minutes within five business days of PatientLock's failure to meet the service level metrics ("Claim Notice"). PatientLock will confirm the information provided in the Claim Notice within five business days of receipt of the Claim Notice. If PatientLock cannot confirm the failure to meet the service level metrics, then Customer and PatientLock agree to refer the matter to executives at each company for resolution. If PatientLock confirms that PatientLock is out of compliance with this Statement of Work, Customer will receive the amount of Service Level Credits above for the affected Service level metric and the affected Users for the affected month, which will be reflected in PatientLock's invoice to Customer in the month following PatientLock's confirmation of the failure.

Service Order Attachment for
Email Protection Services - Social Engineering Protection

1. Email Protection Services - Social Engineering Protection Services. "Email Protection Services - Social Engineering Protection Services" provided under this Attachment will mean Email Protection Services ("EPS") - Social Engineering Protection ("SEP") including Email Security (SPAM and antivirus protection), Email Content Filtering, Email Data Loss Protection ("DLP") and Targeted Attack Protection or as may be further described in the *Service Order*. PatientLock will provide end users authorized by Customer to receive Email Protection - Social Engineering Protection Services (each a "User") with the Email Protection - Social Engineering Protection Services on the domain name(s) Customer specifies to PatientLock, provided that Customer owns the domain name(s). PatientLock will provision Customer's specified domain names and Users on or before the date PatientLock first makes Email Protection - Social Engineering Protection Services available to Customer ("Launch Date"). Additional domain names may be established thereafter.

2. Administrators. Prior to the Launch Date, Customer will appoint up to three administrators, each of whom will have the power to act as Customer's agent, with the authority to make decisions and give notices on Customer's behalf ("Administrators") and whose instructions and representations PatientLock may rely on. Administrators' authority includes, but is not limited to (i) controlling the creation and deletion of Users and domain names; (ii) managing changes to User information (such as changes to User name or password); (iii) serving as PatientLock's authorized technical contact for the Email Protection - Social Engineering Protection Services; (iv) setting business rules/policies and/or filters on the Email Protection - Social Engineering Protection Services that may filter and/or terminate emails sent to or by Users without delivering them; (v) and (vi) instructing PatientLock with respect to Data Sampling as further described in Section 10 below. At least one Administrator must attend a training session on the Email Protection - Social Engineering Protection Services, which PatientLock will provide at no charge. Customer may replace Administrators at any time upon written notice to PatientLock.

3. Technical Support. Customer will have sole responsibility for handling technical support inquiries from Customer's Users. PatientLock will have responsibility for responding to inquiries from Customer's Administrators regarding Email Protection - Social Engineering Protection Services. PatientLock will respond to inquiries from Customer's Administrators on a 24x7 basis; provided that inquiries (i) must be submitted via toll-free telephone or email in the English language, and (ii) such inquiries will be responded to in English.

4. Term and Termination. This Attachment will be in effect during the Initial Term set forth in the *Service Order* and will thereafter automatically renew for a period equal to the initial term as provided in the *Service Order*. The fee schedule listed in the *Service Order* will be subject to annual pricing adjustments. However, such pricing adjustments may not exceed 5%, on an annualized basis, during the Initial Term. Intention not to renew must be provided at least 60 days prior to the beginning of the renewal term. The sections related to Payment Terms, Limitation of Liability, Warranties, Indemnity, Confidentiality and Intellectual Property from the General Terms and Conditions, as provided in the referenced General Terms and Conditions document, will survive the expiration or termination of this Attachment for any reason. Within 10 days after the expiration or termination of this Attachment for any reason, Customer must pay all undisputed fees accrued and unpaid at the time of termination, and the cancellation fee if applicable.

5. Fees. Customer will pay PatientLock the fees set forth in the *Service Order* for Email Protection - Social Engineering Protection Services Customer purchase. PatientLock will invoice Customer for Email Protection - Social Engineering Protection Services according to the Service and PatientLock's established billing cycle.

6. Additional Disclaimers. PatientLock does not guarantee continuous, uninterrupted, virus-free, malware-fee or secure Email Protection - Social Engineering Protection Services, and PatientLock is not liable if Customer or Customer's Users are unable to access the Email Protection - Social Engineering Protection Services at any specific time. PatientLock does not guarantee that PatientLock will be able to replace any of Customer's information, content or other data that may be lost, damaged or stolen resulting from use of the Email Protection - Social Engineering Protection Services. PatientLock does not guarantee the effectiveness of the Email Protection - Social Engineering Protection Services against cyber threats or attacks.

7. Additional Terms. The following terms will apply to the Email Protection – Social Engineering Protection Services provided under this Attachment. These additional terms and conditions constitute Customer's instructions to PatientLock to manually sample emails sent to or from Users to help PatientLock improve the performance of the Email Protection - Social Engineering Protection Services to Customer as described below. Customer may revoke these instructions at any time by following the opt-out process detailed below.

a. **Data Sampling.** PatientLock will manually sample randomly selected emails sent to or from Users during the initial 180 days following the Launch Date ("Sampling Period") so that PatientLock may monitor and optimize the performance and effectiveness of the Email Protection - Social Engineering Protection Services to Customer ("Data Sampling"). A limited and controlled population of PatientLock or PatientLock's Affiliates' personnel will be provided with automatically randomly selected emails (up to no more than 200 per day across all customers' emails processed through the Email Protection - Social Engineering Protection Services) for the sole purpose of monitoring and optimizing the performance and success rate of the analytics model deployed by the Email Protection - Social Engineering Protection Services, including by improving its detection ability (the "Purpose").

b. During the Data Sampling Period, an Administrator may, in accordance with provisions below, revoke Customer's instructions to perform Data Sampling. The Administrator may instruct PatientLock to stop Data Sampling with respect to any or all Users by using the sampling toggle switch (i.e., Social Engineering Sampling) on the Account Details page of the administration portal (the "Sampling Selector").

c. The parties acknowledge that Customer Non-Public Personal Information (NPI) a may be included in such randomly selected emails.

d. Excluding any User(s) opted out by Customer's Administrators, Customer warrant that Customer's Administrators, acting on Customer's behalf, are and will at all relevant times remain effectively authorized to give the instructions set out above on behalf of Customer and all Users.

e. PatientLock shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Customer NPI, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

f. PatientLock shall cease processing the Customer NPI within 90 days upon the termination or expiration of this Services Order Attachment or, if sooner, the Service to which it relates and, subject to the preceding subsection, as soon as possible thereafter delete the Customer NPI from PatientLock's systems.

g. PatientLock may retain or disclose Customer NPI to the extent required by applicable laws.

Statement of Work for Email Protection Services – Social Engineering Protection Services

PatientLock is committed to providing a scalable and highly available solution through the following service commitment.

1. **Service Level Availability Calculation**

$$\text{Availability} = \frac{\text{Total Monthly Minutes} - \text{Maintenance Minutes} - \text{Downtime Minutes}}{\text{Total Monthly Minutes} - \text{Maintenance Minutes}} \times 100\%$$

2. **Term of the Statement of Work.** This Statement of Work becomes applicable to the Services upon the later of (a) completion of a mutually agreed upon stabilization period (if applicable), or (b) 30 days from the Launch Date.

3. **Defined Terms.** For the purposes of this Statement of Work, the following terms shall have the following meanings:

   a. "Available" or "Availability" means that the Customer is able to access the Service via the specific access method for that Service subject to the exclusions defined in Downtime Minutes below.

   b. "Downtime Minutes" means the total number of minutes that Customer's end users cannot access the specific Service via the normal access method for that Service. The calculation of Downtime Minutes excludes time a Service is not Available due to any of the following: (i) the Maintenance Minutes; (ii) Customer's or Customer's end users' own Internet service provider; (iii) a Force Majeure event; (iv) any systemic Internet failures; (v) (vi) third party encrypted email Services; (vii) any failure in Customer's or Customer's end users' own hardware, software or Network connection, (viii) Customer's or Customer's end users' bandwidth restrictions, (ix) Customer's or any of Customer's end users' acts or omissions; (x) Customer configure Customer's email system to function as Open Relay; (xi) unavailability of Customer's primary email service; and (xii) and each Service-specific additional exclusion stated below.

   c. "Filter" means to detect and block or quarantine all email messages with viruses that (i) match against available/known virus signatures or (ii) identifiable by industry standard heuristics.

   d. "Mail Delivery Time" means the time elapsed between entry of an email to PatientLock's gateway and its exit.

   e. "Maintenance Minutes" means the time period during which the Services will not be Available (i) each month so that PatientLock can perform routine maintenance to maximize the performance of the Services, up to 240 minutes (4 hours) per Service per calendar month, and (ii) any emergency maintenance PatientLock deems necessary in PatientLock's sole discretion.

   f. "Maintenance Windows" means the scheduled time period during which PatientLock might perform routine maintenance each week. Current Maintenance Windows are Thursday from 10PM to Friday 5 AM Mountain Time. PatientLock may change Maintenance Window at any time. PatientLock will use reasonable efforts to notify Customer in advance of any changes to PatientLock's normal Maintenance Windows.

   g. "Network" means the network outside of PatientLock's border routers.

   h. "Open Relay" means an email server configured to receive email from an unknown or unauthorized third party and forward the email to one or more recipients who are not users of that email system. PatientLock reserves the right at any time during the supply of the Services to test whether the Customer's email systems function as an Open Relay. If at any time the Customer's email systems are found to function as an Open Relay, then PatientLock reserves the right to suspend all or part of the Services immediately and revoke SLA credit requests until the problem has been resolved.

   i. "Total Monthly Minutes" means the number of days in the month multiplied by 1,440 minutes per day.

   j. "Virus" means a known binary or executable code whose purpose is to gather information from the infected host, change or destroy data on the infected host, or use inordinate system resources in the form of memory, disk space, or network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host's system resources.

4. **Maintenance Notices.** PatientLock will communicate the date and time that PatientLock intends to make Services unavailable through a global "welcome message" or an email sent to Customer's Administrator at least 24 hours in advance or longer, if practical. Customer understands and agrees that there may be instances where PatientLock needs to interrupt the Services without notice in order to protect the integrity of the Services due to security issues, virus attacks, SPAM issues or other unforeseen circumstances.

5. **Measurement.** PatientLock uses a proprietary system to monitor and measure whether the Services have met the Service level metrics below and Customer agree that this system will be the sole basis for resolution of any dispute that may arise between Customer and PatientLock regarding this Statement of Work. PatientLock's measurement system includes log files, database records and audit logs. PatientLock will make information PatientLock uses to validate Customer's claim available to Customer upon request.

6. **Service Level Metrics - Measured on A Calendar Month Basis.**
   a. **Availability**. The service level metric for availability is 99.99%.

   b. **Mail Delivery Time**. The service level metric for Mail Delivery Time is an average of 3 minutes or less, subject to the exclusions defined in Downtime Minutes above and the following:
      Exclusions:
      i. Delivery of email to quarantine.
      ii. Delay associated with third party software (e.g., Microsoft Office 365).
      iii. Customer configuration rules for SPAM/AV or DLP.
      iv. Initial 30 days immediately following deployment of PatientLock's Anti-Virus Service.

   c. **Inbound SPAM.** The Service level metric for inbound SPAM detection is 99.5%
      Exclusions:
      i. Not applicable to false negatives to invalid mailboxes.
      ii. Customer is using less than PatientLock's deployed default settings for SPAM and virus protection.

   d. **Anti-Virus Service.** The Service level metric for Anti-Virus Service is 100%.
      Exclusions:
      i. Cases of self-infection by the Customer.
      ii. Binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware).
      iii. Virus-infected email that is quarantined but is subsequently delivered to an end user or administrator by releasing the message.
      iv. Emails containing attachments that are password protected, encrypted or otherwise under an end users' control.
      v. The infection was determined to originate from a source other than inbound corporate email.
      vi. Customer is not employing PatientLock's defined best practices at the time of infection.
      vii. Customer is not blocking or quarantining emails with encrypted compressed contents.
      viii. Customer is not blocking or quarantining known malicious files as defined by PatientLock.

7. **Amount of Service Level Credits.**
   Availability:
   Applies to Email Security, Email Content Filtering, Email DLP

Availability	Amount of Credit for Affected Users for Affected Month
< 99.99% but ≥ 99.00%	25%
> 97.00% but < 99.00%	50%
< 97.00%	100%

Mail Delivery Time:

Applies to Email Security, Email Content Filtering, Email DLP

Mail Delivery Time (Consecutive Minutes Per Test Seat)	Amount of Credit for Affected Users for Affected Month
≥3 minutes but <10 minutes	25%
≥10 minutes but <15 minutes	50%
≥15 minutes	100%

Inbound SPAM Detection:

Applies to Email Security, Email Content Filtering, Email DLP Detection

SPAM Detection	Amount of Credit for Affected Users for Affected Month
<99.5% but > 98.00%	**10%**
>95.00% but <98.00%	**50%**
<95.00%	**100%**

If SPAM is included with the mailbox, then the credit for SPAM will be 10% of the per mailbox monthly charge based on the table above.

Anti-Virus Service

Applies to: Email Security, Email Content Filtering, DLP, Anti-Virus Service

Virus Filtering	Amount of Credit for Affected Users for Affected Month
<100%	35%

8. **Remedy and Procedure.** Customer's sole remedy and the procedure for obtaining Customer's remedy in the event that PatientLock fails to meet the service level metrics set forth above are as follows:

Customer must notify PatientLock in writing at supportdb@silversky.com of both the date the Downtime Minutes occurred and an estimate of the amount of actual Downtime Minutes within five business days of PatientLock's failure to meet the service level metrics ("Claim Notice"). PatientLock will confirm the information provided in the Claim Notice within five business days of receipt of the Claim Notice. If PatientLock cannot confirm the failure to meet the service level metrics, then Customer and PatientLock agree to refer the matter to executives at each company for resolution. If PatientLock confirms that PatientLock is out of compliance with this Statement of Work, Customer will receive the amount of Service Level Credits above for the affected Service level metric and the affected Users for the affected month, which will be reflected in PatientLock's invoice to Customer in the month following PatientLock's confirmation of the failure.