ATTACHMENT A - MDR AGREEMENT

CRITICAL**START**, Inc. ("CRITICAL**START**" or "MDR") is a Texas based corporation located at 6851 Communications Parkway, Plano, Texas 75024. The following describes CRITICAL**START**'s Service Level Agreements and Managed Security Service Provider terms and conditions for any organization ("Customer") using CRITICAL**START**'s Managed Security Services or Managed Detection and Response Services ("Services").

This CRITICAL**START** Managed Security Services Provider Agreement ("MSSP Agreement") incorporates all terms and conditions from the CRITICAL**START** Master Services Agreement ("MSA"), which can be found at https://www.criticalstart.com/resources/legal/msa. If the Customer and CRITICAL**START** have executed a separate MSA ("Customer MSA"), then the MSSP Agreement incorporates all terms and conditions from the valid Customer MSA. Terms and conditions of the MSSP Agreement take precedence over the Customer MSA in the event of conflicting terms and conditions.

CRITICALSTART AND CUSTOMER RESPONSIBILITIES

INVESTIGATION AND ESCALATION

CRITICAL**START** is responsible for alert detection, analysis, investigation, and escalation. CRITICAL**START** will be responsible for alert analysis and investigation to determine if alerts or security events warrant alert classification. If one or more events are classified as an alert, the MSSP will escalate the alert to the Customer. The Customer is responsible for responding to escalated alerts and comments in order to resolve escalated alerts. MSSP staff will perform alert triage to include determining categorization and prioritization of the alert.

CRITICAL**START** will investigate all initial security alerts identified in our Zero-Trust Analytics Platform ("ZTAP") and escalate alerts as appropriate in accordance with the established and agreed upon Service Level Agreements ("SLAs"). After events and alerts are investigated, the MSSP will escalate alerts requiring action by the Customer. The MSSP will follow established escalation paths and utilize contact information collected during the on-boarding process, as mutually agreed by the Customer and CRITICAL**START**. It is the responsibility of the Customer to ensure that their contact information is correct in ZTAP.

For alerts that are assigned to the Customer after analysis, the Customer is responsible for escalating alerts back to the MSSP that require action or analysis by the MSSP. As events are pulled into the MSSP workflow, it is the MSSP's responsibility to create and classify alerts. As the MSSP is responsible for alert escalation and response, only the MSSP has the authority to classify events or alerts as alerts to ensure due diligence of event investigation and accountability in reporting.

Additional responsibilities of the MSSP include:

- Produce internal reports on security activity and MSSP workload metrics to include events ingested, alerts created, alerts escalated, and metrics around alert management. Additionally, reporting can include other pre-determined metrics around alert categorization, priority, and SLAs.
- Assist in identifying potential impact of alerts on customer systems and using data from our Services to assist customer in determining if data was exfiltrated.
- Create and review playbooks to automate classification of false positives and events that Customer has determined do not require escalation. Playbooks are Security Orchestration Automation Response features within ZTAP that automate classification and routing of security events.
- Escalate alerts to identified customer contacts for clarification and/or remediation.

ZERO-TRUST ANALYTICS PLATFORM

CRITICAL**START** will provide Security Orchestration Automation and Response capabilities using ZTAP. This capability will provide event reduction, supervised learning, alert workflow and alert orchestration. Task ownership underneath the function of security event orchestration is outlined below using a RACI Model.

CAPABILITY	CUSTOMER	PROVIDER
Event Collection	RCI	A
API Integrations	CI	RA
Event Storage and Retention	CI	RA
Filter, Feed, and Orchestration Development and Tuning	CI	RA
Alert Workflow & Notifications	CI	RA
Alert Orchestration	CI	RA
System Maintenance, Health and Performance	I	RA
Reporting and Metrics Development	CI	RA

SERVICE-LEVEL AGREEMENTS

SLA SUMMARY

NAME	DESCRIPTION	SLA
SOC MSSP Portal Availability and Notification Systems SLA	CRITICAL**START** will provide access to ZTAP and associated notification systems with the exception of "Scheduled and Emergency Portal Maintenance". ZTAP Portal availability shall be measured by the number of minutes in the month minus the number of minutes the system is unavailable during the month (adjusted for any scheduled downtime) divided by the total number of minutes in the month x 100.	99.9%
Individual Security Event Investigation SLA – Time to Detection (TTD)	Upon ZTAP receiving an event that creates an alert, the CRITICAL**START** CYBER**SOC** will begin investigation within the given timeframe after delivery to ZTAP. The SLA timeframe in minutes is automatically calculated by ZTAP and annotated in the audit log. This is measured by taking the difference between creation of the alert as shown in the ZTAP audit log and when the alert is either assigned to a CYBER**SOC** analyst, escalated to the Customer, or a determination is made that escalation to the Customer is not required.	60 minutes SLA Miss is available in Portal and MOBILE**SOC** app. Timeframe for SLA measurement is 7 days. Timeframe for SLA credit is one month.

Monthly Median Alert Resolution Time SLA (MTTR)	Time to Respond (TTR) measures the total amount of time to investigate an alert after the last event is added (t=0). This includes the delay to begin investigation (TTD) plus the total time spent for investigation and either escalation to the Customer or a determination is made that escalation to the Customer is not required. For a monthly basis, MTTR will be calculated as shown in ZTAP or in the MOBILESOC app.	60 minutes MTTR available in ZTAP and the MOBILESOC app
Executive Summary Reports	A quarterly executive report will be delivered via email in Microsoft Word document format. This report will include all high-level summary information for the corresponding period. Customer can schedule automatic reports on a more frequent schedule if desired in ZTAP.	Quarterly

SLA METRICS AND CREDIT

The Monthly Service Fees referenced in the following tables excludes the service fees for any vendor product licenses and implementation services.

As the sole remedy for failure to meet any of the guarantees described in the section entitled "CRITICALSTART SOC Services SLA Guarantees", CRITICALSTART, Inc. will credit the Customer's account if CRITICALSTART fails to meet the applicable SLA guarantees during a given calendar month.

If CRITICALSTART fails to meet these guarantees for any 8 to 24-hour period, the Customer account will be credited the applicable charges for one day of the management fee for that specific service. The Customer may obtain no more than one credit for each SLA per day.

Customer will receive credit for any failure to meet the Service Level outlined above within thirty (30) days of notification by Customer to CRITICAL**START** of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to CRITICAL**START** within forty-five (45) days of such failure.

ZTAP MSSP PORTAL AVAILABILITY AND NOTIFICATION SYSTEMS SLA: 99.9%

SYSTEM AVAILABILITY	CREDITS DUE CUSTOMER
99.8%-99.99%	No Credit Due
99.5%-99.79%	1% of the Monthly Service Fee
99.0-99.49%	3% of the Monthly Service Fee
98.5-98.99%	5% of the Monthly Service Fee
Less than 98.5%	10% of the Monthly Service Fee

INDIVIDUAL SECURITY EVENT INVESTIGATION SLA (TTD): 60 MINUTES

NUMBER OF ALERTS IN A 7-DAY PERIOD NOT ASSIGNED, CATEGORIZED, OR ESCALATED WITHIN SLA TIMEFRAME	CREDITS DUE CUSTOMER
10 or less	No Credit Due
11-20 Alerts	5% of the Monthly Service Fee
21 or More	10% of the Monthly Service Fee

CALENDAR MONTH MEDIAN ALERT RESOLUTION TIME SLA (MTTR): 60 MINUTES

MEDIAN TIME TO RESOLVE (MTTR) MEASURES THE AMOUNT OF TIME TO RESOLVE AN ALERT, INCLUDING THE DELAY TO BEGIN INVESTIGATION PLUS THE TOTAL TIME SPENT FOR INVESTIGATION AND EITHER ESCALATION OR CLOSE.	CREDITS DUE CUSTOMER
MTTR > SLA for Calendar Month	15% of the Monthly Service Fee

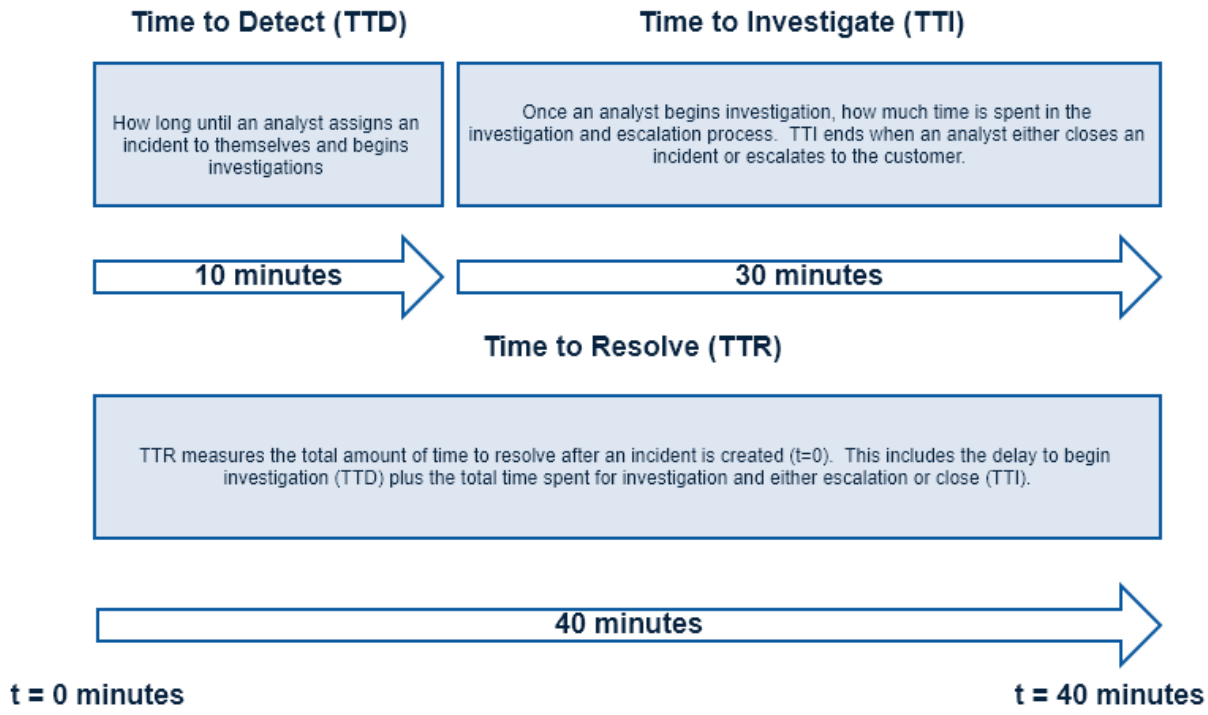
EFFECTIVE DATE OF SLA FOR MONITORING SERVICES

CRITICALSTART SLA's establish response time objectives and countermeasures for Security Alerts. The SLA's become effective when the deployment process has been completed, the devices and security controls have been set to "live", and support and management of the devices and security controls have been successfully transitioned to MSSP Services.

The Customer will be notified in writing or via email that MSSP services have transitioned from deployment phase to full production monitoring. SLA's do not apply for beta, proof of concept, testing, implementation, and deployment phases of the Services, and remedies will not be payable if SLA(s) are not met.

The Customer is responsible for responding to escalated alerts and comments in a reasonable timeframe in order to resolve open alerts and create playbooks to remove future false positives. 3 working days from when an alert is escalated to the Customer is considered a reasonable timeframe. SLA's do not apply during periods of time when the Customer is not responding to multiple requests to resolve open alerts and potential false positives.

EXAMPLE OF HOW INDIVIDUAL ALERT METRICS ARE CALCULATED



CREDIT PAYMENT

Customer will receive credit for any failure to meet the SLA Metrics outlined above within thirty (30) days of notification by Customer to CRITICALSTART of such failure. In order for Customer to receive a Service Level credit, the notification of the Service Level failure must be submitted to CRITICALSTART within forty-five (45) days of such failure. CRITICALSTART will research the request and respond to Customer within thirty (30) days from the date of the request. The total amount credited to a Customer in connection with any of the above Service Levels in any calendar month will not exceed the monthly Service fees paid by Customer for such Service. Except as otherwise expressly provided hereunder or in the Agreement, the foregoing Service credit(s) shall be Customer's exclusive remedy for failure to meet or exceed the foregoing Service Levels.

If Customer pays the Fees annually in advance the credits due to Customer shall be paid to Customer in one of the following methods:

1. Credit to be applied to the next applicable invoice for the annual fees, or
2. In the form of a check to be paid to Customer within thirty (30) days after request by Customer

FILE ANALYSIS SUBMISSIONS AND ENDPOINT ISOLATION

CRITICAL**START** conducts dynamic and static analysis of unknown binaries and unknown files to improve analysis, detection and response to security threats that may impact customer environments. This enables our analysts to provide more in-depth analysis and context to their investigations of potential alerts, as well as enhancing the detection and prevention of future alerts that may involve the same file and/or binary.

Part of this new process may require our analysts to upload unknown binaries and/or files detected in Customer environments to dynamic sandbox and/or static analysis services such as VirusTotal and Palo Alto Networks WildFire ("WildFire"). VirusTotal ("VirusTotal") is owned by Chronicle Security Ireland Limited ("CISL"), an Irish Limited Company with registered number 507502, which is owned by Chronicle LLC, which is owned by Google's parent company Alphabet. At no point will Customer data and/or information be publicly exposed by the MSSP in this process.

CRITICAL**START** MSSP also has the ability to isolate machines on a Customer's network that have a supported endpoint EDR or endpoint protection solution as a part of their managed service offering. The MSSP uses host isolation to prevent the spread of malicious code by preventing a compromised machine from communicating to other network devices on the Internet or the Customer's network. If supported by the solution, the isolated machine will maintain connectivity to our MSSP and allow our analysts to continue investigation without risking other network devices to malicious code or active attacks.

Unless Customer opts-out of File Analysis Submissions and Isolation services then CRITICAL**START** will upload potentially malicious files for analysis as needed and isolate endpoints that investigation proves are potentially compromised.

TERMS AND CONDITIONS FOR FILE ANALYSIS SUBMISSIONS

By allowing permission for the MSSP to upload unknown binaries, CRITICAL**START** MSSP servers will either manually or automatically upload unknown binaries to dynamic sandbox and/or static analysis services such as VirusTotal and WildFire:

- Each binary and/or hash and/or file metadata, as the case may be, will be submitted to VirusTotal and/or WildFire.
- Terms of Service and Privacy Policy of VirusTotal and/or WildFire will apply for each Customer.
- The MSSP shall not be responsible for this submission or for any act or omission by any online service.

You are hereby advised (i) VirusTotal makes the metadata publicly available along with scan results from dozens of anti-virus products and (ii) VirusTotal also makes the files available to VirusTotal partners. WildFire privacy policies are available at https://www.paloaltonetworks.com/resources/datasheets/wildfire-privacy-datasheet or directly from Palo Alto Networks.

TERMS AND CONDITIONS FOR ISOLATIONS

Unless the Customer opts-out, CRITICALSTART will isolate potentially compromised machines. CRITICALSTART will manually isolate the machine using the endpoint solution and notify Customer of the isolation via the alert write-up procedure for escalation. The machines will remain in isolation until the threat has been remediated or Customer has specifically said they accept the risk and request the MSSP to remove the isolation.

- Customer commits to identifying production impacting servers and assets that are NOT to be isolated unless Customer has given written authorization.
- The MSSP commits to isolating machines that are NOT on the unauthorized list only to prevent the spread of malicious code and lateral movement by suspected attackers.
- The MSSP will escalate all alerts that required isolation to Customer for their visibility and active feedback on the alert.

Customers using EDR and/or endpoint protection solutions are hereby advised that the MSSP has the functionality to isolate machines on your network, that the MSSP has the ability to use this function to protect the network, and that the isolated machines will lose all connectivity to all other devices on the network.

MANAGED SECURITY SERVICES GENERAL PROVISIONS

This CRITICALSTART Managed Security Services General Provisions service description applies to all CRITICALSTART managed security services. These general provisions are in addition to the specific terms and conditions provided in the services descriptions.

CUSTOMER RESPONSIBILITIES

Customer understands that CRITICALSTART's performance of the services is dependent in part on the Customer's compliance with the requirements of this SLA. The Customer understands that it is responsible for timely delivery of the items and information listed in the following sections of this SLA. Additionally, the Customer understands that it must perform the tasks, and provide access to Customer's employees, consultants, business processes, and/or systems as contemplated herein for CRITICALSTART to be able to perform such services efficiently. The following list is required to ensure CRITICALSTART's ability to perform the Services:

- Provide reasonable assistance to CRITICALSTART for performance under this SLA, including helping trouble-shoot technical issues within the Customer's environment as well as any services provided by third-parties to the Customer that may affect the delivery of the Services.

- If applicable, provide a permanent, dedicated connection to support the Services. Customer is responsible for maintaining the functionality of the customer's components of this dedicated connection.
- Provide the necessary technical, license, and service information required for implementation prior to the commencement of Services.
- Develop a network map detailing relevant aspects of Customer's network architecture and delivering it to the CRITICALSTART team for their reference when troubleshooting.
- Provide CRITICALSTART with accurate and up-to-date information including, the name, email, landline, and mobile numbers for all designated authorized Customer Points(s) of Contact.
- Maintaining current maintenance and technical support contracts with Customer's software and hardware vendors for any device affected by this SLA.

CUSTOMER ENVIRONMENT FAILURES OR NON-PERFORMANCE

Customer agrees that CRITICALSTART will not be liable for any failure to provide the Services if such failure is caused by Customer's failure to meet the applicable requirements for each Service. At a minimum, Customer is responsible for ensuring the following environmental failures do not negatively impact the Services:

- Service interruptions, deficiencies, degradations or delays due to any Customer supplied Internet or private access whether provided by Customer or third parties engaged by Customer, or equipment when provided by Customer or third parties engaged by Customer. Failure or deficient performance of Customer-supplied power, equipment, services or systems not provided by CRITICALSTART.
- Customer's election to not release a service component for testing and/or repair and to continue using the service component.
- Customer's failure to adhere to CRITICALSTART recommended configurations on managed or unmanaged equipment that affects the Service.
- Service interruptions, deficiencies, degradations or delays during any period when a service component is removed from Service for maintenance, replacement, or rearrangement purposes by Customers submission without a mutually agreed upon change order form.
- Failure to provide a suitable secure environment for on-premise devices, including, but not limited to, secure mounting/racking, appropriate cooling and air handling, premises secure from theft, loose wires bundled neatly, etc.
- Service interruptions, deficiencies, degradations or delays in Service caused by a piece of equipment, configuration, routing event or technology required to be operative in order to perform under this SLA that is under the management and control of Customer.
- Network, software, or server changes or outages to the managed services environment without reasonable prior notification that significantly impact event volumes. This applies to any assets which may affect the

generation of and/or transmission capability of logs, and events or other activity which is monitored by CRITICALSTART for Security Alerts. If Customer fails to notify CRITICALSTART, SLA remedies due to the identified change or outage do not apply.

TESTING OF MONITORING AND RESPONSE CAPABILITIES

Customer may test CRITICALSTART monitoring and response capabilities by staging simulated or actual reconnaissance activity, system or network attacks, and/or system compromises. Such activities may be initiated directly by Customer or by a contracted third party. This includes newly added assets, software changes, threat intelligence feeds, data feeds, and IOC queries that will substantially increase the alerts generated on a temporary basis. These changes and/or activities should be communicated to CRITICALSTART personnel in advance via electronic or written notice to ensure CRITICALSTART personnel have properly onboarded the new information and that all monitoring and response capabilities are working properly.

SLAs will not apply during the period of such staged activities, and remedies will not be payable if the associated SLA(s) are not met for testing alerts.

SCHEDULED AND EMERGENCY MAINTENANCE

Scheduled maintenance means any maintenance that is performed CRITICALSTART during a scheduled maintenance Window or in which Customer is notified at least five days in advance. Notice of scheduled maintenance will be provided to the Customer.

Emergency maintenance means any non-scheduled, non-standard maintenance required by CRITICALSTART.

No statement in the section of any Services Description entitled "Service Level Agreements" shall prevent CRITICALSTART from conducting emergency maintenance if it is critically necessary for the integrity and security of the Services. During such emergency maintenance, Customer will receive notification within 30 minutes of initialization of the emergency maintenance and within 30 minutes of the completion of the emergency maintenance. CRITICALSTART will be relieved of its obligations under the applicable SLAs during scheduled and emergency maintenance.

SYSTEM SPECIFICATIONS AND STABILITY

CRITICALSTART provisions systems involved in providing the Services to specifications for the purchased user count, number of assets, and volume/type of logs ingested as applicable. CRITICALSTART provides administrative access to

the Customer that allow configuration changes that could impact performance of the Services by exceeding provisioned capacity.

The Customer is fully responsible for all impacts to the Services that are caused by its use of administrative privileges to modify the configurations of tools used to provide the Services. Any outages, troubleshooting or support caused by, or required to maintain stability in the environment will incur additional fees for advanced engineering support at a pre-negotiated rate of $225.00 per hour. Additionally, CRITICALSTART will be released from all Service Level Agreements for provided Services until stability is restored.

After deployment is complete and production monitoring has started, if Customer expands use of the Services in a way that requires CRITICALSTART to provision additional resources to support the new configuration, all additional costs will be invoiced to Customer at similar rates to the existing Services. The Customer also has the option of reverting to a configuration that does not require additional resources.

NETWORK SERVER CHANGE NOTIFICATIONS

Customer is responsible for providing CRITICALSTART advanced notice regarding any network or server changes or outages to the managed services environment. In the event advanced notice cannot be provided, Customer is required to provide CRITICALSTART with notification of changes within seven calendar days of such network or server changes. This applies to any assets which may affect the generation of and/or transmission capability of logs, and events or other activity which is monitored by CRITICALSTART for Security Incidents. Unless otherwise specified in the Services Description, notification is completed by the submission or update of an inquiry ticket through the CRITICALSTART Customer Portal for changes that will be implemented by Customer. For changes that must be implemented by CRITICALSTART, Customer must submit a policy change request ticket. If Customer fails to notify CRITICALSTART as stated above, SLA remedies due to the identified change or outage do not apply.

NETWORK TRAFFIC APPLICABLE TO SLAS

Certain SLAs focus on the prevention, identification and notification of security incidents. Such SLAs assume the traffic has successfully reached CRITICALSTART. CRITICALSTART is not responsible for event(s) that do not reach the Security Operations Center due to the sole fault or delay of the Customer or traffic that does not generate a logged event. If event non-receipt is solely attributable to the acts or omissions of Customer or Customer's employees, agents, contractors, or vendors, or anyone gaining access to Customer's Service by means of Customer's Authorized Users' accounts or equipment, CRITICALSTART cannot be held responsible.

SLA COMPLIANCE AND REPORTING

SLA compliance and the associated remedies are based on functional network environments, Internet and current connectivity. Agents and properly configured servers SLA compliance reporting will be provided through the CRITICALSTART Customer Portal.

CONTRACT CHANGES

If CRITICALSTART agrees to a request for an increase in the number of supported devices, or another change that requires a new order be placed with CRITICALSTART (such as an increase in vulnerability scan frequency), the following terms apply to all devices (including those for which Customer initially contracted). They will be governed by the then-current versions of all applicable documents (for example, the Agreement, the SOW, and the Services Descriptions), and by the contract period(s) will be adjusted so the contract/license expiration dates are the same.

DECOMMISSION OR TURN-DOWN OF SERVICES

If the Services contract is not renewed, Customer will have 90 days from the date of termination or 90 days from the date of contract expiration, whichever occurs first, to request the receipt of archived data. Such requests may be submitted through the CRITICALSTART Customer Portal or via email. In cases where the amount of archived data is deemed by CRITICALSTART to be too excessive to make available by download, CRITICALSTART will store the data on encrypted media and ship it to a location specified by Customer.

If a request is not received within the 90-day period described above, CRITICALSTART will provide final notice to Customer in good faith before permanently destroying all archived data no longer under a valid Services contract.

DATA COMPILATION

Customer consents to CRITICALSTART collecting, gathering and compiling aggregated security event log data to look at trends, and real or potential threats. CRITICALSTART may compile or otherwise combine this security event log data with similar data of other Services Recipients so long as such data is compiled or combined in a manner that will not in any way reveal the data as being attributable to Customer.

REGULATORY SERVICES

CRITICALSTART does not operate as a provider of services regulated by the Federal Communications Commission ("FCC") or state regulatory authorities ("State Regulators") and does not intend to provide any services which are regulated by the FCC or State Regulators. If the FCC or any State Regulator imposes regulatory requirements or obligations on any services provided by CRITICALSTART hereunder, CRITICALSTART may (a) modify, replace, or substitute products at Customer's expense, and/or (b) change the way in which such services are provided to Customer to avoid the application of such requirements or obligations to CRITICALSTART (for example, by acting as Customer's agent for acquiring such services from a third party common carrier).