Effective October 16, 2024. This Service Attachment for Managed Compliance Services supersedes and replaces all prior versions.

Service Attachment for Managed Compliance Services

This Service Attachment is between Provider (sometimes referred to as "we," "us," or "our"), and Client found on the applicable Order (sometimes referred to as "you," or "your,") and, together with the Order, Master Services Agreement, Schedule of Services, and other relevant Service Attachments, forms the Agreement between the parties the terms to which the parties agree to be bound.

The parties further agree as follows:

MANAGED COMPLIANCE SERVICE

Provider will deliver only the Services itemized in the Services section of the Order. The following is a list of available Managed Services. Additional Services may be added only by entering into a new Order including those Services.

Risk Assessment

- Conduct a comprehensive risk assessment to identify and evaluate potential risks to the privacy and security of non-personal and protected information ("NPI"), including risks associated with information collection, storage, transmission, and disposal.
- Develop a risk-management plan to address and mitigate identified risks, including prioritizing risks based on their likelihood and potential impact on Client's operations and customer information.

Information Security Program Development

- Develop and implement a written information security program (WISP) that is tailored to Client's specific needs, size, and complexity.
- Establish and maintain appropriate administrative, technical, and physical safeguards to protect the privacy and security of NPI, including access controls, encryption, firewalls, secure disposal procedures, and staff training.

Privacy Notice and Policy Development

- Draft and maintain privacy notices and policies that include providing customers with clear and conspicuous notice of Client's privacy practices and customers' right to opt-out of certain information sharing.
- Review and update privacy notices and policies regularly to ensure they accurately reflect Client's current practices and comply with applicable laws and regulations.

Employee Training and Awareness

© Scott & Scott, LLP

- Develop and implement an ongoing employee training program to educate staff on compliance requirements, policies and procedures, and best practices for protecting customer information.
- Conduct periodic refresher training to ensure employees remain knowledgeable about requirements and any changes to policies and procedures.

Vendor Management

- Establish and maintain a vendor management program to ensure that third-party service providers who have access to NPI are also complying with the requirements
- Review and negotiate contracts with service providers to include appropriate provisions related to privacy and data security, and monitor their compliance with such provisions.

Incident Response and Breach Notification

- Develop and implement an incident response plan to detect, contain, and remediate potential security incidents involving NPI.
- Provide guidance on breach notification requirements and other applicable laws, and assist in coordinating breach notifications to affected customers and regulatory authorities as necessary.

Ongoing Compliance Monitoring and Support

- Conduct periodic reviews and audits of Client's information security program, privacy notices, and policies to ensure ongoing compliance with regulatory requirements.
- Provide ongoing support and guidance on regulatory compliance issues, including updates on regulatory developments, best practices, and industry trends.

Reporting and Documentation

- Provide regular reports to the Client detailing the status of the Managed Compliance Services, including the progress of risk mitigation activities, employee training completion rates, and vendor compliance assessments.
- Maintain up-to-date documentation of the Client's WISP, risk management plan, privacy notices, and policies, ensuring that they remain current and accurate in light of changes to the Client's business or regulatory environment.

ADDITIONAL CLIENT OBLIGATIONS

In addition to the obligations in the Master Services Agreement and other terms and conditions, Client has the following obligations.

Project Coordination

Provider will coordinate with the appropriate contractors and Client representative to ensure the below are completed appropriately.

Ultimate Responsibility for Compliance

Client acknowledges and agrees that, while Provider will use its best efforts to assist Client in complying with the information technology aspects of regulatory rules, Client remains ultimately responsible for its own compliance with all applicable laws, regulations, and industry standards.

© Scott & Scott, LLP

Client shall cooperate with Provider in good faith to implement, maintain, and monitor the necessary safeguards, policies, and procedures to ensure compliance with other relevant regulations.

Access to Information and Facilities

Client shall provide Provider and its authorized personnel with timely and reasonable access to Client's facilities, systems, equipment, and network necessary for the Provider to perform the Services in accordance with the terms and conditions of this Attachment.

Client shall ensure that Provider's access to Client's facilities and systems complies with the Client's internal security policies and procedures, as well as any applicable laws and regulations.

Cooperation and Assistance

Client shall cooperate fully with Provider in the performance of the Services, including providing any necessary information, documentation, or assistance reasonably requested by Provider.

Client shall designate a representative or representatives to serve as the primary point(s) of contact with Provider for all matters relating to the Services. Client's representative(s) shall have the authority to make decisions and provide any necessary approvals on behalf of Client.

Compliance with Laws and Regulations

Client shall comply with all applicable laws, regulations, and industry standards relating to the protection and privacy of (NPI).

Client shall obtain and maintain any necessary permits, licenses, or approvals required for Provider to perform the Services.

Proper Use and Care of Systems and Equipment

Client shall use and operate systems and equipment related to the protection and privacy of NPI in accordance with applicable guidelines, recommendations, and instructions provided by Provider.

Client shall take all reasonable precautions to prevent damage, misuse, or unauthorized access to the systems and equipment.

Notification of Issues or Concerns

Client shall promptly notify Provider of any issues, concerns, or problems relating to the Services, including any non-conforming services, security incidents, or system malfunctions.

Data Backup and Security

Client is responsible for regularly backing up and securing its data and content stored on or transmitted through systems related to the protection and privacy of NPI. Client shall implement appropriate data protection measures, including encryption, access controls, and firewalls, to safeguard its data from unauthorized access, loss, or corruption.

Indemnification

© Scott & Scott, LLP

In addition to the indemnification obligations in the Master Services Agreement, Client shall indemnify and hold Provider harmless for any and all defenses, claims, fines, or damages arising out of or related to a regulatory investigation of Client.

Insurance

In addition to the insurance provision in the Master Services Agreement, Client shall also maintain regulatory, privacy, and security insurance coverage.

EXCLUSIONS

Provider is not responsible for failures to provide Services that are caused by the existence of any of the following conditions:

- Compliance with laws, regulations, or standards other than those identified in the relevant Order.
- Any consequences, liabilities, or damages arising from Client's failure to comply with its obligations under this Agreement or applicable laws and regulations.
- Any consequences, liabilities, or damages resulting from Client's misuse, unauthorized access, or modification of systems, equipment, or data provided or managed by Provider.
- Loss or corruption of Client's data or content, including any costs or expenses associated with data recovery or restoration, unless such loss or corruption is directly attributable to Provider's negligence or willful misconduct.
- Any fines, penalties, or regulatory actions imposed on Client by governmental or regulatory authorities, unless such fines, penalties, or regulatory actions result directly from Provider's failure to perform the Services in accordance with this Attachment and applicable laws and regulations.
- Any consequences, liabilities, or damages resulting from Client's failure to implement or maintain appropriate data backup, disaster recovery, or business continuity measures.
- Any consequences, liabilities, or damages resulting from the actions or inactions of third-party service providers or vendors engaged by Client, unless such actions or inactions are directly attributable to Provider's negligence or willful misconduct.
- Any consequences, liabilities, or damages arising from Client's failure to inform the Provider of changes to its business operations, systems, or processes that could affect the Services or Client's compliance with the relevant regulations.
- Provider is not responsible for any downtime, service interruptions, or performance issues resulting from factors beyond its reasonable control, including but not limited to natural disasters, power outages, network issues, or other unforeseen events.

DISCLAIMER OF WARRANTY

Provider does not warrant that the services will meet the requirements of financial or regulatory auditors, and Provider will not issue a certification of compliance.

TERM AND TERMINATION

Term

© Scott & Scott, LLP

This Service Attachment is effective on the date specified on the Order (the “Service Start Date”). Unless properly terminated by either party, this Attachment will remain in effect through the end of the term specified on the Order (the "Initial Term").

Renewal

"RENEWAL" MEANS THE EXTENSION OF ANY INITIAL TERM SPECIFIED ON AN ORDER FOR AN ADDITIONAL TWELVE (12) MONTH PERIOD FOLLOWING THE EXPIRATION OF THE INITIAL TERM, OR IN THE CASE OF A SUBSEQUENT RENEWAL, A RENEWAL TERM. THIS SERVICE ATTACHMENT WILL RENEW AUTOMATICALLY UPON THE EXPIRATION OF THE INITIAL TERM OR A RENEWAL TERM UNLESS ONE PARTY PROVIDES WRITTEN NOTICE TO THE OTHER PARTY OF ITS INTENT TO TERMINATE AT LEAST SIXTY (60) DAYS PRIOR TO THE EXPIRATION OF THE INITIAL TERM OR OF THE THEN-CURRENT RENEWAL TERM. ALL RENEWALS WILL BE SUBJECT TO PROVIDER’S THEN-CURRENT TERMS AND CONDITIONS.

Month-to-Month Services

If the Order specifies no Initial Term with respect to any or all Services, then we will deliver those Services on a month-to-month basis. We will continue to do so until one party provides written notice to the other party of its intent to terminate those Services, in which case we will cease delivering those Services at the end of the next calendar month following receipt such written notice is received by the other party.

Early Termination by Client With Cause

Client may terminate this Service Attachment for cause following sixty (60) days’ advance, written notice delivered to Provider upon the occurrence of any of the following:

- Provider fails to fulfill in any material respect its obligations under the Service Attachment and fails to cure such failure within thirty (30) days following Provider’s receipt of Client’s written notice.
- Provider terminates or suspends its business operations (unless succeeded by a permitted assignee under the Agreement).

Early Termination by Client Without Cause

If Client has satisfied all of its obligations under this Service Attachment, then no sooner than ninety (90) days following the Service Start Date, Client may terminate this Service Attachment without cause during the Initial or a Renewal Term (the “Term”) upon sixty (60) days’ advance, written notice, provided that Client pays Provider a termination fee equal to fifty percent (50%) of the recurring, Monthly Service Fees remaining to be paid from the effective termination date through the end of the Term, based on the prices then in effect.

Termination by Provider

Provider may elect to terminate this Service Attachment upon thirty (30) days’ advance, written notice, with or without cause. Provider has the right to terminate this Service Attachment immediately for illegal or abusive Client conduct. Provider may suspend the Services upon ten (10) days’ notice if Client violates a third-party’s end user license agreement regarding provided software. Provider may suspend the Services upon fifteen (15) days’ notice if Client’s action or inaction hinder Provider from providing the contracted Services.

© Scott & Scott, LLP

Effect of Termination

As long as Client is current with payment of: (i) the Fees under this Attachment, (ii) the Fees under any Project Services Attachment or Statement of Work for Off-Boarding, and/or (iii) the Termination Fee prior to transitioning the Services away from Provider's control, then if either party terminates this Service Attachment, Provider will assist Client in the orderly termination of services, including timely transfer of the Services to another designated provider. Client shall pay Provider at our then-prevailing rates for any such assistance. Termination of this Service Attachment for any reason by either party immediately nullifies all access to our services. Provider will immediately uninstall any affected software from Client's devices, and Client hereby consent to such uninstall procedures.

Upon request by Client, Provider may provide Client a copy of Client Data in exchange for a data-copy fee invoiced at Provider's then-prevailing rates, not including the cost of any media used to store the data. After thirty (30) days following termination of this Agreement by either party for any reason, Provider shall have no obligation to maintain or provide any Client Data and shall thereafter, unless legally prohibited, delete all Client Data on its systems or otherwise in its possession or under its control.

Provider may audit Client regarding any third-party services. Provider may increase any Fees for Off-boarding that are passed to the Provider for those third-party services Client used or purchased while using the Service.

Client agrees that upon Termination or Off-Boarding, Client shall pay all remaining third-party service fees and any additional third-party termination fees.

© Scott & Scott, LLP