EXHIBIT B
SECURITY SCHEDULE AS APPLICABLE

Capitalized terms used in this Schedule but not defined have the meanings set forth in the Agreement.

1. Definitions

1.1. Client Systems means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, licensed or leased by Client, or operated by a third party on behalf of Client, that: (a) connects to or otherwise interacts with Signal Systems; or (b) is enabled or intended to access or interact with Client Data Processed in connection with the Agreement.

1.2. Signal Systems means any computer, computer network, computer application, imaging device, storage device, mobile computing device or software owned, leased or controlled by Signal, or operated by a third party on behalf of Signal, that Processes User Data or is connected to any Client Systems.

1.3. Industry Standards means industry standards and best practices relating to the security of Client Data including, without limitation, industry standards and best practices of Signal's industry and standards and best practices employed by Signal's industry peers.

1.4. Information Security Incident means (a) loss or theft of Client Data; (b) unauthorized use, disclosure, acquisition of or access to, or other unauthorized Processing of Client Data that reasonably may compromise the confidentiality of Client Data; or (c) unauthorized access to, use of, modification of, or inability to access, Client Systems or Signal Systems that reasonably may compromise the confidentiality of Client Data.

1.5. Information Security Program means Signal's technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices, standards and controls that (a) manage the confidentiality, integrity and availability of Client Data; (b) protect against any anticipated threats or hazards to the security of Client Data; and (c) address Information Security Incidents.

1.6. Process or Processing means any operation or set of operations performed upon Client Data, such as accessing, obtaining, storing, transmitting, using, maintaining, disclosing or disposing of the information.

2. Signal's Obligations

2.1. Disclosure of and Access to Client Data

2.1.1. Client Data will be considered Confidential Information of Client under the Agreement.

2.1.2. Prior to providing access to Client Data to any subcontractor, or other third party, Signal shall: (a) conduct a reasonable investigation of such third party to determine that the third party will process the Client Data in a manner that is consistent with, and permits Signal to comply with, the requirements imposed on Signal under this Schedule; (b) contractually impose upon such a third party the same or substantially similar contractual duties imposed on Signal by this Schedule; and (c) contractually secure rights with respect to such third party that enable Signal's compliance with this Schedule.

2.2. Compliance with Security Requirements

2.2.1. Signal shall comply with all Applicable Privacy Laws and Industry Standards.

2.2.2. Signal shall promptly notify Client in writing if Signal determines it cannot comply with its obligations under this Schedule. If this is the case, Client and Signal shall use commercially reasonable efforts to remedy the situation. Client may, in its sole discretion and without penalty of any kind to Client, suspend the transfer or disclosure of Client Data to Signal or access to Client Data by Signal, terminate any further Processing of Client Data by Signal, and terminate the Agreement, if doing so is necessary to comply with applicable Privacy

and Security Laws, is required or requested by a regulator or other governmental body, or Client otherwise believes it is necessary to do so to protect its interests, in its sole discretion.

2.3. Information Security Program

2.3.1. Signal shall develop, maintain and document reasonable technological, physical, administrative and procedural safeguards, including without limitation, policies, procedures, guidelines, practices, standards, controls that (a) manage the confidentiality, integrity, and availability of Client Data); (b) protect against any reasonably foreseeable threats or hazards to the confidentiality, integrity, or availability of Client Data; and protect against any Information Security Incident.

2.3.2. Signal shall conduct information security risk assessments at least annually and whenever there is a material change in the organization's business or technology practices that may impact the confidentiality, integrity or availability of Client Data.

2.3.3. Signal shall maintain a secure method for selecting, assigning, and changing (when appropriate) unique user identification codes and authentication credentials (including passwords, biometrics, or token devices) for individuals who access Client Data and/or Client Systems.

2.3.4. Signal shall maintain procedures to detect, monitor, document and respond to Information Security Incidents.

2.3.5. Signal shall apply Industry Standard cryptographic protections for any Client Data Processed by Signal.

2.3.6. Signal shall maintain commercially reasonable firewalls, or substantially similar technology to limit communications between network zones possessing differing levels of trust, Signal Systems and the Internet (including internal networks connected to the Internet) and other public networks.

2.3.7. Signal shall maintain software that detects, prevents, removes and remedies malicious code designed to perform an unauthorized function on, or permit unauthorized access to, any information system.

2.4. Data Retention and Disposal

2.4.1. When Client Data is no longer necessary for the performance of services for or on behalf of Client, or promptly upon the expiration or earlier termination of the Agreement, whichever is earlier, or at an earlier time as Client requests, Signal shall securely destroy or, at Client's written request, return to Client or its designee, in the format determined by Client, each and every original and copy in every media (including both active data and backup data) of all Client Data in Signal's possession, custody or control. In the event applicable law does not permit Signal to comply with the delivery or destruction of the Client Data, Signal warrants that it shall ensure the confidentiality of the Client Data and that it shall not use or disclose any Client Data after termination of the Agreement, except as required by law. Upon Client's request, Signal shall provide written certification by one of its senior officers that Client Data has been returned or securely destroyed in accordance with this Schedule.

2.5. Periodic Reporting and Assessments

2.5.1. Signal shall notify Client within fifteen (15) business days of discovery by Signal of any security vulnerability that could materially adversely impact the confidentiality, integrity, or availability of Client Data, Client Systems, or Signal Systems. Notice pursuant to this Section shall not be required for security vulnerabilities affecting third party technology that have been remedied by a patch, hotfix, reconfiguration, or workaround within forty-eight (48) hours of discovery by Signal.

2.5.2. Upon the provision of reasonable notice to Signal, (a) following any discovery or reasonable suspicion by Client that Signal is not in compliance with this Schedule or (b) as demanded

or required by any regulator or government body or by Applicable Privacy Laws, Client may retain an independent auditor or reviewer to, or if required a regulator may, undertake a security assessment, network scan, forensic investigation and/or audit of Signal Systems and Information Security Program. Any audit must be limited in scope to a determination of whether Signal is in compliance with this Schedule (or if conducted by a regulator or government body, to whether Signal is in compliance with the Applicable Privacy Laws in question). Audits will be conducted at Signal's offices, during regular business hours, and in a manner that does not unreasonably interfere with the conduct of business in the ordinary course by Signal. Client will be responsible for the cost of any audit conducted under this provision, unless it is found that Signal is in fact not in compliance with this Schedule (or Applicable Privacy Laws, as the case may be), in which case, Signal will reimburse Client for the costs of the audit (subject to a cap of $2,500).

2.6. Information Security Incident Response

2.6.1. Signal shall notify Client within forty-eight (48) hours of any Information Security Incident. Such notice shall summarize in reasonable detail the effect on Client, if known, of the Information Security Incident and the corrective action taken or to be taken by Signal

2.6.2. In the event of an Information Security Incident, Signal shall:

2.6.2.1. Conduct a reasonable investigation of the reasons for and circumstances of the Information Security Incident.

2.6.2.2. Use best efforts and promptly take all necessary actions to rectify, prevent, contain and mitigate the impact of the Information Security Incident, and remediate the Information Security Incident; provided that if such remediation shall reasonably cause a material adverse impact to Client Data or Signal's ability to provide services pursuant to the Agreement, Signal shall obtain Client's written consent prior to undertaking such remediation.

2.6.2.3. Collect, preserve and document all evidence regarding the discovery and cause of, and vulnerabilities, response, remedial actions and impact related to the Information Security Incident, using means that shall meet reasonable expectations of forensic admissibility; and provide such documentation to Client upon request.

2.7. Cooperation and Information Requests

2.7.1. Signal agrees to reasonably cooperate and coordinate with Client concerning: (a) Client's investigation, enforcement, monitoring, document preparation, notification requirements, efforts to prevent and mitigate, and reporting concerning Information Security Incidents; and (b) any other activities or duties set forth under this Schedule for which cooperation between Signal and Client may be reasonably necessary.

3. Notices

3.1. The following individuals shall be the primary contacts at Client and Signal for any coordination, communications or notices with respect to Client Data, this Schedule, or any Information Security Incident: Signal: Adam Van Dyk, Director of Legal, avandyk@signal.co; and security@signal.co; Client: the contact(s) listed in the applicable Order Form. Each party shall promptly notify the other if any of the foregoing contact information changes.

4. Miscellaneous

4.1. This Schedule is the part of the Agreement and is the complete agreement between Signal and Client and supersedes any prior oral or written agreement between the parties concerning the security of Client Data.

4.2. Signal's obligations and Client's rights set forth in this Schedule shall continue as long as Signal, or any third party acting on Signal's behalf, processes Client Data, including after expiration or termination of the Agreement.