

CREDENTIAL WATCHER

1. Credential Watcher Services:

- 1.1. Following completion of the service activation process described below, and subject to the Client responsibilities outlined below, BlueVoyant will search for evidence of compromises of credentials related to corporate email domains and email-addresses of key-personnel of Client in the open, deep, and dark web, as well as criminal instant messaging groups.
- 1.2. When a Client credential compromise is detected, a report is generated detailing the compromised credentials, the threat actors responsible for the compromise, and the platforms where they are operating (when available), as well as such other relevant information as BlueVoyant may determine. If a detected Client credential compromise involves a malicious domain or sub-domain, the report will also include actionable information such as the domain name, IP and registration details of that domain/sub-domain.
- 1.3. Reports are made available for Client to access via Wavelength™, BlueVoyant's secure communication portal, which is accessible over the Internet through a web browser.
- 1.4. When a report is ready, an email notification is generated alerting Client to the waiting report.

2. Credential Watcher Service Levels:

- 2.1. **Service Availability:** Subject to the maintenance windows noted below, searches for compromised credentials are conducted 24 hours a day, 7 days a week.
- 2.2. **Report Generation:** BlueVoyant will generate a report on discovery of a compromised credential within 30 minutes of detection.

2.3. Maintenance Windows:

- 2.3.1. **System Maintenance:** System maintenance-related service outages may occur from time to time. BlueVoyant will provide Client with 24-hours' notice of any such outage.
- 2.3.2. **Emergency System Maintenance:** Emergency system maintenance may occur. To the extent it does, BlueVoyant will use commercially reasonable efforts to provide notice and to minimize the impact to service delivery.

-
- 2.3.3. **Service Levels During Maintenance Windows:** Service levels shall not apply during maintenance outages and therefore are not eligible for any service level credit during these periods.
- 2.4. **SLA Credits:** Client will receive service credits for any failure by BlueVoyant to meet the service levels specified above within thirty (30) days of notification by Client to BlueVoyant of such failure. Upon receipt of an SLA failure notification, BlueVoyant will research the request and respond to Client within thirty (30) days from the date of the request. The total amount credited to Client in connection with any of the above service levels in any calendar month will not exceed the monthly services fees paid by Client for such services. Except as otherwise expressly provided hereunder or in the relevant Master Services Agreement, the foregoing service level credit(s) shall be Client's exclusive remedy for failure to meet or exceed the applicable service levels.
3. **Credential Watcher Service Activation:** Credentials Watcher service activation consists of three phases: introduction, provisioning, and tuning. Service activation begins with entry into a BlueVoyant order form and associated Master Services Agreement, and ends with the activation of the Credential Watcher service.
- 3.1. **Introduction Phase:** The introduction phase consists of a service kickoff meeting. Either during or immediately following the service introduction meeting, Client will provide BlueVoyant with a list of (a) corporate and key-personnel email addresses to search for, and (b) Client's authorized users and their contact information.
- 3.2. **Provisioning Phase:** During the provisioning phase, BlueVoyant will provide Client's authorized users with Wavelength™ credentials, and will configure multi-factor authentication for those users. BlueVoyant will also conduct Wavelength™ training for Client's authorized users.
- 3.3. **Tuning Phase:** As part of the tuning phase, BlueVoyant will work with Client over a 14 day period to hone BlueVoyant's searches such that the output of those searches is optimized for visibility and accuracy.
4. **Client Responsibilities:**
- 4.1. **Notification of Credentials, Authorized Users, Changes:** During the introduction phase Client will promptly provide BlueVoyant with a list of (a) the corporate domain or key-personnel email addresses Client would like monitored, and (b) Client's authorized users and their contact information. Thereafter, Client will

promptly notify BlueVoyant of any changes to those credentials and/or authorized user changes.

- 4.2. **Confidentiality of Wavelength™ Credentials:** Client must ensure that Client's authorized users take appropriate steps to protect the confidentiality of the usernames, passwords, and other information necessary to access Wavelength™.
- 4.3. **Notification of Lost or Compromised Credentials:** Client will promptly notify BlueVoyant of any lost or compromised authorized user credentials.
- 4.4. **Software, Hardware, Equipment:** Client is responsible for obtaining and maintaining all software, hardware and/or other equipment necessary for its authorized users to access Wavelength™ over the Internet through a web browser. This responsibility includes keeping Internet access security features up to date.

5. **Additional Terms and Conditions:**

- 5.1. **Suspension of Wavelength™ Access:** BlueVoyant reserves the right to suspend or terminate Wavelength™ access for any authorized user whose account shows signs of suspicious activity. In such a situation, Client typically will be notified so that BlueVoyant can verify the activity with Client. All Wavelength™ activity is logged in order to preserve all of the information necessary to validate the transmission of data.
- 5.2. **Modification of Terms:** BlueVoyant reserves the right to modify the terms of this statement of work, including the service levels, with 30 days prior notice.