BRAND PROTECTION SERVICE

1. Brand Protection Services:

1.1. Web Impersonation (Anti-Phishing Detection):

1.1.1. Following completion of the service activation process described below, and subject to the Client responsibilities outlined below, BlueVoyant will search open source and proprietary data sets for malicious Internet domains and sub-domains that mimic monitored Client brand names, logos, trademarks, service marks, and corporate domains and sub-domains.

1.1.2. When a malicious domain or sub-domain is detected, a report is generated and sent to the client. Reports include actionable information such as the domain name, IP and registration details.

1.1.3. BlueVoyant will conduct ongoing monitoring of inactive suspicious domains and sub-domains and alert when it discovers phishing campaigns go live.

1.2. App Impersonation (Rogue Application Detection):

1.2.1. Following completion of the service activation process described below, and subject to the Client responsibilities outlined below, BlueVoyant will search official and unofficial app-stores for rogue applications, both for mobile devices and desktops, that resemble monitored Client brand names, logos, trademarks and service marks.

1.2.2. When a rogue app is detected, a report is generated and sent to the client. Reports include actionable information such as the application URL link and screenshot.

1.3. Social Media Impersonation (Fake Social Media Accounts Detection):

1.3.1. Following completion of the service activation process described below, and subject to the Client responsibilities outlined below, BlueVoyant will search social media for fake profiles, pages and groups that utilize monitored Client brand name, logos, trademarks and service marks for fraudulent purposes. Additionally, BlueVoyant will search social media for fake accounts that impersonate key-personnel of Client.

1.3.2. BlueVoyant cover Facebook, Twitter, Instagram and LinkedIn platforms.

1.3.3. When a fake profile, page or group is detected, a report is generated and sent to client. Reports include actionable information such as the URL of the fake account and screenshot.

1.4. 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.

1.5. In addition, upon request from Client, BlueVoyant personnel will engage with the relevant entities on the Client's behalf and provide actionable information that helps speed the take-down process. Once the removal of an impersonation attack is confirmed, the Client is notified via Wavelength™.

2. Brand Protection Service Levels:

2.1. Service Availability: Subject to the maintenance windows noted below, searches for phishing websites and domains are conducted 24 hours a day, 7 days a week. Searches for rogue applications and fake social media accounts are conducted Sunday through Friday during the hours of 09:00 am through 5:00 pm Israel time, with the exclusion of holidays.

2.2. Report Generation: BlueVoyant will generate a report on discovery of a malicious domain/sub-domain within 1 (one) hour of detection. Reports on rogue applications and fake social media accounts will be generated within 24 hours of detection.

2.3. Take Down Requests: Take-Down service requests will be acknowledged through email or the BlueVoyant ticketing system, and an abuse complaint will be sent to the relevant entities within 6 (six) hours from acknowledgement.

2.4. Maintenance Windows:

2.4.1. 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.

2.4.2. 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.

2.4.3. 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.

2.5. 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. Brand Protection Service Activation: Brand Protection 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 Brand Protection 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) Client brand names, logos, trademarks, and service marks, and (b) corporate domains and sub-domains to monitor, and (c) Client's legitimate applications, and (d) Client's legitimate official social media pages and key-personnel profiles, and (e) 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 brand names, logos, trademarks, service marks, and (b) corporate domains and sub-domains Client would like monitored, and (c) Client's legitimate applications, and (d) Client's legitimate official social media pages and key-personnel profiles, and (e)

Client's authorized users and their contact information. Thereafter, Client will promptly notify BlueVoyant of any changes to those details.

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.