RECEIVED
By Office of the Commission Secretary at 4:53 pm, Jun 12, 2019

GARVEY SCHUBERT BARER
A PROFESSIONAL SERVICE CORPORATION

WASHINGTON, D.C. OFFICE
flour mill building
1000 potomac street nw
suite 200
washington, d.c. 20007-3501
TEL 202 965 7880 FAX 202 965 1729

OTHER OFFICES
seattle, washington
portland, oregon
new york, new york
beijing, china
GSBLAW.COM

Please reply to DANIEL A. PETALAS
dpetalas@gsblaw.com
Direct Dial 202 298 1791

June 12, 2019

VIA EMAIL

Lisa J. Stevenson
Acting General Counsel
Federal Election Commission
1050 First Street NE
Washington, DC 20463

Re: Advisory Opinion Request—Area 1 Security, Inc.

Dear Ms. Stevenson:

On behalf of Area 1 Security, Inc. ("Area 1") we request an advisory opinion under 52 U.S.C. § 30108 of the Federal Election Campaign Act of 1971, as amended (the "Act"). We request confirmation that Area 1 may offer its anti-phishing cybersecurity services, on a non-partisan basis, to election-sensitive organizations, including but not limited to federal candidates and political committees, at little to no cost, based on commercial and not political considerations, consistent with Area 1's current business practices and without violating the Act.

1. Foreign Cyber Actors Are Phishing for Highly-Prized Political Targets

Foreign cyber actors have interfered with elections in the United States and around the world. There will be more cyberattacks throughout the 2020 election cycle in the United States.[1] While much of the public discourse surrounding cybersecurity and elections has focused on social media influence and the integrity of voting systems, the greatest risk to electoral integrity is phishing attacks that target federal candidates and political committees.

A phishing attack is an attempt to mislead the user of a computer to take an action that unwittingly causes harm. That action could be the downloading of a file, clicking on a link, visiting a website, completing an

[1] *See* Daniel R. Coats, Director of National Intelligence, *Statement for the Record*, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (Jan. 29, 2019), *available at* https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

online form, or transferring sensitive data. The result of these actions can include installation of malware, theft of credentials, loss of data, theft of intellectual property and financial assets, and brand and reputation damage. Nine in ten cybersecurity breaches world-wide begin with phishing.

It takes only a single click by an individual at an election-sensitive organization to erode a foundational element of our democracy: free and fair elections.

- During the 2016 election cycle, foreign cyber actors launched phishing attacks against election-sensitive organizations. These included state boards of election, secretaries of state, the Democratic Congressional Campaign Committee (DCCC), the Democratic National Committee (DNC), and Hillary Clinton's Campaign.[2]

- During the 2018 election cycle, foreign cyber actors continued launching phishing attacks against election-sensitive organizations. These included political candidates, think tanks, and non-profits.[3]

- In the current 2020 election cycle, foreign cyber actors have already targeted election-sensitive organizations via phishing attacks.

Foreign cyber actors targeting election-sensitive organizations begin and intensify their attacks in concert with campaign milestones. These milestones include announcements of candidacy, FEC filing deadlines, debates, caucuses, primaries, and other major campaign milestones. The risk of damage increases as candidates gain momentum, expand their staffs, and get closer to election day.

Federal candidates and political committees are at a significant risk of phishing.[4] They assemble quickly and have limited resources to protect themselves. They employ a variety of full-time and part-time

---

[2] *See United States v. Netyksho*, No. 1:18-cr-00215-ABJ (D.D.C. filed Jul. 13, 2018), *available at* https://www.justice.gov/file/1080281/download.

[3] *See* Brad Smith, *We Are Taking New Steps Against Broadening Threats to Democracy*, MICROSOFT (Aug. 20, 2018), *available at* https://blogs.microsoft.com/on-the-issues/2018/08/20/we-are-taking-new-steps-against-broadening-threats-to-democracy; Natalie Andrews, *McCaskill Says Senate Office Was Target of Phishing Scam*, WALL ST. J. (July 26, 2018), *available at* https://www.wsj.com/articles/mccaskill-says-senate-office-was-target-of-phishing-scam-1532656049; Andy Kroll, *Documents Reveal Successful Cyberattack in California Congressional Race*, ROLLING STONE (Aug. 15, 2018), https://www.rollingstone.com/politics/politics-news/california-election-hacking-711202/.

[4] *See* Jeff Stein, *Exclusive: Russian Hackers Attacked the 2008 Obama Campaign*, NEWSWEEK (May 12, 2017), *available at* https://www.newsweek.com/russia-hacking-trump-clinton-607956; Dan Goodin, *Russia's Cozy Bear Comes Out of Hiding with Post-Election Spear-Phishing Blitz*, ARSTECHNICA (Nov. 19, 2018), *available at* https://arstechnica.com/tech-policy/2018/11/russian-hackers-suspected-of-launching-post-election-spear-phishing-party/; Adam Segal, *Will China Hack the U.S. Midterms?*, NY TIMES (Oct. 5, 2018), *available at* https://www.nytimes.com/2018/10/05/opinion/china-cyberattack-hacking-us-midterm-election.html.

employees, consultants, and volunteers on their staff who operate in multiple places of business, extending the impact of attacks to a larger network of organizations.

2. Area 1 Security Corporate Background

Area 1 has developed the most imaginative, comprehensive, and effective solution for eliminating phishing attacks.

The company is a privately-held corporation, owned principally by its employees and a group of private investors. Area 1 is not owned in any degree by any federal candidate or political committee. Area 1 has fewer than 100 employees, does not engage in lobbying, and retains no lobbyists or lobbying firms. Before founding Area 1, its co-founders worked in senior computer science and computer security positions at the National Security Agency and United States Cyber Command.

Area 1 has developed the industry's only preemptive and comprehensive solution to stop phishing, the root cause of damage in 95% of all cybersecurity incidents. Unlike the ineffectiveness of email gateways, anti-spam filters, and awareness programs, Area 1's solution preemptively tracks phishing campaigns in their formative stages and comprehensively stops them before they arrive in email in-boxes and give hackers access to sensitive information, causing damage.

Area 1's software is 100% cloud-based and takes advantage of the unlimited elasticity that the cloud provides. The ability to scale the service up or down on demand enables Area 1 to protect any new customers, regardless of size. Implementation of Area 1's software requires very little effort on the part of limited campaign technology staff, particularly important in the early stages of a campaign.

Area 1 has built distinctive technology that can protect any organization in the world that wants protection from phishing and the ensuing damages phishing causes. Area 1 believes that cybersecurity should be accessible to every organization that is at risk of being phished and that desires to protect itself. This protection is particularly critical for political campaigns targeted by hostile and technologically sophisticated foreign actors.

3. Area 1's "Little to No Cost" Pricing Strategy

Area 1's pricing strategy is called Pay Per Phish. Under Pay Per Phish, the client pays $10 per phish that the company catches, with a non-negotiable predetermined cap or maximum for budgetary control. The predetermined cap or maximum is determined by the number of employees at an organization. Some clients prefer a negotiated fixed fee structure under an Enterprise License Agreement approach in lieu of the performance-based pricing afforded by Pay-Per-Phish, which can variably fluctuate monthly. Under Enterprise License Agreement pricing, clients negotiate fixed-term contracts and pay a fixed amount up front to use the product for the duration of that contract.

Area 1's commercial team directly engages organizations that have more than 5,000 employees.[5] When an organization has fewer than 5,000 employees and provides a significant opportunity to improve its research and development initiatives, Area 1 offers a "little to no cost" pricing tier. Clients in the "little to no cost" tier are non-profits, humanitarian organizations, and startups. They pay an annual rate of $1,337 or less.[6] Presently, Area 1 works with a significant number of non-political clients in the "little to no cost" tier.

4. Application to Federal Candidates and Political Committees

Area 1 proposes to offer anti-phishing cybersecurity services to federal candidates and political committees on a nonpartisan basis within its established "little to no cost" pricing tier.[7] Federal candidates and political committees eligible for the "little to no cost" pricing tier would have fewer than 5,000 employees.

Moreover, and very significantly to Area 1, in providing anti-phishing solutions to federal candidates and political committees, Area 1 expects to gain essential, highly valuable research and development benefits. Foreign cyber actors specifically target federal candidates and political committees with unique phishing campaigns unlikely to be seen by commercial customers for some time. Area 1 would gain highly valuable insight into new attack methodologies and other valuable threat intelligence data and would advance its product in the most challenging threat environment available. Area 1 firmly believes that experience would enhance its product for all of its clients as a result, with direct commercial benefits for the company.

Area 1 seeks an advisory opinion to clarify to federal candidates and political committees that they can accept the company's services in the "little to no cost" tier without violating the Act or Commission regulations.[8]

---

[5] "Employees" refers to the number of full-time employees who have an email account at the client.

[6] To be clear, Area 1 views $1,337 as a negligible amount, consistent with its "little to no cost" pricing strategy. It selected that amount because "1337" is a numerical transposition of "leet," a term referring to an "elite" hacker or computer coder.

[7] To be clear, for non-political clients that qualify for "little to no cost" pricing, Area 1 charges between zero and $1,337 per year. Area 1 exercises discretion in selecting that price. However, Area 1 will charge all federal candidates and political committees that qualify for the "little to no cost" pricing tier the same fee of $1,337 per year.

[8] The presidential debates in late June 2019 may trigger more attacks. Area 1 respectfully requests a decision as quickly as possible. The company would be pleased to forego a hearing to the extent a favorable decision by tally vote may be available.

Very truly yours,

GARVEY SCHUBERT BARER, P.C.

By 

Daniel A. Petalas