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

GARVEY SCHUBERT BARER
A PROFESSIONAL SERVICE CORPORATION

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

April 9, 2019

VIA EMAIL AND U.S. MAIL

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

Re: Advisory Opinion Request—Area 1 Security

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 specific 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 business practices, prior advisory opinions, and without violating the Act.

FACTUAL BACKGROUND

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, and 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

[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.

an 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 only takes 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 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 *See United States v. Netysksho*, 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.

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, or awareness programs, Area 1's solution preemptively tracks phishing campaigns in their formative stages and comprehensively stops them before they cause 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. Area 1 offers accountability-based pricing determined by the number of phishing attacks it stops and organization size.[5]

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. Cybersecurity should be accessible to everyone who is at risk of being phished and who desires to take action. As such, Area 1 often provides its product at little to no cost to support organizations with limited financial resources and limited full time professional cybersecurity staff. These clients present a significant research and development opportunity, and Area 1 feels proud when it provides the world's best cybersecurity to organizations that cannot protect themselves from cyberattackers otherwise.[6]

3. Proposed Activities Relating 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. Area 1 would apply its standard commercial strategy, where federal candidates and political committees may qualify for services at little to no cost. Area 1 seeks an advisory opinion to provide clarity to federal candidates and political committees that they can accept Area 1's services and stay in compliance with the Act.

---

5 *See* Shannon Vavra, *New Cybersecurity Business Model: Pay-Per-Phish*, AXIOS (Oct. 23, 2018), *available at* https://www.axios.com/company-area-1-tries-breaking-up-overwhelming-cybersecurity-market-ab01cb23-9372-4037-b370-a32f03aefcf8.html.

6 *See* JON KATZENBACH, WHY PRIDE MATTERS MORE THAN MONEY (Crown 2003).

Area 1's standard commercial strategy considers the client's financial resources, the research and development opportunity, the time duration of a client relationship, and the pride factor. Area 1 will inform federal candidates or political committees of the company's offerings. The company expects that federal candidates and political committees will immediately grasp the value proposition, as Federal candidates and political committees know they are receiving phishing attacks by foreign cyber actors, and they are concerned about avoiding the damages that have plagued candidates in prior election cycles.

One element of the company's standard pricing strategy considers a client's financial resources. Federal candidates and political committees do not have financial resources to spend on cybersecurity products. Area 1 would provide services to these resource-constrained clients at *de minimis* cost.

Area 1 further considers the research and development opportunity associated with protecting a client. In providing anti-phishing solutions to federal candidates and political committees, the company would gain valuable research and development benefits, which is particularly significant in the context of servicing highly vulnerable federal candidates and political committees.

As part of Area 1's standard pricing strategy, the company considers the longevity of a given client relationship. Area 1's products are today in use by the largest global corporations in the world. These commercial business transactions are defined to go on for years. When Area 1 engages federal candidates and political committees, it does so understanding that the longevity of these client relationships are inherently time bound to election day.

Area 1's commercial strategy also considers pride. When an organization presents a unique opportunity to motivate Area 1's employees, the company will make commercial pricing considerations. Federal candidates and political committees are now getting targeted by sophisticated and creative foreign cyber actors. The potential hacking of U.S. elections is a high-visibility problem. It would give Area 1's employees a greater sense of pride to solve this problem. Pride is linked to intrinsic motivation. When employees feel greater intrinsic motivation—i.e., motivation other than money—they are happier and more productive. As a small company in a fiercely competitive technology field, the effect of pride on its employees is a critical element of Area 1's business strategy.

These factors—client resources, research and development, client longevity, and pride—lead Area 1 to price our services for federal candidates and political committees at little to no cost. Area 1 therefore seeks an advisory opinion to signal that federal candidates and political committees can accept our services at little to no cost and stay in compliance with the Act.

QUESTION PRESENTED

May Area 1 offer specific anti-phishing cybersecurity services at little to no cost to federal candidates and political committees on a nonpartisan basis and on consistent terms as its similarly situated nonpolitical clients without making a prohibited, in-kind contribution under the Act?

LEGAL ANALYSIS

Area 1 intends to provide cybersecurity services to federal candidates and political committees at little to no cost, consistent with its business practices and for purely commercial, non-political reasons. This proposal is consistent with the Act and Commission regulations and the Commission's prior advisory opinions on related matters. As explained below, Area 1's proposed offerings for federal candidates and political committees are based on commercial considerations, not political considerations. This would not result in an impermissible corporate in-kind contribution. Moreover, the proposal presents no corruption risks. And Area 1 would advance a key priority of the Commission by preventing foreign interference in our country's democratic processes during a time of exceptional vulnerability. We therefore respectfully request confirmation that Area 1's plan with respect to federal candidates and political committees complies with federal campaign finance law.

The Act and Commission regulations prohibit, with certain exceptions, corporations from making contributions to federal candidates, political party organizations, and political committees that make contributions to federal candidates and political party committees.[7] A "contribution" is limited to things of value that are provided "for the purpose of influencing any election for Federal office."[8] For corporations, a "contribution" also includes any "direct or indirect payment, distribution, loan, advance, deposit, or gift of money, or any services, or anything of value . . . in connection with any [federal] election."[9] "Anything of value" includes all in-kind contributions, such as the provision of goods and services without charge or at a charge that is less than the usual and normal charge.[10] The "usual and normal charge" for services is the commercially reasonable prevailing rate at the time the services were rendered.[11]

The Commission has recognized that "a corporation's *bona fide* commercial activity is neither 'for the purpose of influencing any election for federal office' nor 'in connection with any election' and thus is

---

7 52 U.S.C. §§ 30118(a), (b)(2); 11 C.F.R. § 114.2(b).

8 52 U.S.C. § 30101(8)(A)(1).

9 *Id.* § 30118(b)(2); *see id.* § 30101(8)(A)(i); 11 C.F.R. §§ 114.2(b), 100.52(a).

10 *See* 11 C.F.R. § 100.52(d)(1).

11 *Id.* § 100.52(d)(2).

not a contribution or otherwise subject to regulation under the Act."[12] Consequently, "corporations may charge lower rates to political committees without being considered to have made a prohibited in-kind contribution as long as the rate structure 'reflects commercial considerations and does not reflect considerations outside of a business relationship.'"[13] In Advisory Op. 2018-11, the Commission addressed the proposal of Microsoft Corporation ("Microsoft") to provide without charge an enhanced suite of cybersecurity services to certain "election sensitive" customers. Those recipients included federal, state, and local candidate committees, national and state political party committees, campaign technology vendors, and think tanks and democracy advocacy nonprofits.[14] Microsoft's proposed free corporate services included providing cybersecurity training materials and potentially offering training in-person, investigating and notifying clients about account targeting or breaches by nation-state actors, and providing technical support services by email and telephone to secure targeted accounts and remediate breaches. The specific suite of additional free services proposed in the request were not made available to all Microsoft clients as such, but similar free services were available from Microsoft to various clients.[15]

The Commission approved the request, concluding that the free services were offered based on nonpolitical, commercial considerations. The Commission cited five such factors in support of its determination: (1) the proposal afforded Microsoft the ability to protect its brand reputation from damage

---

12 Advisory Op. 2014-06 (Ryan) at 9.

13 Advisory Op. 2018-11 (Microsoft Corp.) at 4 (quoting Advisory Op. 2012-31 (AT&T) at 4). The Commission's recent activity is consistent with its long-standing recognition, from the inception of the agency's operations, that the Act's prohibition on corporate in-kind contributions to federal candidates, political committees, and other regulated political groups does not preclude those groups from receiving the same commercial discounts and complimentary services that service providers otherwise make available, for commercial reasons in their business judgment, to similarly-situated, non-political customers or potential clients across a wide variety of circumstances and factual settings. *See, e.g.*, Advisory Op. 2018-05 (CaringCent) (approving charge of different fees to political committee clients from charges to nonpolitical clients where variation based on business and not political considerations); Advisory Op. 2012-26 (m-Qube II) (concluding no in-kind contribution where lower rates applicable to political committees "reflected commercial considerations"); Advisory Op. 2006-01 (Pac for Change) (purchase of books at a discount permissible if discount available in the ordinary course of business and on same terms and conditions offered to other non-political customers); Advisory Op. 1994-10 (Franklin National Bank) (recognizing that a political committee can obtain goods or services at a discount or complimentary if available to others on equal terms); Advisory Op.1989-14 (Anthony's Pier 4) (discounts given in ordinary course of business to political and nonpolitical customers alike are permissible); Advisory Op. 1988-25 (GM) (loaning fleets of GM vehicles without charge to nominating conventions was consistent with practice of making vehicle fleets available without charge to other nonpolitical conventions and thus not a prohibited corporation contribution to nominating conventions); Advisory Op. 1987-24 (Hyatt) (hotel corporation offering discounted or complimentary rooms to federal candidates permissible if on same terms made available to nonpolitical customers); Advisory Op. 1987-27 (Bell Atlantic Corp.) (special designation of corporate employees to manage telephone service accounts of presidential campaigns permitted because those services were also normally provided to certain other, nonpolitical "high-volume" customers); Advisory Op.1976-86 (McDonald) (no contribution to continue to display billboard political advertisement beyond the term of paid rental so long as extended display was consistent with ordinary practice in billboard corporation's business with respect to advertisements of non-political customers).

14 Advisory Op. 2018-11 at 2.

15 *Id.*

if its existing client accounts were hacked; (2) it allowed Microsoft to obtain "highly valuable" data about online security threats; (3) the offering was made on a non-partisan basis; (4) the proposal "resembles" Microsoft's "other commercial offerings" to nonpolitical clients; and (5) the proposal was particularly important "at this time given the public scrutiny regarding foreign attempts to influence U.S. elections."[16]

The Commission's reasoning in the Microsoft decision strongly counsels in favor of approving Area 1's request as well. The first factor in the Microsoft decision is not relevant to Area 1's situation. Microsoft wanted to give free services to pre-existing clients. Area 1 wants to provide services at little to no cost to new clients. The second factor in the Microsoft decision is directly relevant, however. Like Microsoft, Area 1 would benefit significantly from the research and development opportunities presented by providing its services to vulnerable and aggressively targeted federal candidates and political committees. Foreign cyber actors use highly developed methods when targeting federal candidates and political committees. If Area 1 can help those clients, Area 1 would learn from the experience. This opportunity would help Area 1 improve its anti-phishing product in the most challenging testing ground available.

Third, as in AO 2018-11, Area 1 will offer its services on a non-partisan basis. Indeed, the company intends to provide its product to any federal candidate or political committee that is interested.

Fourth, Area 1 will provide services to political clients on the same terms that it now provides similarly situated nonpolitical clients. The service offerings will be identical.

Fifth, Area 1 wants to provide services to federal candidates and political committees who will be targeted by foreign cyber actors. There is broad agreement, bordering on certainty, that federal candidates and political committees will be targeted by phishing attacks in future elections. And many of those attacks, in turn, are sourced in foreign nation-state threat actors. The Area 1 anti-phishing service can harden political targets in the United States against such attacks and enhance the nation's federal election security as a result.

There is also an important distinction between Microsoft and Area 1. Microsoft has a market capitalization of nearly a trillion dollars. Microsoft routinely engages with regulators and politicians on a wide range of issues. For that reason, Microsoft spent nearly $10 million in 2018 and almost $45 million over the last 5 years on federal lobbying alone. Microsoft's corporate political action committee ("PAC") reported $1.5 million in transfers to federal candidates and committees during 2017 and 2018. When a highly-regulated company like Microsoft provides free services to federal candidates and officeholders, that benefit could raise the specter of improper influence on the regulatory process. The sole comment on the Microsoft request recognized that risk.[17] That comment warned that influential companies like Microsoft might offer "below-market rate services to candidates 'to facilitate relationship-building in the service of

16 *Id.* at 4-5.

17 Comments of Campaign Legal Center, Advisory Op. Req. 2018-11 (Sept. 6, 2018).

lobbying efforts.'"[18] Nonetheless, the Commission unanimously approved Microsoft's proposal for the reasons identified. Whatever corruption concerns the Microsoft request might have presented, those concerns are entirely absent here. Area 1 is a startup with fewer than 100 employees. The company does not engage in lobbying, has no corporate PAC, and has no intention of pursuing those activities.

The Commission's reasoning in prior advisory opinions also fully supports Area 1's request. For instance, in Advisory Opinion 2018-05 (CaringCent), the Commission expressly concluded that a for-profit contribution-processing service could provide its services to political committees, even though the requestor proposed to charge "different fees to political committee clients than it charges to non-political clients."[19] The Commission reached that conclusion because counsel for the requestor confirmed that "any variation in fees will be based on business considerations and will not be based on political considerations."[20] Although the requestor did not specify the particular considerations that would be employed when assessing those variances, the Commission correctly concluded that the proposal to apply ordinary commercial "business considerations" to price determinations does not give rise to a prohibited corporate in-kind contribution.[21] Similarly here, Area 1 intends to offer its services to political clients at little to no cost. Under Area 1's normal commercial practices, the company would give its product at little to no cost to similarly situated non-political clients based on the same business assessments.

The Commission has previously considered what may constitute legitimate commercial business considerations in a variety of settings. In addressing provision of cellular and text messaging services to campaigns at lower rates, for example, the Commission concluded in each instance that the proposal was consistent with ordinary commercial practices and not a political contribution. In Advisory Opinion 2012-31 (AT&T), the Commission approved a lower rate structure for political committees that was premised on the volume of anticipated transactions, dollar value of those transactions, and volume of work that processing those transactions would require. Similarly, in Advisory Opinion 2012-26 (m-Qube II), the Commission approved lower rates that were based on the company's assessment of "volume of messages, refund rates, customer satisfaction, and technical level of efforts." In Advisory Opinion 1987-27 (Bell Atlantic Corp.), the Commission approved the provision of centralized service for the exchange of local and long distance telephone services for presidential candidates without charge for centralizing that service, where candidates were made to agree to more stringent terms of eligibility, use, and payment frequency than other telephone customers. Equally so, Area 1 proposes to structure its pricing for federal candidates and political committees using the same commercial considerations it has identified in this request and currently applies to non-political clients that present similar business values.

---

18 *Id.* at 1-2.

19 Advisory Op. 2018-05 at 5 (citing AOR010).

20 *Id.*

21 *Id.*

Area 1's proposal is different from what the Commission rejected in Advisory Opinion 1996-02 (CompuServe). CompuServe wanted to provide free user accounts to enable federal candidates to engage in direct advocacy with voters. Typically, CompuServe charged a fee for user accounts.[22] CompuServe justified its free pricing by claiming that "publicity obtained through such users heightens the company's prestige and goodwill, stimulates usage by existing CompuServe members, and encourages non-members to subscribe to CompuServe."[23] The requestor offered no justification other than the anticipated branding and goodwill. The Commission rejected CompuServe's request, presumably in fear that those criteria taken alone might swallow the rule.

Unlike CompuServe, Area 1's motive is not branding or goodwill. In addition to the other cited business considerations, Area 1's motive is to provide employees an opportunity that would give them a special feeling of pride. Per the earlier discussion, employees at Area 1 would feel particularly proud if they could protect federal candidates and political committees. Pride is linked to the intrinsic motivation of the employee. An employee that feels greater intrinsic motivation is happier and more productive. It would be easier for Area 1 to attract and retain the best talent if the company could give employees this opportunity. Intrinsic motivation is different from branding and goodwill. Branding and goodwill are linked to impressing a customer or bystander. Branding and goodwill are related to marketing. The pride factor is oriented to increasing the employee's intrinsic motivation to work hard every day. If Area 1's employees feel greater intrinsic motivation, the company will be more successful.

In addition, a significant motive for Area 1 is research and development. Area 1's products improve as it encounters more diverse phishing attacks. Federal candidates and political committees present a significant research and development opportunity with unique timing dynamics. Area 1 would encounter phishing methods used by sophisticated cyberattackers. And the challenge would be time-limited in a way that differs from Area 1's typical engagement. The research and development opportunity would be special.

In sum, the Commission should conclude that Area 1's proposal to provide anti-phishing cybersecurity services at little to no cost to federal candidates and political committees is *bona fide* commercial activity, consistent with the Act and Commission regulations. Area 1 would gain a significant research and development opportunity and act consistent with its standard pricing strategy. The Commission has repeatedly found that commercial businesses can give federal candidates and political committees the same discounted and free services they provide to similarly situated non-political clients when justified by legitimate business considerations. Accordingly, recognizing Area 1's ability to proceed as described in this request therefore would not constitute a prohibited in-kind corporate contribution under the Act or Commission regulations.[24]

---

22 Advisory Opinion 1996-02 (CompuServe).

23 *Id.* at 4.

24 *See, e.g.*, Advisory Ops. 2018-11, 2018-05, 2012-31, 2012-26.

CONCLUSION

Area 1 Security has developed the most imaginative, comprehensive, and effective solution for eliminating phishing campaigns available. It now seeks to offer its services to federal candidates and political committees at no cost, as it does certain small nonpolitical organizations, for a host of commercially reasonable and nonpolitical considerations, as described. The Commission has recognized that would not violate the Act in similar circumstances. We respectfully request that the Commission confirm that Area 1 may provide its services at no charge to vulnerable federal candidates and other regulated political committees, on a nonpartisan basis and under the terms it offers similarly situated nonpolitical clients, without making a prohibited, in-kind corporate contribution under the Act.

Please do not hesitate to contact me should you have any questions regarding this request.

Very truly yours,

GARVEY SCHUBERT BARER, P.C.

By
Daniel A. Petalas

cc: Ellen L. Weintraub, Chair
Matthew S. Petersen, Vice Chairman
Caroline C. Hunter, Commissioner
Steven T. Walther, Commissioner