RECEIVED
By Office of the Commission Secretary at 5:30 pm, Jun 03, 2019

FEDERAL ELECTION COMMISSION
Washington, DC 20463

AGENDA DOCUMENT NO. 19-23-B
AGENDA ITEM
For meeting of June 6, 2019
SUBMITTED LATE

June 3, 2019

MEMORANDUM

TO: The Commission

FROM: Lisa J. Stevenson
Acting General Counsel

Neven F. Stipanovic
Acting Associate General Counsel

Robert M. Knop
Assistant General Counsel

Joseph P. Wenzinger
Attorney

Subject: AO 2019-07 (Area 1 Security, Inc.) Draft B

Attached is a proposed draft of the subject advisory opinion.

Members of the public may submit written comments on the draft advisory opinion. We are making this draft available for comment until 9:00 am (Eastern Time) on June 6, 2019.

Members of the public may also attend the Commission meeting at which the draft will be considered. The advisory opinion requestor may appear before the Commission at this meeting to answer questions.

For more information about how to submit comments or attend the Commission meeting, go to https://www.fec.gov/legal-resources/advisory-opinions-process/.

Attachment

ADVISORY OPINION 2019-07

Daniel A. Petalas, Esq.
Garvey Schubert Barer, P.C.
Flour Mill Office Building
1000 Potomac Street, NW #200
Washington, DC 20007-3501

DRAFT B

Dear Mr. Petalas:

We are responding to your advisory opinion request on behalf of Area 1 Security, Inc. ("Area 1"), concerning the application of the Federal Election Campaign Act, 52 U.S.C. §§ 30101-45 (the "Act"), and Commission regulations to its proposal to offer free or low-cost cybersecurity services to federal candidates and political committees. Because Area 1 proposes to deviate substantially from its ordinary business practices by not applying either of its established pricing strategies to federal candidates and political committees, the Commission concludes that its proposal would result in prohibited in-kind contributions and is, therefore, impermissible.

Background

The facts presented in this advisory opinion are based on your letter on behalf of Area 1, received on April 18, 2019.

Area 1 states that it can provide users of computers with "the most imaginative, comprehensive, and effective solution for eliminating phishing attacks." AOR003; *see also id*. (describing Area 1's services as "the industry's only preemptive and comprehensive solution to stop phishing"). A phishing attack allows the aggressor to entice a victim to download a file, click on a link, visit a website, complete a form, or transfer sensitive data, and to cause harm through such actions, such as by downloading malware or stealing or purging

credentials, data, intellectual property, or financial assets. *Id*. Area 1 preemptively tracks phishing threats and stops them before they cause damage. *Id*.

The request describes two different pricing models that Area 1 uses in determining how much to charge potential clients for its services. First, you state that Area 1 employs "accountability-based pricing" and you provide a link to a news article describing this strategy as a "pay-per-phish" model under which clients pay a set fee when Area 1 foils a phishing attempt. AOR 003.[1] Second, for clients that do not agree to the "pay-per-phish" payment arrangement, you state that Area 1 applies a four-factor test (the "four-factor pricing model") to determine the appropriate amount to charge for the company's services. The four-factor pricing model takes into account (1) the strength of a client's financial resources, (2) the potential longevity of a relationship with the client, (3) the opportunity the client presents for research and development of Area 1's products, and (4) the "special feeling of pride" Area 1 would obtain in servicing the client. AOR004, AOR009. You state that applying this four-factor pricing model to its existing client base has "often" resulted in Area 1 providing its anti-phishing services for free or low cost to organizations with limited financial resources and without full-time cybersecurity staff, if it detects enough of a benefit in accepting such clients. AOR003-004.

You state that, in applying the first two factors of Area 1's four-factor pricing model to federal candidates and political committees, Area 1 has determined that such potential clients should receive services at no or little cost because "[f]ederal candidates and political committees do not have financial resources to spend on cybersecurity products," and "[w]hen Area 1 engages

[1] *See* Shannon Vavra, *New Cybersecurity Business Model: Pay-Per-Phish*, AXIOS (Oct. 23, 2018), https://www.axios.com/company-area-1-tries-breaking-up-overwhelming-cybersecurity-market-ab01cb23-9372-4037-b370-a32f03aefcf8.html. At the time of the article, Area 1 was charging $10 per foil. *Id*.

federal candidates and political committees, it does so understanding that the longevity of these client relationships are inherently time bound to election day." AOR004. You further assert that, regarding the research and development opportunity afforded in providing anti-phishing services, federal candidates and political committees provide a particularly valuable opportunity because they are "aggressively targeted" and, if foreign actors used highly developed methods in targeting federal candidates and political committees, Area 1 "would learn from the experience." AOR004, AOR007. Discussing the fourth factor, you assert that Area 1 anticipates benefitting from the "pride" provided by servicing federal candidates and political committees because the potential hacking of such users presents a "high-visibility problem" that, if solved by Area 1's employees, would increase "intrinsic motivation" that, more than money, would make them "happier and more productive." AOR004. Thus, according to the request, "Area 1 would provide resources to [federal candidates and political committees] at *de minimis* cost."[2]

Last, Area 1 represents that it would offer its proposed services on a nonpartisan basis and to enhance the nation's security against foreign interference in American elections, would not take any political considerations into account when determining the price to charge federal candidates and political committees, and would provide its services on the same terms and conditions that apply to similarly situated nonpolitical clients. AOR001, AOR007.

Question Presented

May Area 1 offer anti-phishing services at little to no cost to federal candidates and political committees without making prohibited, in-kind contributions under the Act?

[2] The Commission notes that, in several other areas of the request, you state that Area 1 proposed to provide the services described in the request at *little or no* cost. *E.g.*, AOR001.

Legal Analysis and Conclusions

No. Because Area 1 proposes to deviate substantially from its ordinary business practices by not applying either of its established pricing strategies to federal candidates and political committees, the Commission concludes that its proposal would result in prohibited in-kind contributions.

Under the Act and Commission regulations, corporations may not make "contributions" to federal candidates, political party organizations, and political committees that make contributions to federal candidates and political party committees. 52 U.S.C. §§ 30118(a), (b)(2); 11 C.F.R. § 114.2(b).[3] A "contribution" 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." 52 U.S.C. § 30118(b)(2); *see* 11 C.F.R. § 114.2(b). "Anything of value" includes all in-kind contributions, such as the provision of goods and services to federal candidates and political committees without charge or at less than the "usual and normal charge," defined in context of services as the commercially reasonable prevailing rate at the time the services are rendered. *See* 11 C.F.R. § 100.52(d).

The "usual and normal charge" generally includes goods and services provided to federal candidates and political committees at a discount, as long as such discounts are provided in the ordinary course of business and on the same terms and conditions available to all similarly

[3] The Commission notes that the Act and Commission regulations' prohibition on corporate contributions no longer applies to corporations making contributions to nonconnected political committees that make only independent expenditures, *see*, *e.g.*, Advisory Opinion 2011-11 (Colbert); *Citizens United v. FEC*, 558 U.S. 310 (2010); *SpeechNow.org v. FEC*, 599 F.3d 686 (D.C. Cir. 2010) (*en banc*), and to non-contribution accounts of hybrid political committees, *see* Press Release, FEC Statement on *Carey v. FEC*: Reporting Guidance for Political Committees that Maintain a Non-Contribution Account (Oct. 5, 2011), https://www.fec.gov/updates/fec-statement-on-carey-fec/.

situated non-political clients. *See* Advisory Opinion 2018-11 (Microsoft) at 3 (concluding that Microsoft may provide enhanced online security services at no additional charge on nonpartisan basis to election-sensitive customers, including federal candidates and national party committees); Advisory Opinion 2004-06 (Meetup) at 1 (concluding that corporation may provide federal candidates, political committees, and supporters both free and fee-based online platform for arranging local gatherings). For example, in Advisory Opinion 2018-11 (Microsoft), the Commission permitted Microsoft to provide federal candidates and national parties who were existing, full-paying users of the company's productivity and email services with add-on cybersecurity services at no additional cost. Advisory Opinion 2018-11 (Microsoft) at 1. In reaching this conclusion, the Commission noted Microsoft's existing practice of offering packages and pricing "in the ordinary course of business" to provide additional cybersecurity services at no cost to similarly situated pre-existing customers, including public-sector entities, educational institutions, teachers and students, small and large businesses, start-up companies, and 501(c)(3) non-profit organizations. *Id*. at 3.

Here, Area 1 proposes to deviate substantially from either of the pricing models it applies to its non-political clients by charging an entire category of clients — federal candidates and political committees — little or nothing in return for providing anti-phishing services. Area 1 does not propose to charge such clients according to its price-per-phish model. And although Area 1 purports to have applied its four-factor pricing model to federal candidates and political committees, it essentially omitted the first two factors (the financial resources of the potential client, and the longevity of the potential client relationship) from its analysis in reaching the conclusion that such potential clients should be charged little to nothing in return for the

company's services. Area 1 states broadly that "[f]ederal candidates and political committees do not have financial resources to spend on cybersecurity products," and that "the longevity of these client relationships are inherently time bound to election day," AOR004, ignoring the reality that not all federal candidates and political committees carry the same amount of financial resources or possibility for longevity. By not taking those factors into account, Area 1 would charge federal candidates and political committees, such as those with substantial financial means and those whom it might reasonably expect to develop a profitable long-term relationship, the same as those that do not meet those qualifications.

Although Area 1 claims that its application of its four-factor pricing model to its non-political clients "often" results in its charging little or nothing in return for its services to organizations with limited financial resources and without full-time cybersecurity staff, it applies all four factors of its pricing model to each client in determining the amount to charge them. *See, e.g.* AOR003 (stating that Area 1 provides cybersecurity at little to no cost to "organizations with limited financial resources"). Area 1 makes no representation that it routinely omits taking into account the first two factors of its four-factor pricing model for an entire category of any of its non-political clients. Moreover, because Microsoft had an established practice of providing free cybersecurity services to entire categories of its pre-existing, non-political clients, Advisory Opinion 2018-11 (Microsoft) is inapplicable here. Consequently, the Commission concludes that providing services for little or no charge to federal candidates and political committees is not consistent with Area 1's ordinary business practices and would, therefore, result in Area 1 making impermissible in-kind contributions to those candidates and committees.

This response constitutes an advisory opinion concerning the application of the Act and Commission regulations to the specific transaction or activity set forth in your request. *See* 52 U.S.C. § 30108. The Commission emphasizes that, if there is a change in any of the facts or assumptions presented, and such facts or assumptions are material to a conclusion presented in this advisory opinion, then you may not rely on that conclusion as support for its proposed activity. Any person involved in any specific transaction or activity which is indistinguishable in all its material aspects from the transaction or activity with respect to which this advisory opinion is rendered may rely on this advisory opinion. *See* 52 U.S.C. § 30108(c)(1)(B). Please note that the analysis or conclusions in this advisory opinion may be affected by subsequent developments in the law including, but not limited to, statutes, regulations, advisory opinions, and case law. Any advisory opinions cited herein are available on the Commission's website.

On behalf of the Commission,

Ellen L. Weintraub
Chair