Computer & Communications
Industry Association
Tech Advocacy Since 1972

July 22, 2019

Office of Foreign Assets Control
U.S. Department of the Treasury
1500 Pennsylvania Avenue, NW
Freedman's Bank Building
Washington, DC 20220

Re: Docket No. OFAC-2019-0003; Request for Comments (Amendments to OFAC's Reporting, Procedures, and Penalties Regulations)

Dear sir(s):

I write on behalf of the Computer & Communications Industry Association (CCIA) in response to the interim final rule and request for comment published by the Office of Foreign Assets Control in the Federal Register at 84 Fed. Reg. 29,055 (June 21, 2019). CCIA represents technology product and service providers of all sizes, including hardware and software, electronic commerce, telecommunications and Internet products and services. CCIA members employ more than 750,000 workers and generate annual revenues in excess of $540 billion.

CCIA's comments focus on the revised definitions in the § 501.604 requirements for reporting transactions that have been rejected pursuant to OFAC regulations. In particular, OFAC's apparent expansion of the set of entities who must report and the volume of interactions that must be reported will likely have the unintended consequence of over-burdening firms providing goods or services over the Internet, particularly small and medium-sized enterprises. Because the interim final rule is open to an interpretation in which businesses may be expected to file a large volume of reports containing little meaningful data, CCIA encourages OFAC to withdraw the rule pending further consultation with stakeholders.

At a minimum, OFAC should clarify when the reporting requirement is triggered, and that OFAC did not intend to require that every interaction rejected as a result of a compliance program must be reported to the Treasury Department. In particular, OFAC should clarify that the reporting requirements for rejected transactions in revised § 501.604 do not apply to the following activities: (1) where a party refrains from pursuing or engaging in interactions with or potentially involving a specially designated national (SDN) or other prohibited party; and (2)

where a party refrains from pursuing or engaging in interactions with or potentially involving a person or entity in an OFAC-sanctioned country.

The interim final rule expands the scope of who must report rejected transactions from "financial institutions" to include "any U.S. person". 31 CFR § 501.604(a)(1). At the same time, whereas OFAC previously required reporting of rejected "funds transfers", the interim final rule now refers to reporting of all "transactions" rejected pursuant to the relevant chapter. "Transaction" is defined to include—but is not limited to—"transactions related to wire transfers, trade finance, securities, checks, foreign exchange, and *goods or services*." 31 CFR § 501.604(a)(3) (emphasis supplied). While OFAC's notice indicates the goal is to "lessen the overall reporting burden for submitters", a broad interpretation of these newly revised definitions would substantially burden U.S. e-commerce and service providers with reporting requirements for millions of transactions, and at the same time swamp OFAC with a large volume of reports providing little or no useful information.

For example, pursuant to General License D-1 governing personal communications services, software, and hardware, U.S. persons may export or reexport a variety of personal communications services and related connectivity functions to certain sanctioned territories. Nevertheless, some e-commerce and service providers may, as part of a risk-based compliance strategy, decline to provide services in these and other high-exposure jurisdictions and/or OFAC-sanctioned territories. With respect to a provider of digital services, this approach may, for example, entail an automated refusal to provide access using location-based information (such as an IP address) at the time of interaction or account creation, or it may include blocking ongoing service at a time when an otherwise lawful user travels to a sanctioned jurisdiction. In the latter scenario, the only meaningful "transaction" information that would be available to report to OFAC may be the date, account credentials, and IP address connection information. In the former scenario, the only meaningful "transaction" information would include the date and IP address connection information, since no account would exist, and the availability of this data is predicated upon the assumption that the service provider logs all such refusals. Due to the exceptionally high volume of interactions that digital services process, this may not be the case.

By contrast, OFAC guidance appears to contemplate transactions of a different nature, referring to online remittance and payment services.[1] Similarly, § 501.604(b) requires reporting of variables such as the identity of the persons participating in the transaction, including financial institutions, customers, and their beneficiaries, "a description of the property that is the subject of the transaction," that property's estimated value, and other information likely irrelevant to the provision of digital services. Because little of this data pertains to refused transactions, businesses may be in the burdensome position of regularly filing a large volume of reports that contain little useful data. Moreover, if companies are required to report opportunities that were declined on the advice of in-house or outside counsel, this will compromise attorney-client privilege and force companies to disclose details on proprietary business opportunities that they refused.

The root cause of this potential confusion is the definitional expansions proposed by the interim final rule, which could be construed as transforming economic sanctions restricting the movement of assets, financial instruments, and other property into a general purpose regulation of all cross-border interactions, including digital interactions. The asymmetry between the intended goal of enforcing economic sanctions and the breadth of the interim final rule is particularly evident where the notice indicates that OFAC expects a total number of annual responses in the vicinity of 31,000, when some digital services and applications may routinely refuse far more IP connections than this through the regular operation of their compliance program.

The request for comments suggests that the compliance burden of the interim final rule "is minimal because the records required to be maintained should already be maintained under standard business practice." The expanded definitions, however, may be interpreted to suggest that a far larger set of entities—all U.S. persons—must preserve and report records that were not previously required, *i.e.*, all refused interactions from embargoed territories and designated entities. While this is not the only plausible interpretation of the interim final rule, nor is it an interpretation that CCIA would urge, the potential ambiguity warrants clarification.

[1] OFAC FAQs: Sanctions Compliance, Paras. 72-73 ("Compliance for Internet, Web Based Activities, and Personal Communications"), *at* https://www.treasury.gov/resource-center/faqs/sanctions/pages/faq_compliance.aspx

Accordingly, CCIA urges OFAC to withdraw this rule. At a minimum, OFAC should clarify the scope of "rejected transaction" and, as set out above, which activities are excluded from the scope of the requirements.

Sincerely,

Matthew Schruers
Chief Operating Officer
Computer & Communications Industry Association
25 Massachusetts Avenue, NW
Suite 300C
Washington, DC 20001
Telephone: (202) 783-0070

July 22, 2019