



U.S. DEPARTMENT OF JUSTICE
Antitrust Division

WILLIAM J. BAER
Assistant Attorney General

RFK Main Justice Building
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001
(202)514-2401 / (202)616-2645 (Fax)

October 2, 2014

Steven A. Bowers
Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, D.C. 20005

Dear Mr. Bowers:

This letter responds to your request for the issuance of a business review letter pursuant to the Department of Justice's Business Review Procedures, 28 C.F.R. § 50.6. The Department of Justice has no present intention to challenge the True Security Through Anonymous Reporting ("TruSTAR") cyber intelligence data-sharing platform that CyberPoint International LLC ("CyberPoint") proposed in its July 1, 2014, business review request ("Request").¹ In a joint policy statement that the federal antitrust agencies issued in April of this year, the Department of Justice and the Federal Trade Commission recognized that the ability of private entities to share cyber threat information is an important component in combating cyber attacks.² In that Policy Statement, the agencies made it clear that the antitrust laws are not an impediment to legitimate private-sector initiatives to share specific information about cyber incidents and mitigation techniques in order to defend against cyber attacks.³ Your proposal to share information is consistent with the type of information sharing that the agencies indicated would not raise competition concerns and has the potential to be procompetitive to the extent it provides your members a more efficient means of reducing cyber-security costs.⁴

¹ After filing its Request, CyberPoint changed the name of its information-sharing platform from "SecurityStarfish" to "TruSTAR."

² See Department of Justice and Federal Trade Commission: Antitrust Policy Statement on Sharing of Cyber Security Information (April 10, 2014) ("DOJ and FTC Antitrust Policy Statement").

³ *Id.*

⁴ See also October 2, 2000, Letter from Assistant Attorney General Joel I. Klein to Barbara Greenspan (favorable business letter issued to the Electric Power Research Institute ("EPRI") regarding EPRI's proposal to exchange cyber security information).

The Proposed Information Exchange

CyberPoint, a privately held company, provides cyber-security products, services, and solutions to commercial and government customers, including malware analysis and reverse engineering; digital forensics and incident response; and risk analysis and vulnerability assessments.⁵

CyberPoint's Request notes that the evolving sophistication and severity of cyber threats could have serious economic and security consequences for both U.S. and global security. The Request further notes that adversaries regularly collaborate in the sharing of information and have become increasingly adept at identifying vulnerable targets and launching effective attacks.⁶

The TruSTAR platform is designed to provide members accurate and timely intelligence to more effectively respond to these growing cyber threats. The platform will "allow members to share threat and incident data, attack information and remediation solutions to help define more-effective strategies across industries to prevent successful attacks."⁷ The platform will collect incident reports that include specific and technical information regarding current attack actors (e.g., IP addresses and file hashes), targets of attack, contextual information regarding threats (e.g., adversary tactics, techniques and procedures), and remediation solutions.⁸ Incident report content will be based on the Structured Threat Information eXpression ("STIX") language, a free and open industry-standard language for describing cyber-threat information.⁹ Members may use the incident reports to focus on cyber threats within their particular business sector, geography, and technology.¹⁰ The information will also allow members to assess their organization's security posture, evaluate the effectiveness of their defenses, and predict likely threats before an attack.¹¹

An important component of the TruSTAR platform is that members are able to submit incident reports with complete anonymity. The TruSTAR platform uses encryption and other technologies to allow members to excise all identifying information in the incident reports.¹² The TruSTAR platform also uses encryption and other technologies to ensure information is securely and anonymously transferred to TruSTAR.¹³ Once the incident reports are submitted to TruSTAR, they are distributed to the members. The Request explains that all members in a particular industry sector will

⁵ Request at 1.

⁶ Id. at 1-2.

⁷ Id. at 3.

⁸ Id. at 3-4.

⁹ Id. at 4.

¹⁰ Id. at 3

¹¹ Id.

¹² Id. at 3-4.

¹³ Id. at 4.

be treated equally in terms of receiving incident reports, so there is no discrimination against particular industry participants.¹⁴

The TruSTAR platform provides a community forum where members can collaborate with their peers on cyber threats and techniques for responding to them. The forum will allow for anonymous participation, while still permitting members to direct questions to the particular firm that filed an incident report.¹⁵ This ability to ask follow-up questions and for more detailed information is important to enabling effective collaboration. In order to participate on the TruSTAR community forum, members must agree that they will not share “competitively sensitive information – such as recent, current, and future prices, cost data, or output levels – or otherwise attempt price or other coordination.”¹⁶

Membership is open to all firms that have a Dun and Bradstreet D-U-N-S number and are in good standing with local, state, and federal governments, agencies and relevant industry groups.¹⁷ Members must also satisfy certain minimum technical performance criteria.¹⁸ Similar to the terms of use for the community forum, TruSTAR members must agree not to share competitively sensitive information or use the TruSTAR platform as a vehicle to reach anticompetitive agreements.¹⁹

Analysis

The Department typically analyzes competitor collaborations to share cyber-threat information under a rule of reason analysis.²⁰ “Rule of reason analysis focuses on the state of competition with, as compared to without, the relevant agreement. The central question is whether the relevant agreement likely harms competition by increasing the ability or incentive profitably to raise price above or reduce output, quality, service, or innovation below what likely would prevail in the absence of the relevant agreement.”²¹ A rule of reason analysis is a flexible inquiry that focuses on those factors necessary to evaluate the overall competitive effect of an agreement. The factors relevant here are: (1) the business purpose and nature of the agreement; (2) the type of information shared; and (3) safeguards implemented to minimize the risk that competitively sensitive information will be disclosed.

¹⁴ CyberPoint will allow particular industries to “slightly delay” the release of their incident reports to other industries. The example given is that the aviation industry might want some time to fix a vulnerability before an alert is shared with non-aviation-industry sectors. Request at 5.

¹⁵ Request at 5.

¹⁶ Terms of Use for TruSTAR Software-as-a-Service Products at 2.

¹⁷ Master Software Subscription Service Agreement, Exhibit D.

¹⁸ Id.

¹⁹ Id. at 7.

²⁰ DOJ and FTC Antitrust Policy Statement at 5.

²¹ Id. *quoting* Department of Justice and Federal Trade Commission Antitrust Guidelines for Collaborations Among Competitors (April 2000) at 4.

First, the business purpose and nature of the information sharing agreement does not suggest competition or consumers will be harmed. The business purpose of the proposed agreement is to share cyber-security information among private entities to protect networks and deter cyber attacks. Second, the nature of the information that will be shared is unlikely to facilitate tacit or explicit price or other competitive coordination among competitors. The information to be shared through incident reports and the collaboration forum are very technical and is the type of information sharing contemplated by the DOJ and FTC Antitrust Policy Statement. In that Statement, the federal antitrust agencies recognized the important role that information sharing plays in securing the nation's IT infrastructure. For example, in the DOJ and FTC Antitrust Policy Statement, the agencies indicated that the sharing of cyber threat information, such as that contemplated by the TruSTAR platform, "is very different from the sharing of competitively sensitive information" and "can improve efficiency and help secure our nation's networks of information and resources."²²

The ability of competitors to exchange competitively sensitive information, either through the TruSTAR platform itself or the collaboration forum, could raise antitrust concerns under the rule of reason. However, no competitively sensitive information about recent, current, and future prices, cost data, output levels, or capacity will be exchanged through the TruSTAR platform or the collaboration forum. CyberPoint will obtain commitments from members that they will not use the TruSTAR platform or collaboration forum to share competitively sensitive information. Because CyberPoint has taken steps to ensure that competitively sensitive information won't be exchanged, we believe that competitive harm is unlikely. Additionally, consumers may benefit from the TruSTAR platform to the extent it provides members a more efficient means of securing networks and information and reducing cyber-security costs.

Conclusion

Based on the information you submitted and your representations, the Department has no present intention to challenge the operation of the TruSTAR platform under the antitrust laws.

²² DOJ and FTC Antitrust Policy Statement.

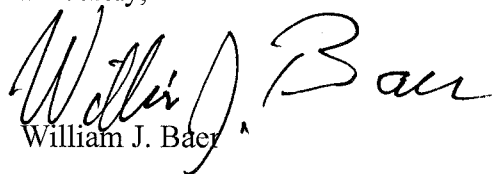
Steven A. Bowers

October 2, 2014

5

This statement is made in accordance with the Department's Business Review Procedure, 28 C.F.R. §50.6. Pursuant to its terms, your business review request and this letter will be made publicly available immediately, and any supporting data will be made publicly available within thirty (30) days of the date of this letter, unless you request that any part of the material be withheld in accordance with Paragraph 10(c) of the Business Review Procedure.

Sincerely,

A handwritten signature in cursive script, appearing to read "William J. Baer". The signature is written in dark ink and is positioned above the printed name.

William J. Baer