New York State Department of Taxation and Finance
Office of Counsel

TSB-A-15(47)S
Sales Tax
November 18, 2015

STATE OF NEW YORK
COMMISSIONER OF TAXATION AND FINANCE

ADVISORY OPINION PETITION NO. S130215A

The Department of Taxation and Finance received a Petition for Advisory Opinion from [redacted] (Petitioner). Petitioner asks whether it has nexus with New York, whether its cloud-based services are subject to New York sales or use tax as information or protective services or whether it is making taxable sales of software, and whether it is a vendor required to register for sales tax purposes and collect tax on its sales.

We conclude that Petitioner or its predecessor LLC has had nexus with New York, at least since 2006 when the LLC established a data center in this state. Petitioner's sales of its five levels of enterprise service and of its home service to its customers in New York are subject to State and local sales or use tax as the sale or use of a protective service. Petitioner's transfers of pre-written computer software plug-ins to its New York customers that enable its mobile and roaming functionalities and of the plug-in that enables its more detailed monitoring/report-generating functions are not separately subject to sales tax, because Petitioner uses the software plug-ins to provide its services and the transfers are included in the purchase price of the service to which those plug-ins apply. The fact that its monitoring/report-generating plug-in enables its customers to interact with Petitioner's software and create tailored reports does not change this conclusion, because the primary purpose of Petitioner's services and of the plug-in is to provide what are overwhelmingly protective services and the reports generated are part of the service. However, if Petitioner purchases those software plug-ins from another person and transfers them to its customers in New York, Petitioner is deemed to be using those plug-ins in New York in providing its service to New York customers, and Petitioner's use of such plug-ins would be subject to use tax. Petitioner is a vendor and is required to register for sales tax purposes and collect tax on its sales of taxable services provided to customers in this state.

Facts

Petitioner is a Delaware corporation, incorporated in 2009, headquartered in California. Petitioner has servers in data centers located in New York and in other states. Petitioner does not have an office in New York or any employees stationed here, and it is not registered in New York for sales and use tax purposes. Petitioner's predecessor LLC first established a data center in New York in February, 2006, and Petitioner continues to operate that data center. Petitioner's employees come into New York to maintain the servers, although these visits are infrequent because the servers need little hands-on attention.

Petitioner is a cloud-based professional services firm that uses internally developed software to route customers' Internet communications to its own servers around the world to speed up the translation to customers' "DNS" servers. A DNS server converts a written Internet site name into a series of numbers that constitute the Internet address of the destination server. This conversion process takes time and can cause delay. Petitioner uses its own software

algorithm to route its customers' queries with the least delay to the targeted site. In addition, its servers recognize queries sent previously by a customer. This allows the servers to return the same route result without making the customer wait on the query process. Thus, Petitioner's DNS service benefits its customers by speeding up the translation of natural language to the numbers that are the Internet address. Petitioner's basic DNS service is offered in an advertising-based model, under which users are not charged and ad revenue supports Petitioner's costs to provide the service.

Petitioner provides five levels of enterprise service for which it charges customers. Service A is the basic enterprise service, as described below. Service B is the same as A, plus a mobile phone component. Service C is also the same as A, but with a roaming component. Service D is also the same as A, plus a "monitoring/report-generating" component – but no mobile phone or roaming component. Service E includes A, plus the mobile phone, roaming, and monitoring/report-generating components. Charges for the components of each of the five services are not broken down – the customer buys the entire service, and cannot choose to purchase only a part of that service. Petitioner sells its services on an annual subscription basis, with the fee based on the service selected and the total number of users. "Users" of Petitioner's enterprise services means the customer's employees that use the service. Components of the various levels of service and the price of the service may change over time. Petitioner also provides its DNS service with each of its enterprise services, for no additional charge.

According to Petitioner's web site, each enterprise service combines multiple security enforcement technologies into one cloud-delivered security service. Each service combines leading security intelligence with robust security enforcement to block malware, botnets, phishing, and other high-risk sites and locations, as well as drive-by exploits, mobile threats, and dynamic DNS. All five also provide aggregated reports on Internet usage. They also provide DNS-based filtering for an Internet-wide layer of security over every port, protocol, and app. All but Service A also allow the customer to establish acceptable use or compliance policies enforced by using customizable content categories and bypass options. Services B, C, D, and E also provide encrypted DNS resolution service, and some of the services provide encrypted VPN services to securely redirect traffic. Petitioner's web site describes its service as an anti-fraud and identity theft protection service.

A customer that purchases Service A, B, or C can view and/or download reports of certain information, such as the number of times that its employees in the aggregate tried to access prohibited websites, but the customer cannot see an individual employee's information. The customer can also see the domain names of the attempted websites and the number of total attempts blocked for each domain, but not the URLs. This component has default settings that the customer may or may not choose to adjust to tailor the settings and reports. There is an initial set-up, and a menu of choices. Once the customer tailors the settings, they are not usually changed. In addition to what an A, B, or C customer can view or download, a customer that purchases Service D or E can also define the communications handling policy at a group or individual user level, and extract other data that Petitioner may capture in performing its services, so that the customer can see the actual employees who attempted to access prohibited sites and the number of times each of them did so, and can tailor permissions for groups or individual employees to have access to otherwise prohibited sites.

Petitioner's contracts with its enterprise customers provide that any information or reports its services provide to them will not or may not be substantially incorporated in reports furnished to other persons.

Petitioner also sells a service on an annual basis to home customers. This service protects every device in the customer's home that shares the customer's Internet connection, such as computers, game consoles, tablets, smart phones, and other devices. This home service identifies fraud and phishing websites and blocks them automatically in the customer's household. It also allows individuals to manage Web access of every device that accesses the Internet on their home network, including phones and computers that are brought into the house. The service blocks phishing emails and websites that aim to trick the customer into handing over personal or financial information and protects everyone on the customer's network. Even if a link manages to trick the customer, the service prevents the phishing website from loading. The home service does not have a monitoring/report-generating component that provides detailed control or reports. Home users have extremely limited interaction with parental controls or other settings. There are just a few 'buttons' to 'check' to block certain types or classes of usage. Likewise, the home service does not provide any of the detailed reports that the Service D or E monitoring/report-generating component does. The only reports a Home service customer receives show total usage and the extent to which traffic was speeded up by using the service.

Petitioner's software operates solely on its own servers and Petitioner uses its software exclusively to provide its various services and does not sell or license its software to customers or place it on their computers, except as regards the following software plug-ins that it places on computers of customers that purchase certain services.

Prior to about February, 2012, Petitioner did not download any of its software to customers' computers. Customers used their regular browsers to access the Internet, without needing any download of Petitioner's software. Starting in November, 2012, Petitioner released a software plug-in for mobile smart phone users of Service B, and a roaming plug-in for Service C. These plug-ins can be used only in conjunction with Petitioner's service and provide no functionality other than connectivity. The mobile phone plug-in allows users to receive Petitioner's DNS services when their phones access the Internet. This puts the phones on par with a connected computer but provides no other functionality. The roaming plug-in allows a customer's computers to receive Petitioner's DNS services when roaming. There is no separate charge to the customer for the plug-ins. Customers do not use or interact with Petitioner's mobile phone- or roaming-related plug-ins downloaded to their PCs. Thus, Service B, C, and E customers have no control over or use of these software plug-ins. Rather, only Petitioner uses those downloads in order to provide its mobile phone- or roaming-related service components.

Petitioner's only other software download to its customer's computers is the plug-in that provides the monitoring/report-generating component of Services D and E. Beginning about February, 2012, this plug-in allows D and E customers to make tailored configuration settings per user, device, group, or internal IP address, set more specific parameters of the service, and to view more information and monitor the service in a more active way.

Analysis

Nexus

Petitioner's predecessor LLC established its data center in New York in 2006, and Petitioner continues to use that data center. The physical presence of this center and its property constitute more that the slightest presence in the state. Thus, the LLC had nexus with New York at least from 2006, and Petitioner had nexus from the time it succeeded the LLC and continued to operate its data center in the state. *Orvis Company, Inc. v Tax Appeals Tribunal*, 86 NY2d 165 (1995), *cert denied* 516 US 989 (1995).

Petitioner's DNS Service -

Petitioner's stand-alone DNS service is free to all users, without the need to purchase any of Petitioner's enterprise services or home service that includes protective features. Petitioner's DNS service by itself does not constitute a protective service, because it acts to replace the DNS service that a customer would otherwise use for Internet access service provided by the customer's Internet service provider. In addition, because Petitioner does not charge its users for basic DNS service, it is not making sales of its DNS service to those users. Petitioner's inclusion of DNS service with its fee-based enterprise services or home service described below does not change the characterization of those services, because the DNS service is otherwise free and because the nature of enterprise and home services is determined by other factors.

Petitioner's Fee-Based Services –

Tax Law § 1105(c)(8) imposes State sales tax on sales, other than for resale, of protective services, including, but not limited to, all services provided by or through protective systems of every nature, including, but not limited to, protection against burglary, theft, or any malfunction of industrial processes or any other malfunction of or damage to property or injury to persons, whether or not tangible personal property is transferred in conjunction therewith. Tax Law § 1110(a)(C) imposes the State's compensating use tax on the use in this State of protective services.

The sales tax status of an integrated service depends on the primary function of the service. A service designed to prevent unauthorized access to or use of a customer's information technology (IT) assets is subject to sales tax under Tax Law §1105(c)(8) as a protective service, if the IT assets are located in New York. Similarly, the service of monitoring for unauthorized access to or use of a customer's IT assets and issuing reports to the customer about those unauthorized activities would be taxable as protective services if the IT assets are located in New York. Antivirus/anti-spyware protection comes within the definition of a protective service and is taxable under Tax Law §1105(c)(8) when the customer's IT assets are located in New York. Further, the service of monitoring a customer's IT assets to notify the customer when an asset malfunctions would constitute a taxable protective service. *See* TSB-A-10(14)S.

Each of Petitioner's enterprise services A, B, C, D, and E block malware, botnets, phishing, and other high-risk sites and locations, as well as drive-by exploits, mobile threats, and dynamic DNS. They also provide DNS-based filtering for an Internet-wide layer of security over every port, protocol, and app. They also provide encrypted DNS resolution service for secure, transparent traffic redirection, and some provide encrypted VPN Services for secure,

transparent traffic redirection. The services allow a customer to see how many times its employees tried to go to a blocked web site, such as one known to contain malicious software. Service D and E customers can see the actual users who attempted to access the prohibited sites and number of times each of them did so and can tailor permissions for groups or individual employees to have access to otherwise prohibited sites. Petitioner's filtering service may not actually block viruses, spam, and other malware from running on its customers' computing devices, but it does redirect customers' Internet connections for malicious domain names to prevent Internet connections to malicious sites, thereby helping to protect its customers' users from access to those dangerous sites. Thus, because the primary function of each of Petitioner's enterprise services is overwhelmingly protective in nature, each of them is a protective service, and Petitioner's sales of these services provided to customers in this State are subject to sales tax.

The reports that Petitioner includes in its enterprise services provide information that, if sold by themselves, might constitute an information service under by Tax Law § 1105(c)(1). But those reports provide the customer with information that allows it to consider the actions of its employees that use the Internet in ways that threaten the safety of the customer's computer systems and property, allowing the customer to take corrective action to protect its property, in the same way that a customer of a private detective or protective service provider may take action based on reports that the customer received from the detective agency or protective service provider. In TSB-A-10(14)S, similar reports were a component of a taxable protective service. In the same manner, Petitioner's reports to its enterprise services customers are a component of its taxable protective service. Thus, Petitioner's reports are not Tax Law § 1105(c)(1) information services and, separately stated, reasonable charges for the reports are not subject to tax.

Similarly, the primary function of Petitioner's home service is protective in nature. The service protects every device in the customer's home that shares the customer's Internet connection. It automatically identifies and blocks fraud and phishing websites, allows individuals to manage Web access of every device that accesses the Internet via their home network, and catches and blocks phishing emails and websites. Even if a link manages to trick a customer, the service prevents the phishing website from loading. Petitioner describes its service as an anti-fraud and identity theft protection service. Thus, Petitioner's home service is also overwhelmingly a protective service, and Petitioner's sales of this service delivered to customers in this State are subject to tax.

Petitioner's Software -

Tax Law §§ 1105(a) and 1110(a)(A) impose State sales tax on retail sales of tangible personal property and compensating use tax on the use of such property purchased at retail. Section 1101(b)(6) defines "tangible personal property" to include pre-written computer software, whether sold as part of a package, as a separate component, or otherwise, and regardless of the medium by means of which the software is conveyed to the purchaser. Tax Law § 1101(b)(14) defines "pre-written computer software" as software (including pre-written upgrades thereof) that is not software designed and developed by the author or other creator to the specifications of a specific purchaser.

No use tax is imposed on software used by its author if the author does not offer similar software for sale in the regular course of business. Where software is used by its author and the author does sell the same or similar software in the regular course of business, the author would be liable for use tax on its use of such software. In that case, the use tax would be computed on the cost of the medium (floppy disk, magnetic tape, etc.) that contains or is used in conjunction with the program. *See* TSB-M-93(3)S, TSB-A-13(30)S.

A person is not selling software when it installs software agents on its customers' IT assets for its exclusive use in providing services to its customers. The software agents, which act for and report to the person, are used only by the person to perform its services, and not by the customer on whose computer the software agent is installed. If the person installs a software agent at a customer location in New York State, the person will owe sales or use tax on the software unless it was created specifically for the person or the person created the software itself and does not sell it. Tax Law § 1110(a). If the person purchased the software from a third party and the software was not created specifically for the person (i.e., the software was prewritten software as defined in Tax Law § 1101[b][14]), the person's tax is based on the consideration paid for the software. If the person created the software and does sell it in the regular course of business, the use tax is based on the consideration paid for the blank medium, such as disks or tapes, used in conjunction with the software. Tax Law § 1110(g). *See,* TSB-A-10(14)S. If there is no tangible medium, the base would be zero.

The sales tax status of an integrated service depends on the primary function of the service. The primary function of Petitioner's enterprise and home services is overwhelmingly protective in nature. Because Petitioner does not charge its customers when its installs the mobile-phone or roaming plug-ins on its customers' IT assets, it is not selling that software to them. Those plug-ins, which act for and report to Petitioner, are used solely by Petitioner to provide its services. If Petitioner installs these plug-ins at a customer location in New York, Petitioner will owe sales or use tax on the software unless it was created specifically for Petitioner or Petitioner created the software itself and does not sell it to anyone. Tax Law § 1110(a). If Petitioner purchased those software plug-ins from a third party and they were not created specifically for Petitioner (i.e., the software was prewritten software as defined in Tax Law § 1101[b][14]), Petitioner's tax would be based on the consideration it paid for the software. If Petitioner created the software and does sell it in the regular course of business, its use tax obligation would be based on the consideration paid for the blank medium, such as disks or tapes, used in conjunction with the software. Tax Law § 1110(a)(F) and (g).

As indicated, Petitioner's enterprise services D and E are taxable protective services. In order to provide the service, and for no additional charge, Petitioner transfers the monitoring/report-generating plug-in to customers of those services for Petitioner's use in providing the services. While Service D and E customers can change the settings to customize the reports available with those services, the reports relate to the protective nature of the service and do not change its primary function of protection; rather, they enhance that function. If this plug-in was designed and developed specifically for or by Petitioner, and it does not sell it to anyone else, then Petitioner's use of it is not subject to use tax. However, if Petitioner were to make a separate charge for the software module/plug-in provided to a customer located in New York, that would constitute a sale by Petitioner of tangible personal property and its charge for

the plug-in would be taxable as a sale. In that case, Petitioner would have to collect sales tax on that separate charge.

Sales Tax Registration Requirement –

Petitioner provides protective services to its customers in New York. Its receipts from its sales of those services are taxable. Thus, it is a vendor under Tax Law §1101(b)(8). As a vendor, Petitioner is also a "person required to collect tax" under Tax Law § 1131(1). As a person required to collect tax, it must register for sales tax purposes under Tax Law § 1134(a) and collect tax on its sales to New York customers and file returns and remit tax required to be collected under Tax Law §§ 1136 and 1137.

DATED: November 18, 2015

/S/
DEBORAH R. LIEBMAN
Deputy Counsel

NOTE: An Advisory Opinion is issued at the request of a person or entity. It is limited to the facts set forth therein and is binding on the Department only with respect to the person or entity to whom it is issued and only if the person or entity fully and accurately describes all relevant facts. An Advisory Opinion is based on the law, regulations, and Department policies in effect as of the date the Opinion is issued or for the specific time period at issue in the Opinion. The information provided in this document does not cover every situation and is not intended to replace the law or change its meaning.