New York State Department of Taxation and Finance
Office of Counsel
Advisory Opinion Unit

TSB-A-11(14)S
Sales Tax
May 3, 2011

STATE OF NEW YORK
COMMISSIONER OF TAXATION AND FINANCE

ADVISORY OPINION PETITION NO. S100928A

Petitioner [redacted] requests an Advisory Opinion about whether its sales of its authentication service are subject to New York State and local sales and use taxes. We conclude that Petitioner's authentication service described below is not subject to State and local sales and use taxes.

Facts

Petitioner is a provider of authentication solutions for businesses and individuals seeking to perform secure electronic commerce and communications over the Internet. One such solution is the provision of a "digital certificate" and authentication and resolution services on a subscription basis.

Digital certificates are commonly used to facilitate secure transmissions between end users' browsers and Petitioner's customers' servers. A digital certificate allows an end user to recognize that they are accessing a customer's website, rather than a fake website, because Petitioner's trademarked logo will appear on the real website, indicating that it has been authenticated by Petitioner. The trademarked logo serves as a visible indication on the end user's screen that the customer's website is what it purports to be.

A digital certificate is provided through an online process, which the customer initiates by accessing Petitioner's online portal and completing a registration form. As part of this process, a private and public key pair is generated by the customer's web server. The private key is retained by the customer on its web server. The public key is part of the customer's information sent to Petitioner during the registration process.

Petitioner performs all due diligence necessary to authenticate the identity of the applicant, the related website and business, and the information provided by the customer during the registration process, including the public key (authentication service). There are two components of the "authentication service." The first authentication occurs when a customer requests a certificate. At that time, the customer gives Petitioner certain information. The customer can request a level of authentication from basic to advanced. Examples include verifying the existence of the customer's business, the ownership of the domain, and the requestor's authority to apply for the certificate. This process is completed by Petitioner's "trust center," and may involve Petitioner requesting a credit check or other report on the customer, along with various proprietary techniques to verify the customer's information.

Once Petitioner authenticates the applicant's identity, a digital certificate is sent to the customer electronically. A digital certificate is a flat file (i.e., does not contain code) that includes: the customer's public key; metadata that includes the certificate expiration date; the certificate owner's name; the name of the issuer (in this case, Petitioner); serial number of the certificate; and an electronic signature of the issuer. The exact contents of a certificate adhere to certain industry-established standards. The digital certificate is installed by the customer on the customer's web server.

The second authentication component occurs when the end user's web browser connects to a secure website (web server). The browser requests that the server identify itself. The server sends the browser a copy of its digital certificate. The browser checks the certificate's authenticity by matching it against a list that resides in the browser of all authentic certificate providers. If the browser establishes the certificate's authenticity, it initiates a secure transmission between it and the web server. All subsequent transmissions between the browser and the web server are securely encrypted.

When an end user's web browser attempts to communicate with a customer's web server, a secure link is established for that "session." The end user's web browser generates a unique "session key" to encrypt the transmission between the customer's server and the end user's browser, so that a secure communication can begin. The software to create a session key already resides in all web browsers and is not supplied by Petitioner. However, before encrypted communications can begin, the end user's browser must transmit the session key to the web server so that both servers will know how to encrypt and decrypt the transmission. To do this, the web browser uses a public key supplied by the web server to encrypt the session key and sends the session key to the customer's web server. The web server uses its private key to decrypt the session key so that both the web server and browser can begin using the session key to encrypt and decrypt all subsequent transmissions between the web server and the browser. The keys are generated in pairs by the customer's web server and are mathematically linked. Petitioner does not provide the keys. The public key is made available by the customer's web server through its digital certificate. The private key is retained by the customer's server. The encryption/decryption is performed by cryptographic software built into the end user's web browser and the customer's server. This software is not provided by Petitioner.

The resolution service is a process whereby the end user's browser verifies that the digital certificate is valid and has not been revoked. The web browser does this by contacting Petitioner's server in real time and Petitioner's server tells the web browser if the certificate is current and not revoked. Each certificate has a validity term, so a browser will validate that the certificate of the website it is connecting to has not expired. The certificate can also be validated by contacting Petitioner's server, which checks the certificate against a list of revoked certificates. The second method may be used when real-time servers are down.

The charges for the authentication service, digital certificate, and resolution service are part of a lump sum subscription charge and must be renewed periodically.

Analysis

We conclude that Petitioner's service is not subject to sales and use taxes. Sales tax is imposed on receipts from every sale of tangible personal property. *See* Tax Law § 1105(a). Prewritten computer software is included within the definition of tangible personal property, "regardless of the medium by means of which such software is conveyed to the purchaser." Tax Law § 1101(b)(6). Petitioner does not provide customers with tangible personal property. The certificate and services are not provided in tangible form; rather, they are delivered electronically. The digital certificate itself is not software and does not contain code. Petitioner does not provide its customer with any software. The software used during the encryption and decryption processes already resides on the customer's server and the end user's browser.

Sales tax is also imposed upon the receipts from every sale, except sales for resale, of certain enumerated services. *See* Tax Law § 1105(c). Petitioner's service is not among the services enumerated

under Section 1105(c) of the Tax Law. *See* TSB-A-00(7)S. Accordingly, Petitioner's service is not subject to State and local sales or use taxes.

DATED: May 3, 2011

/S/
DEBORAH 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.