

New York State Department of Taxation and Finance
Taxpayer Services Division
Technical Services Bureau

TSB-A-97(86)S
Sales Tax

STATE OF NEW YORK
COMMISSIONER OF TAXATION AND FINANCE

ADVISORY OPINION

PETITION NO. S971015D

On October 15, 1997, the Department of Taxation and Finance received a Petition for Advisory Opinion from NYCE Corporation, 300 Tice Boulevard, Woodcliff Lake, New Jersey 07675.

The issue raised by Petitioner, NYCE Corporation, is whether the fee it charges members of its banking network per transaction for electronic banking services performed through Automated Teller Machines (ATMs) and other similar machines is subject to New York State and local sales taxes under Section 1105(b) of the Tax Law.

Petitioner submitted the following facts as the basis for this Advisory Opinion.

Petitioner operates and administers a network through which it handles electronic banking transactions for members of the network. Members include both "banks" and "non-banks." All members pay a one-time initiation fee to join the network, but no annual fee thereafter. Each member participates in the network through a contract with Petitioner that is called a "Participation Agreement." The Participation Agreement incorporates by reference certain "Operating Rules." Petitioner included with its Petition, a copy of the Participation Agreement and the Operating Rules.

There are thousands of possible combinations of activities and functions that Petitioner might perform with respect to an individual banking transaction. Petitioner must react to each transaction depending on the circumstances surrounding it. However, a "simple" transaction through the network from start to finish would generally take the following steps.

Transaction Acquisition. In the most fundamental way, Petitioner allows depositors at one of its member banks to use that bank's services from a remote terminal and conduct banking transactions electronically without the need for a teller. The bank at which the cardholder (or depositor) holds the account is the "Issuer Bank." The cardholder inserts his or her card into an ATM. The ATM is viewed as having "acquired" the transaction request. Thus, the financial institution that owns the ATM is the "Acquirer Bank." The Acquirer Bank has a computer driver which allows the ATM to function and read the magnetic strip on the back of the card. From the strip, the ATM reads a series of numbers. The series contains subsets consisting of an identifying number for the Issuer Bank (for example, Issuer Bank ID Number ABC) and an identifying number for the cardholder (for example, Cardholder ID Number 123). The ATM then requests the cardholder to enter his or her Personal Identification Number (for example, PIN QQQ). The ATM then requests information regarding the type of transaction the cardholder would like to conduct and the specific details of that transaction. For example, the cardholder might ask to withdraw \$150 from his or her checking account.

The ATM then prepares a message to Petitioner, identifying itself as the Acquirer Bank and indicating that Cardholder ID Number 123 is standing before one of its terminals and would like to withdraw \$150 from a checking account maintained at Issuer Bank ID Number ABC. This message includes an encrypted version of the PIN QQQ. The Acquirer Bank has no idea who Cardholder ID Number 123 is, what bank is Issuer Bank ID Number ABC, whether the cardholder has entered his or her correct PIN, whether the cardholder has an account with the Issuer Bank, whether there are sufficient funds in the account, or whether the cardholder has initiated a transaction which the Issuer Bank will allow.

Message Editing and Translation. Petitioner receives this message in a computer language that is consistent with the Acquirer Bank's system. As indicated, the part of the message that pertains to the cardholder's PIN is encrypted; that is, it is scrambled in a code which requires a key to unscramble. When Petitioner receives the message, it does a number of things. First, Petitioner identifies the ATM, and its driver, so that Petitioner can pull from its files the identity of the language in which the message has been sent. Second, once it knows who the Acquirer Bank is, Petitioner can identify the key that will enable it to unscramble the encrypted PIN.

Petitioner's system then translates the message into its own internal computer language. Once the message is translated into Petitioner's internal computer language, its contents are edited to meet the specifications and parameters of Petitioner's system. After editing, the message is checked for completeness and read. If the message does not contain all of the information necessary, for example the PIN, Petitioner corresponds directly with the Acquirer Bank to ascertain the missing information.

Network Confirmation/Authorization. By reading the message, Petitioner can identify the Issuer Bank ID Number ABC, and confirm that the institution is a member of Petitioner's network. This identification also serves to route Petitioner's request for transaction authorization to the appropriate source. Two initial responses can result.

If the Issuer Bank is not a member of Petitioner's network, a message is prepared (first in Petitioner's internal computer language and then translated into a language that is compatible with the Acquirer Bank's computer) that the Issuer Bank is not a member of Petitioner's network. This message is then transmitted to the ATM driver which, through its own internal processes, instructs the ATM to return the cardholder's card and to display a message indicating that the Issuer Bank is not a member of the network. Petitioner monitors the ATM's performance of this function and waits for confirmation from the driver that it did, in fact, instruct the ATM to display the appropriate message. If this confirmation is not forthcoming within a specified period of time, Petitioner creates and then transmits a message to the ATM driver informing it that a problem has developed. Petitioner also creates an internal message for its own use to the effect that until it receives a reply message indicating that the problem ATM has been fixed, no new transactions should be accepted from that

machine. This "handshake" and "standing by" for confirmation is an aspect of Petitioner's service which applies to all situations where Petitioner transmits a message to an end-point that is outside of its internal system. Every time Petitioner sends a message out, whether it is to an ATM or an Issuer Bank, it awaits confirmation that the message was received and the instructions were carried out.

If, after reading the translated message from the ATM, Petitioner determines that the Issuer Bank is a member of Petitioner's network, Petitioner consults its database and identifies the language that the Issuer Bank's computer uses. Petitioner then consults its database to determine what key the Issuer Bank's encryption system uses. Petitioner will then translate its internal message into the Issuer Bank's computer language and translate the encrypted PIN, as received from the Acquirer Bank, into the encrypted PIN that meets the Issuer Bank's key. Petitioner also edits the translated message to fit the ordering and content parameters of the Issuer Bank. Finally, Petitioner edits the message to add records of transactions conducted by that same cardholder through Petitioner earlier that day, as well as any information regarding the cardholder that Petitioner maintains in its "negative file," for example, that the card was reported stolen. The Issuer Bank might use the transaction records to determine whether any daily maximum withdrawal amount has been exceeded or whether the level of activity indicates that the card is being used in an unauthorized manner.

Issuer Authorization. When the message is transmitted to the Issuer Bank, Petitioner stands by for authorization. At this juncture, there are three basic responses from the Issuer Bank: a positive response, a negative response, and no response. (See Stand-In Authorization, infra, in the case of no response.)

If there is a positive response from the Issuer Bank, Petitioner prepares an internal log entry in its own computer language documenting the transaction and indicating that the Issuer Bank has authorized the transaction. This entry is used to settle accounts at the end of the banking day. The Issuer Bank will debit the cardholder's account on its own, in the case of this example, \$150. Petitioner then prepares and transmits a message in the Acquirer Bank's computer language instructing it to dispense the cash. Petitioner waits for confirmation from the Acquirer Bank that the cash has, in fact, been dispensed.

If the Issuer Bank responds with a negative, Petitioner reads the denial for any specific details and prepares an internal message indicating this denial. If for example, the authorization is negative because the Issuer Bank has indicated that the cardholder's card was reported stolen, Petitioner will prepare a message to the Acquirer Bank instructing it to "capture" the card. If the negative is simply because the cardholder's account has insufficient funds, Petitioner will prepare a message to the Acquirer Bank informing it that the request has been denied because of insufficient funds. Again, Petitioner will wait for confirmation from the Acquirer Bank that the instructions conveyed were, in fact, carried out.

Stand-In Authorization. If the Issuer Bank, after a specified time period, does not respond with any authorization information, Petitioner consults its own databases to determine whether it has secondary authorization powers on behalf of the Issuer Bank. With respect to some members, Petitioner has permission to "authorize transactions" on its own if the Issuer Bank's system is down or unresponsive. In the usual case, Petitioner reviews its internal file of lost, stolen, inactive or otherwise unauthorized cards (its "negative file") to determine whether the card is still active. If stand-in authorization is negative, Petitioner prepares its own message handling the transaction as if it had received a negative authorization directly from the Issuer Bank. For example, a "capture card" message might be prepared if the card was reported stolen. Petitioner then translates its internal message into the Acquirer Bank's computer language informing it of its decision -- in this case, instructing the ATM to capture the card. As is the case with all messages sent by Petitioner, the Petitioner's computer will stand by and wait for confirmation from the endpoint.

If the cardholder's card is not contained on the "negative file," Petitioner prepares an internal message that the transaction has been authorized. In this example, Petitioner has secondary authorization powers, but only up to \$100 per transaction. Accordingly, the amount of the withdrawal is limited to \$100. Petitioner then sends instructions in the Acquirer Bank's computer language to dispense \$100. Petitioner also instructs the Acquirer Bank to display a message explaining why the withdrawal amount is limited. Like all transmissions, Petitioner stands by and waits for confirmation from the Acquirer Bank that it dispensed the \$100 to the cardholder. The Issuer Bank in this case needs to be informed that the transaction took place, because Petitioner authorized the transaction. As a result, Petitioner prepares a message to the Issuer Bank which will be queued (i.e., stored) until the Issuer Bank comes back on-line. This message informs the Issuer Bank that Petitioner authorized a \$100 withdrawal from the cardholder's account and instructs the Issuer Bank to debit the account.

Transaction Confirmation/Reversal. After a message to dispense cash (based on a positive authorization) has been transmitted, if the Acquirer Bank does not confirm that it dispensed the cash to the cardholder, Petitioner prepares and transmits a follow-up message to the Acquirer Bank. If that message also goes unanswered, Petitioner will "reverse" the transaction. To reverse the transaction, Petitioner prepares and transmits a message to the Acquirer Bank that Petitioner has not been able to confirm that it dispensed the \$150 as directed, and that Petitioner assumes that it did not dispense the funds. Petitioner also prepares and transmits a "reversal" message to the Issuer Bank, instructing it to "reverse" the debit it just made to the cardholder's account because the ATM did not actually dispense the funds.

Also, the possibility exists that the Acquirer Bank was only able to complete a portion of the transaction. For example, the ATM may only have \$50 cash left, but the cardholder's full withdrawal request of \$150 has been authorized. In this case, the Acquirer Bank would respond that it was only able

to dispense \$50 of the authorized \$150. Petitioner, in response, would prepare a message to the Issuer Bank informing it that the transaction was only partially completed and that it should change the debit of \$150 it just entered on the cardholder's account to \$50. This is referred to as a "partial reversal."

Settlement. Because the transactions handled by Petitioner are banking transactions, they must be settled at the end of each day. Thus, at the end of each day, Petitioner retrieves its internal log of authorized and confirmed transactions for settlement. Settlement is the method of managing the net flow of funds daily between the member banks. At the time of an ATM transaction, the cardholder's account is debited or credited. At the end of each banking day, funds must be settled between the Issuer Bank and the Acquirer Bank. Petitioner records all transactions and then adjusts the net financial position of each of its members according to their net transactions for the day. Netting is required because an Issuer Bank might also be an Acquirer Bank. The two amounts (typically debits for transactions as Issuer, and credits for transactions as Acquirer) are netted and summed, resulting in a posting total. The net posting total for each member is then settled by Petitioner who communicates with the New York Automated Clearing House which, using the Federal Reserve Bank, debits and/or credits the cash positions of the various members to reflect their net settle amounts.

The settlement procedure is performed by Petitioner for all network members. Transactions are funded by and to Petitioner's own settlement account, with the aggregate transaction amounts passed through Petitioner's account that day equalling zero. Thus, at the end of the day, assuming that the cardholder's \$150 withdrawal was transacted without the need for secondary authorization or any reversal and that it was the only transaction involving these two banks, Petitioner would use the Automated Clearing House to create a debit of \$150 for the Issuer Bank and a credit of \$150 for the Acquirer Bank.

Fee. For this entire transaction, Petitioner imposes a charge of approximately 10 cents.

Telecommunications. Petitioner requires and uses a telecommunications interface with its members through which all transactions flow. The Operating Rules provide that each member must establish and maintain the telecommunications link between itself and Petitioner. These telecommunication lines are the members' financial responsibilities. As a practical matter, however, Petitioner orders the lines on behalf of its members so that it may monitor the lines' performance and ensure that they meet the standards of quality and responsiveness necessary for the network to function properly. When Petitioner receives the invoices for the telecommunication lines, Petitioner is charged by and pays sales tax to the telecommunication carriers. Since Petitioner is merely arranging for the lines on its members' behalf, Petitioner passes through the charge (sales tax as well) to its members. This charge is not included in the 10 cent transaction fee and is not at issue in this Opinion.

Petitioner actively participates in executing banking transactions -- all the way through settling the transaction among and between the institutions at issue. Petitioner does not simply redirect calls between two members of the network. It reads the messages, reformats the messages, edits the messages, adds to the messages, prepares entirely new messages, and acts upon the messages.

Applicable Law and Regulations

Section 1105(b) of the Tax Law imposes sale tax, in part, upon:

The receipts ... from every sale, other than sales for resale, of telephony and telegraphy and telephone and telegraph service of whatever nature except interstate and international telephony and telegraphy and telephone and telegraph service

Section 527.2(d)(4) of the Sales and Use Tax Regulations provides, in part:

A service is not considered telegraphy or telephony if either of these services is merely an incidental element of a different or other service purchased by the customer.

Opinion

The transaction fees received by Petitioner from members of its banking network for electronic banking services performed through Automated Teller Machines, and other similar machines, are not subject to New York State and local sales taxes. Section 1105(b) of the Tax Law imposes sales tax on the receipts from certain sales of telephony and telegraphy, and telephone and telegraph services. Petitioner's services, as described in this Opinion, are not included within the meaning and intent of Section 1105(b). The telephony and telegraphy services that Petitioner describes furnish the means by which Petitioner provides its electronic banking services to the members of its banking network and are incidental to Petitioner's electronic banking services. (See, Matter of Holmes Electric Protective Co. v McGoldrick, 262 AD 514, *aff'd* 288 NY 635.)

DATED: December 29, 1997

/s/
John W. Bartlett
Deputy Director
Technical Services Bureau

NOTE: The opinions expressed in Advisory Opinions are limited to the facts set forth therein.