FEDERAL RESERVE BANK *of* NEW YORK

THOMAS C. BAXTER, JR.
GENERAL COUNSEL AND
EXECUTIVE VICE PRESIDENT

April 14, 2016

The Honorable Carolyn B. Maloney
2308 Rayburn House Office Building
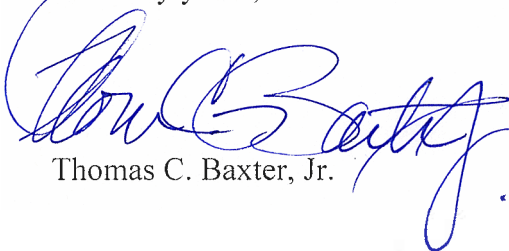Washington, DC 20515-0001

Dear Representative Maloney:

I have been asked to respond to your letter dated March 22, 2016, to William Dudley, President of the New York Fed, regarding press reports of transfers involving the central bank of Bangladesh.

We treat with the utmost importance and concern reports that one of our central bank clients has fallen victim to cyber fraud. As we have noted previously, there is no evidence of any attempt to penetrate Federal Reserve systems in connection with the payments in question, and there is no evidence that any Federal Reserve systems were compromised.

Consistent with the confidentiality concerns that you acknowledge in your letter, as well as the policy imperative that we not inadvertently interfere with an active criminal investigation, we have prepared the enclosed responses to the questions posed in your letter. We would be happy to brief you or your staff further, subject to these constraints.

Sincerely yours,

Thomas C. Baxter, Jr.

Enclosure

Is it appropriate to rely solely on authentication from SWIFT for outgoing payments from the accounts of foreign central banks? Are additional authentication protocols necessary to prevent this kind of cyber theft in the future?

The vast majority of both commercial banks and central banks around the world rely on SWIFT's secure communication channel and authentication protocols as their primary method of verifying that banking instructions received from counterparties are authentic. Given SWIFT's predominance around the world, SWIFT is used routinely by banks in the United States to communicate payment instructions for cross-border payments. As is the case with all communication channels, the security of the channel depends in part on the security environment at the end users, including foreign central bank end users. For this reason, institutions that use the SWIFT system commit to take certain actions to protect the security of the SWIFT network, including implementing technical, operational, managerial, and procedural controls designed to protect the security of the information technology environment used by the institution to access the SWIFT network. Such measures are critical to the security of the system. The Federal Reserve is continually assessing its own internal control environment as security threats evolve, and we expect other central banks and commercial banks to do the same.

Why did the New York Fed block the last 30 transfer orders, but not the first 5 orders? What was it about the last 30 transfer orders that raised the New York Fed's suspicions?

When the New York Fed receives an authenticated payment instruction via SWIFT, there are additional processing steps that must take place before the New York Fed acts on the instruction. Unlike the SWIFT authentication protocols, these steps are not designed to protect our customers from an unauthorized transfer. Rather, the New York Fed performs diligence to protect itself from unwittingly transferring dollars to a sanctioned jurisdiction or person. Automated systems screen the payment instructions for sanctions compliance and also to ensure the instructions are properly formatted. If an instruction fails one of these automated screens, a New York Fed employee will manually review the payment instruction for the cause of the failure. The vast majority of authenticated instructions received from foreign official account holders are not flagged for manual review by the automated systems. Manual reviews can result in a range of actions, from a quick resolution of the specific issue flagged by automated screening to a stop on all payment requests pending further clarification from the account holder.

The New York Fed also has processes and procedures designed to allow the New York Fed to identify, investigate and, where appropriate, refer to law enforcement, payment activities of its foreign official account holders, such as money laundering, that might raise law enforcement concerns. In some cases payment instructions are manually reviewed for this purpose prior to being executed, and in other cases this review occurs after execution. However, if a manual review occurs, either before or after execution, it is not a review for authenticity of the SWIFT sender and does not supplant the SWIFT authentication procedures on which the New York Fed and its foreign official account holders rely.

If an authenticated payment instruction passes all of the automated screens or is otherwise cleared after manual review, and provided a check of the account balance confirms that there are adequate funds in the account, the New York Fed executes the payment instruction. When that instruction is executed, a message (called an "advice") is automatically released to the foreign official account holder over SWIFT providing notice that the New York Fed has carried out its payment instruction.

On the afternoon of February 4, 2016, after certain earlier payments had been screened and cleared for execution, several instructions submitted in a batch of 30 were flagged for sanctions compliance review. These instructions were flagged close in time to each other. As a result of the manual review of the group of flagged messages, the New York Fed determined that the activity in question was potentially suspicious and the payment instructions should not be executed without additional inquiry to the central bank, including an inquiry as to the intended purpose of the payments.

Press reports indicate that the New York Fed requested reconfirmation from Bangladesh Bank of all 35 transfer orders, but executed the first 5 transfer orders without receiving any reconfirmation. Why did the New York Fed request reconfirmation from Bangladesh Bank, but not wait until it received reconfirmation before executing the first 5 transfer orders?

The press reports suggesting that the New York Fed executed payments for which it had requested reconfirmation prior to receiving such reconfirmation are incorrect. On February 4th, the New York Fed contacted the central bank of Bangladesh to inquire about the purpose of certain pending payments that had not yet been executed. Consistent with our procedures and in part as a result of determining that there was potentially suspicious activity with respect to the pending payments, on the next day, February 5th, the New York Fed reviewed all transactional activity in the Bangladesh account from February 4th that had been executed before the potentially suspicious activity was detected. Based on this review, on February 5th we again contacted the central bank of Bangladesh, this time with additional inquiries about the purpose of certain payments that had been executed the prior day.

What is the New York Fed's policy regarding reconfirmations of large transfers from the accounts of foreign central banks, and was that policy followed in this case?

As noted above, every payment that is executed by the New York Fed on behalf of our central bank account-holders results in an advice being issued to the account-holder indicating that its instructions have been carried out. The advice is sent immediately after the payment is executed. It is the responsibility of the account-holder to review such notices. We do not have a policy of "reconfirming" payment instructions from central banks unless there is a fatal formatting error or a manual review, either prior to or after payment execution, gives us a reason to inquire about the nature or purpose of an instruction.

***Why did the New York Fed not question the apparent misspelling in the $20 million transfer
order to the Sri Lankan account, as a correspondent bank did?***

In this case, the Sri Lankan beneficiary bank (and not the U.S. correspondent bank) appears to have noted an inconsistency between the beneficiary name and account number. The beneficiary bank in a funds transfer is the bank that can determine whether or not the beneficiary is accurately described. In this case, neither the Federal Reserve nor an intermediary bank had the information necessary to make such a determination. If the beneficiary is described by name and number inconsistently, and the beneficiary's bank knows of this inconsistency, then it should not accept the payment. *See* Uniform Commercial Code 4A-207.