MIAMIBEACH

OFFICE OF THE CITY MANAGER

NO. LTC # **009-2017**

LETTER TO COMMISSION

TO: Mayor Philip Levine and Members of the City Commission

FROM: Jimmy L. Morales, City Manager

DATE: January 9, 2017

SUBJECT: Report regarding the theft of funds from a City bank account

The purpose of this Letter to Commission is to provide a more detailed report to the City Commission regarding (i) how the funds were stolen from the account, (ii) the steps we are taking to recapture the funds, and (iii) the steps we have taken to ensure that our internal controls and cash management procedures provide the highest level of protection going forward. In preparing this report, I am being careful not to discuss information that could in any way compromise the criminal investigation that the U.S. Attorney's office, the FBI and Miami Beach Police are spearheading.

Explanation of the theft

The account in question is the core account in the system of the general depositary account that the City maintains with SunTrust Bank (the "Account").1 The Account dates back to 1995, and was most recently renewed pursuant to a competitive RFP in 2012. The average daily balances in the Account range from $46 million to $144 million. This account is where all funds received by the City are deposited daily either from a direct deposit or from an overnight sweep from five (5) receiving sub-accounts (Parking, Resort Taxes, Liens, Red Light Camera and Parks & Recreation) Although most of the transactions in the Account consist of deposits to the Account, there are some disbursements from the Account to third parties (approximately 300 monthly), mostly consisting of electronic transfers to other governmental entities and fees and charges paid to banks for credit charges and related items. When the City has to pay vendors for good and services, payroll and claims, funds from the Account are transferred to the applicable zero balance account (ZBA) disbursement account for payment therefrom. The web of accounts that collectively comprise the City's general depository account has approximately 1,500 incoming transactions and 1,100 outgoing transactions per month.

The theft in question took place pursuant to the electronic transfer of funds under the Automated Clearing House (ACH) system. Under that system (regulated by Federal statute), correspondent banks engage in electronic funds transfers on behalf of their customers. All requests have to be processed within 24 hours. If you have ever authorized the electronic transfer of funds from your checking account to pay a utility bill,

---

1 The City maintains 27 accounts with SunTrust, including the Account. The average daily balance in all accounts with SunTrust is approximately $171 million.

for example, you recall that you provided the account number and the A.B.A. routing number for your account (often by a cancelled check that contains said information) and the required authorization form for the electronic debits.

What occurred in this instance (and apparently is a fairly common and widespread form of fraud) is that third parties obtained the account number and A.B.A. routing number for the Account. They then provided that information to various vendors, and represented that this was their bank account. The vendors then provided this information to their respective banks, and when the time came to pay invoices, those banks sent electronic requests for funds transfer to SunTrust, believing that the Account was actually the account of the customer of the vendor in question. SunTrust processed the request and electronically transferred the funds to the banks in question. This took place over a six month period with numerous transactions, resulting in the transfer of over $3.6 million in funds from the Account. Finance department staff discovered the transfers in December, and I learned of these transfers on December 19th.

As a result of the mechanism utilized, we actually know specifically which banks requested and received the transfers, and which bank customers (vendors) had initiated the request for transfers. We also have alleged names for the individuals or entities that provided the false account information to the vendors. All of this information has been provided to law enforcement and they are investigating. Finance staff also alerted SunTrust, who immediately stopped any further electronic transfers under the ACH system for our accounts. We have since reviewed all activity in the Account, as well as all our other accounts at SunTrust and other financial institutions, and we have not identified any other fraudulent activity. The activity appears to be limited to the Account.

One question that comes up is how the Account information became available to the third parties that perpetrated the theft. While the criminal investigation may shed light on that (including whether any City employee was complicit in this fraud), it is also possible that we may never truly know. Bank account numbers and A.B.A. routing numbers are usually in the possession of a wide array of individuals. Any check ever written contains the information. Any wire transfer sent/received contains the information. Any valid electronic transfer sent/received contains the information. Given the level of activity in the Account and the age of the Account, the number of individuals that have, at some point, had access to the information is too large to measure.

Another question is whether this has had an adverse impact on the ability of the City to provide services, maintain its operations or meet financial obligations (including bonds and pensions). The answer is no. The City's Pension Funds, for example, are held with the pension trustees in different bank accounts. They were not impacted. It is also important to note that bond proceeds for funding capital projects (including the MBCC) are not held at SunTrust but in protected investment accounts at other institutions and considered to be fully secured. The impact of this fraud does not affect the City's ability to pay obligations and fund payroll pursuant to the approved fiscal budget. Until it is returned to the City, the $3.6 million is deemed to have been removed from the City's contingency funds, which currently has a balance of approximately $48 million.

Efforts to Recapture the Funds

Once I learned of the theft of our funds, we immediately contacted Miami Beach Police to investigate the fraud. Within 24 hours, we met with police and the FBI, and staff has been working with those agencies, providing information as requested. I have also been in communication with the US Attorney's office on several occasions to discuss the case. While the goal of any criminal investigation is to identify and bring the culprits to justice, we also anticipate that information gathered therein will assist us in recapturing funds and/or assets.

SunTrust also initiated the claims process under the federal statute governing ACH transactions. Under that statute, if a bank that transfers electronic funds subsequently discovers (within 60 days from the transfer in consumer cases and 2 days in non-consumer cases) that the request was not valid, it is entitled to file a claim with the bank that originated the request. The statute provides that the originating bank shall, within ten (10) business days of the request, either provide documentation evidencing that the transaction in question was properly authorized or, if such documentation is not available, it must return the funds. SunTrust has filed claims with respect to all the electronic transfers out of the Account. Since none of the bank customers in question were vendors of the City or in any other way in any relationship with the City, we believe that there is no way that any documents will be produced that evidence authorization of withdrawal from the Account. To date, pursuant to the process and also pursuant to due diligence by the City, $691,770 has been returned to the Account.

We are in constant communication with officials at SunTrust and are cooperating with them in the effort to recapture the funds from the banks that received them. I have met twice with senior officers of SunTrust, including the South Florida President, and they are cooperating with the criminal investigation as well as conducting their own internal analysis of the transactions. The goal, of course, is to recapture as much of the money as humanly possible. Much work remains to be done in this regard, and all the parties in question are working collaboratively to reach that goal. Depending on the results of that effort, we will, of course, examine any other remedies available to us.

Ensuring the security of City funds going forward

Just as important as recapturing the dollars is making sure this never happens again. The steps we have taken include:

- Opened new general depository bank account with SunTrust and in process of closing current one. Given the number of accounts that pay into the Account, we cannot just simply close it without a transition time during which we provide notice to third parties that pay into the account.

- Implemented ACH Fraud Control on the new and existing account which allows the City to set parameters for which ACH transactions are allowed.2 This gives

2 Unfortunately, the last time the Account was renewed in 2012, ACH Fraud Control was made available by SunTrust at no cost to the City, but the Finance staff at that time elected not to apply it to the Account. The protection was only applied to our disbursement accounts.

the City the tools needed to monitor electronic payments and block unauthorized ACH debits before they post to our account.3 We have similarly made sure that all other accounts that might be a target also have ACH Fraud Control or some similar protection.

- Set up UPIC, a unique account identifier issued by financial institutions that allows organizations to receive electronic payments without divulging confidential banking information.

- Unless pre-authorized, discontinued ACH payments for good and services

- Discontinued ACI with MasterCard payments.

- Instituted a daily review and reconciliation of all non-check disbursements.

- Accepted the resignation of the Treasury Manager and the Accounts Payable Director.4 As I have indicated publicly, while the theft may not have been entirely preventable, the amount could have been mitigated by better performance of the treasury management and account reconciliation process.5 I am continuing to examine how we could have minimized the extent of the theft and further personnel decisions may be necessary. Obviously, if the criminal investigation identifies any employee-related issues, those will be addressed as well.

As I reported to you last week, I used my emergency procurement authority to retain the accounting firm BDO to conduct a review and risk assessment of our internal controls and procedures in our Treasury management and disbursement function. We will be working with both the New York and Miami offices. They also have a cyber security department that can assist with any issues that may arise with respect thereto. The goal is to ensure that our internal controls represent best practices going forward. We anticipate that the review will be completed in 4-6 weeks.

I have personally spoken with our financial advisor to determine if she thought that this event would have any impact on our bond ratings, and she was of the opinion that since the funds in question do not impact our debt coverage ratios or the City's economic forecasts, there should be no impact. Finally, I met with our outside independent auditing firm and have asked them to provide me a time and cost estimate with respect to expanding the scope of future annual audits to include the effectiveness of our internal controls with respect to cash management. This is not something that is required by Florida with respect to the audit of municipal financial statements, but is something that is done with respect to publicly traded companies.

If you have any questions, please feel free to contact me.

---

3 In fact, the ACH Fraud Control program already prevented an unauthorized ACH transfer last Friday.

4 The Treasury Manager had been with the City for 14 years and had served as Treasury Manager for the last 10 years. The Accounts Payable Director similarly served in that capacity for the past 10 years.

5 We are in the process of hiring a new Treasury Manager who comes to us with many years of experience as a Finance Director in two other municipalities in Miami-Dade County.