MEMORANDUM

DATE: August 19, 2019

TO: Assembly Finance Committee

FROM: Jeff Rogers, Finance Director

SUBJECT: CBJ Victim of Financial Wire Fraud

155 Municipal Way
Juneau, AK 99801
Phone: (907) 586-5215
Fax: (907) 586-0358

Background

Nationwide, the occurrence of financial theft by means of wire fraud is an increasingly alarming occurrence. The schemes vary, but requests to change ACH (i.e., direct deposit) payment information are on the rise and increasing in their sophistication. CBJ Finance staff have thwarted many such attempts, including many attempts to change payroll ACH information for prominent city employees.

CBJ now finds itself to have been a victim of one such coordinated and sophisticated scheme. A timeline follows as well as a description of corrective action taken.

Timeline

December 27, 2018

CBJ was contacted by an individual (later identified to be an impersonator) who purported to be associated with SECON Construction, a company under contract with CBJ to provide construction services. In that communication, the individual requested that CBJ update the company's ACH payment information. The request asked that the bank account number alone be changed; not the routing number. Over the next several months, CBJ and the individual made several infrequent contacts, arranging for receipt of an updated W-9 form and voided check before allowing an update to the banking information.

March 21, 2019

The fraudulent individual provided an updated W-9 form and a voided check. At this time, CBJ Purchasing & Accounts Payable reviewed the information and updated the bank account number assigned to SECON Construction. CBJ also conducted a "pre-note" process in which a zero-dollar test transaction was sent to validate the bank account information. That process was successful. Meanwhile, SECON Construction was an active vendor performing construction work for CBJ. During its normal course of business, SECON sent a legitimate invoice to CBJ for actual work performed.

April 11, 2019

After appropriate review and approval of the legitimate SECON invoice for payment, CBJ issued an ACH payment for $329,630.21 to the new bank account. As with all ACH payments to vendors, CBJ e-mailed SECON indicating a notice indicating they would be receiving a direct deposit on April 12, 2019 for the specific invoice.

May 6, 2019

SECON staff contacted CBJ indicating they had not received the payment on April 12, 2019. Upon investigation of the situation, CBJ became aware of the fraudulent change to the banking information and confirmed the payment never made it to SECON; instead, it went to the fraudulent bank account set up by the individual impersonating a SECON employee.

May 7, 2019

CBJ reported the crime to the Juneau Police Department and the Federal Bureau of Investigation. Additionally, CBJ immediately implemented measures to secure banking information of CBJ payees to limit any future similar incidents. CBJ also notified their insurance carriers of the incident. CBJ's bank, First National Bank Alaska, also attempted to recall the ACH payment but were unsuccessful.

July 23, 2019

CBJ received reimbursement from our insurer for $250,000—the policy limit for this type of fraud. At this time, we believe the FBI investigation continues, but CBJ staff have had little follow-up interaction with the investigator assigned to the case.

Corrective Action Taken

Since the incident, CBJ Finance leadership has finalized and implemented a new policy for changes to ACH banking information for all payees of CBJ. That new policy is attached to this memorandum.

Recommended Assembly Action

At this time, a supplemental appropriation to the Risk Fund does not appear to be necessary for FY19, so no action by the Assembly Finance Committee is necessary.

If the Committee desires further discussion of the details of the incident, I recommend that the committee enter into executive session so as not to interfere with the ongoing FBI investigation.

MEMORANDUM

DATE: August 19, 2019

TO: All Finance Department Staff

FROM: Sam Muse, Controller

SUBJECT: Security policies over Purchasing, Accounts Payable, Treasury & Payroll

155 Municipal Way
Juneau, AK 99801
Phone: (907) 586-5215
Fax: (907) 586-0358

Background

Nationwide, the occurrence of financial theft by means of wire fraud is an increasing troublesome occurrence. The schemes vary, but requests to change ACH (i.e. direct deposit) payment information are on the rise and the increasing in their sophistication.

Policy Update

Vendor setup

When the CBJ procures a new vendor to provide goods/services, or procures a vendor that has been previously inactivated, that vendor will be required to complete a "Vendor Information Form". This form indicates the reason for update to the vendor database (e.g. a new vendor, or an update of previous vendor information).

A section of the Vendor Information Form will specifically address electronic payments and banking information. As a part of this section, the vendor will be required to provide a PIN which will be entered on the AP10.1, TELEX field. Additionally, the vendor will be required to include a minimum of two known contacts, including phone numbers/emails. These contacts will be added to the AP14.1 screen. Specific details for data entry can be found using the procedure for "Adding New Vendors" located in Purchasing (Accounting Tech Desk Manual). CBJ will ensure that the vendors are aware that these contacts/PINs are being requested in the specific case of banking changes.

It will be the Purchasing department's responsibility to enter all information in to the vendor database and to maintain the vendor record and any related changes requested. Copies of the vendor paperwork will be provided to Accounts Payable, who will audit each entry with supporting backup documentation. Requests for updates to data by Accounts Payable will be given back to Purchasing for official edit. The vendor will pre-note with the next check run performed by Accounts Payable. If successful, Purchasing will then have the vendor status changed to "Accepted" (at the direction of AP) in the database. This process generally takes two weeks.

REQUIREMENT SPECIFIC TO ACH

- A voided check must be provided and it must be a negotiated item (the vendor must provide a copy of a check that was issued and processed through their account within the last 90 days).
- If a voided check is not available, the Vendor should provide banking information on bank letterhead. Letter must be signed and include contact phone number.

The number of active vendors will be limited. Vendors that have not had invoices paid on for the preceding three years will be inactivated in the payable system. When a vendor is inactivated, purchasing and accounts payable will be required to obtain a new vendor information from a known contact of the vendor (if one can still be identified, if not other measures) in order to reactivate that vendor.

Changes to Vendor Banking Information

CBJ will validate all new electronic payment instruction and other bank change requests received even if the request is internal.

Upon notice of possible changes by a vendor an email will be sent to acknowledge the recipe of the email and the PIN (noted above) will be requested.

All follow up, including the acknowledgment email, will be to the email addresses and phone numbers of known contacts, as detailed in initial vendor setup or through previously verified changes to vendor information. The vendor must be reached via direct phone call at least once during the process. Purchasing & Accounts Payable will verify the new information provided by the vendor through this direct communication.

As part of the process, a "Banking Data Change Form" will be prepared and reviewed by Purchasing and Accounts Payable. This form will verify that the contacts were spoken to, and will be signed off on by all relevant parties. This requires that old banking information (if applicable) be confirmed and will also be maintained in the master vendor file.

Any request that comes outside of the known contacts will need to be verified independently. If a known number is not available or a PIN has been forgotten, the respective department will perform their own search for a correct number, outside of any information provided in the original request sent to the department.

Security over email/trainings

Email is set up so that all external emails are identified as such upon arrival.

Details of e-mail address are scrutinized for suspicious components, i.e., name does not match, email server inconsistent, extension indicate foreign or suspicious address

Phishing or scams are shared with MIS.

Results of all internal phishing campaigns are shared with relevant employees. For example, if the payables tech is subject of a phishing campaign, this is shared with the supervisors and with purchasing.

Purchasing/accounts payable/payroll/treasury are required to undergo training for fraud, such as social engineering, yearly or if a new employee is hired within the department.

Requests from outside for information regarding our Vendors

Requests for certain information regarding CBJ vendors (known contacts, banking information, tax I.D. numbers, etc.) should be confidential. Any request from a vendor regarding their own information should be verified independently, via phone call with known contact.

Additionally, information requested from the outside regarding non-confidential information must have a request for information form filled out and filed with the Clerk's office. The request will be vetted and only the information in the request will be provided.

Payroll Specific

Payroll staff will personally verify any direct deposit changes NOT received in-person in the Payroll Office. Employees will receive a call from payroll staff to verify the change(s). Payroll staff will fill out a form recognizing that this step has been completed. The change will not be processed until this step is complete. A "Direct Deposit Authorization form" will be completed and kept on file in the employee's master file.