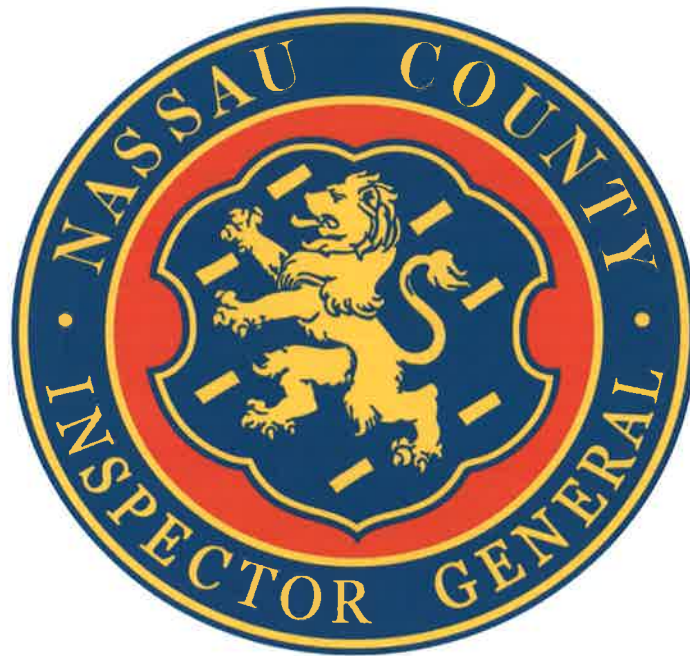


Nassau County Office of the Inspector General



Review of 2019 Vendor Impostor Fraud Incident

JODI FRANZESE
Inspector General

November 19, 2020

Table of Contents

Executive Summary	2
Background.....	4
Origin and Objectives	4
Findings.....	6
Conclusions	13
Controls at the Time of the Incident	17
Controls Implemented After the Incident.....	21
Recommendations	27
Appendix A – Comptroller’s Office Response, with OIG’s Follow-up Comments.....	30
Appendix B – Comptroller’s Office Response, as Submitted	49

Executive Summary

The Nassau County Office of the Inspector General (OIG) conducted an independent review of a fraud incident perpetrated in September 2019 against the Office of the Nassau County Comptroller. OIG's objectives in conducting this review were to ascertain the facts of the fraud, assess the impact on County Information Technology (IT) infrastructure, and assess the internal controls in place before and after the fraud occurred.

OIG determined that the Comptroller's Office (CO) was the victim of a vendor impostor fraud scheme, in which a fraudster utilized email to impersonate a legitimate County vendor and cause CO staff to change that vendor's Automated Clearing House (ACH) banking information. With the banking information changed, the County's legitimate electronic payments were diverted from the true vendor's bank account to a bank account under the fraudster's control.

OIG found that the CO authorized 11 payments totaling \$2,095,813.92 to a bank account controlled by the fraudster on seven dates in September and October 2019. Of this total, eight payments totaling \$710,955.92 were deposited in the fraudster's bank account. The bank, on its own initiative, restricted ("froze") this account due to a fraud notification, unrelated to Nassau County, that it received from another bank. The bank's action caused the rejection of the remaining \$1,384,858 in pending CO-approved payments, thereby preventing the successful diversion of this larger amount of County funds to the fraudster's account.

The bank notified the CO of the account freeze on October 22, 2019. Two days later, the CO learned, as a result of communications from the true vendor, that the deposits had been fraudulently diverted, and the CO accordingly notified the Nassau County Police Department (NCPD).

At the time of the bank freeze the fraudster's account contained only \$608,606.72 but the County was ultimately able to recover all the money that had been deposited into the fraudster's account.

OIG also determined that, although the fraud was committed via the use of email, it did not constitute a technological cyber-attack on the County's IT infrastructure.

OIG further determined that the internal controls the CO had in place at the time for the vendor information change process were not effective in preventing the fraud scheme, and that its staff was not trained to detect such fraud.

In the wake of the fraud incident, the CO put into place controls that are consistent with a number of anti-fraud measures recommended by the Government Finance Officers Association, and also provided relevant training to its Vendor Claims Division (VCD) employees. Additionally, the CO reported it has contracted an independent auditing firm to assist in an assessment of the CO's cybersecurity needs and fraud risks.

Subsequent to the subject fraud event, there were two other, apparently unrelated attempts at vendor impostor fraud that did not succeed in diverting County funds. The CO reported one of these attempts to the NCPD.

OIG identified possible opportunities to further reduce fraud risks. OIG accordingly makes the following recommendations to the CO:

- Further strengthen controls through periodic, comprehensive fraud risk assessments
- Provide fraud awareness training for VCD staff on a recurring basis.
- Train Accounting Division staff on significance of ACH return reason codes.
- Expedite issuance of pending written procedure for vendor information change processing.
- Ensure consistent reporting of fraud attempts.

OIG provided the Comptroller's Office for comment a draft of this report. The Comptroller's Office response to our draft is attached to this report as Appendix B including, in part, their description of the steps they have taken concerning our recommendations. The OIG's follow-up comments to their response are attached as Appendix A. This, our final report, incorporates some modifications of the draft, based in part upon the Comptroller's Office response.

OIG appreciates the cooperation of the Comptroller's Office throughout our review.

Background

Pursuant to New York state law and the Nassau County Charter, the Office of the Nassau County Comptroller (Comptroller's Office or CO) has general superintendence over the County's fiscal affairs and is charged, in part, with monitoring the County budget and financial operations.¹ The CO is composed of four divisions, including the Vendor Claims Division (VCD), which reviews and approves claims on County contracts and manages vendor payment information. As part of this responsibility, the VCD also receives and processes vendor requests to change their banking information for receipt of electronic payment. Such requests are common and accepted through multiple means of communication, including email, fax, and the postal service. The CO's Accounting Division is responsible, in part, for receiving and processing notifications from the County's bank of rejected electronic (Automated Clearing House or ACH) payments to vendors.

On October 24, 2019, the CO reported to the Nassau County Police Department (NCPD) that it had been the target of a fraud. The CO informed detectives that approximately \$710,000 in CO-approved payments to a vendor had instead been diverted to a bank account under the control of a fraudster. The fraud was investigated by NCPD and was subsequently the subject of publicity and a hearing of the Finance Committee of the Nassau County Legislature.

Origin and Objectives of this Review

On January 24, 2020, the Nassau County Office of the Inspector General (OIG) received correspondence from the Nassau County Legislature's Deputy Presiding Officer, Howard Kopel, Chairperson of the Finance Committee, requesting that OIG conduct an independent review of the incident and of the internal security and cybersecurity controls

¹ NY County Law, § 577 (1); Nassau County Charter §§ 401-402.

of the CO. OIG determined the subject to be consistent with its statutory oversight mission and initiated the present review.

The objectives of this review were to:

- Ascertain the facts of the fraud incident perpetrated against the CO beginning in September 2019.
- Determine what impact, if any, the fraud had on the County's Information Technology (IT) infrastructure.
- Assess the internal controls in place at the time of the fraud incident.
- Assess the internal controls implemented after the fraud incident.

To achieve these objectives, OIG requested and obtained documents, correspondence, and information from the CO. In the course of its review, OIG interviewed personnel from the CO, as well as representatives of the Nassau County Treasurer's Office, the Department of Public Works (DPW), the County's bank, the impersonated vendor, and the NCPD. OIG examined a sample of the forms submitted by vendors to the CO to change their banking information, and associated documents. Additionally, OIG explored cybersecurity related questions with Nassau County's Department of Information Technology (DIT), conducted research into cybersecurity concepts, and identified recommended strategies for prevention of vendor impostor fraud.

The CO cooperated with OIG throughout the review.

Findings

OIG determined the following sequence of events to have occurred.

Fraudster Impersonated a County Vendor to Redirect Payments

On September 2, 3, and 4, 2019, an unidentified person (the fraudster) posing as an employee of a legitimate County vendor, repeatedly emailed the County, each time requesting a copy of the form needed to update the vendor's banking information for receipt of electronic payments. The fraudster directed two requests to the CO's Accounting email address and two to a DPW employee's email address, the last of each on September 4, 2019. The four emails included a signature line showing the name, address, and telephone number of an actual employee of the vendor, and the web address of the vendor. The fraudster utilized tactics to make his/her communications with the County appear legitimate. The fraudster used the name of a real vendor, the name of an actual employee of the impersonated vendor, and created an email address only slightly different from the impersonated vendor's email address, ending in a different top-level domain name (i.e., ".org" instead of ".com"). The impostor's email address was created on September 1, 2019, the day before the first message was sent.

CO Changed Vendor Electronic Bank Payment Information in Response to Fraudster's Request

On September 4, 2019, the manager with access to the CO's public email account forwarded the latest email received to the Fiscal Officer who heads the VCD. Minutes later, the Fiscal Officer replied to the fraudster by emailing a blank copy of the County's Form 700² and writing "Attached please find the relevant form. Please complete and return to my attention. Should you have any questions, please feel free to let me know." The form instructed in part that the submitter attach an image of a voided check showing the account number to which payments were to be sent.

On September 5, 2019, the fraudster emailed to the Fiscal Officer a scan of a completed Form 700 and, as required per the form's instructions, an image of a voided check that

² Titled "Nassau County Request for Taxpayer Identification Number and Certification," and based on the IRS Form W9, the Form 700 (also known as W9/700 or 700-W9) is the County's form to set up new vendors and to change existing vendor's key information, including payment information.

bore the name and address of the vendor. The Fiscal Officer forwarded these to an Auditing Assistant IV in the CO's VCD with the instructions, "please see attached." The Auditing Assistant IV in turn directed an Auditing Assistant II in the same unit to process the change to the vendor's banking information in the Nassau Integrated Financial System (NIFS), the County's mainframe computer system. This entry replaced in NIFS the legitimate vendor's bank account with an account controlled by the fraudster.

CO Authorized Nearly \$2.1 Million in Payments to a Bank Account Controlled by a Fraudster

After changing the vendor's banking information in NIFS, CO VCD staff subsequently authorized 11 electronic payments, on seven dates, totaling \$2,095,813.92 (see Table 1 below). These payments were based on invoices submitted by the legitimate vendor for work performed in accordance with its County contracts. By changing the vendor's banking information in NIFS, the CO thereby caused these payments to be routed to a bank account controlled by the fraudster.

Breakdown of \$2,095,813.92 authorized for payment into fraudster's account*

Payment Date	Amount	
9/11/2019	\$188,750.00	} \$710,955.92 paid into fraudulent account.
9/11/2019	\$116,385.00	
9/20/2019	\$30,402.42	
9/25/2019	\$42,162.24	
10/4/2019	\$73,760.44	
10/9/2019	\$100,970.61	
10/9/2019	\$1,700.00	
10/11/2019	\$156,825.21	} \$1,384,858 stopped by bank freeze.
10/18/2019	\$63,508.00	
10/18/2019	\$65,150.00	
10/18/2019	\$1,256,200.00	
Total	\$2,095,813.92	

**Compiled from data received from the Nassau County Treasurer's Office*

Bank Froze Fraudster's Account, Preventing Transfer of Three Additional Payments

On October 17, 2019, the fraudster's account was restricted ("frozen") by his/her bank, thereby preventing further deposits into that account.³ According to the bank's investigator, the restriction was placed after a notification the bank received from another bank, that a transaction associated with this account was fraudulent. The fraud that precipitated the account freeze was separate and apart from the Nassau County incident.

Bank Rejected Payments, Notified CO's Accounting Division

On October 22, 2019, designated employees within the CO's Accounting Division, including the Specialist responsible for processing ACH returns (the Specialist), received via email from the bank an ACH Return Report. The Report notified the CO that the three ACH transfers initiated on October 18, 2019, totaling \$1,384,858, had been rejected (returned). The return reason code (return code) noted for each of the three returned payments was "R16-Account Frozen." As the three transfers had been rejected, \$1,384,858 was returned to the County's bank account.⁴

At this time, however, eight preceding payments, totaling \$710,955.72, had already been transferred into the fraudster's account before the bank initiated the account freeze.

Accounting Division Specialist Requested that the Actual Vendor Submit a New Form 700

The CO's practice in the event of an ACH return was to confirm the payee's correct address and to manually generate a paper check to replace the rejected electronic payment. On October 23, 2019, the Specialist followed this practice by emailing a blank Form 700 to two employees in the Financial Services Unit of DPW, the County department for which the vendor performs services, and writing:

We received an ACH reject for this vendor stating Bank Account Frozen. Please have the vendor complete and return a new 700 form with a cancelled check. Please

³ As it happens, the County's bank account and the bank account controlled by the fraudster were with the same financial institution.

⁴ On October 25, 2019, the Nassau County Treasurer's Office mailed the vendor a check in the amount of \$1,384,858 to replace the three ACH payments that had been rejected due to the bank account freeze.

confirm their mailing address is correct on file, so we can issue a manual check for the rejected payment.

DPW Notified Actual Vendor of Account Freeze; Vendor Responded

On October 23, 2019, the above email was duly forwarded by DPW staff to a representative of the actual vendor, who then replied:

Please send payment ASAP. Our account is not frozen... I will have the new form filled out ASAP. How come no one let us know about this?

Later that day, DPW staff forwarded the vendor's reply to the CO Specialist.

Vendor Notified CO and DPW that the Account Did Not Belong to Vendor

In subsequent correspondence on October 23rd, the Specialist provided the vendor via email with a copy of the ACH rejection report and indicated that payment of the returned \$1,384,858 would be made by check.

On October 24th, in reply to the CO, the vendor advised that the bank account and routing number on the ACH return report did not belong to the vendor.⁵

DPW Provided Copy of Fraudulently Completed Form 700 to Actual Vendor

On October 24, 2019, a DPW staff member emailed the vendor, the Specialist, and the Fiscal Officer, stating that, based upon information from the CO, the vendor's bank information had been changed because the CO received an email from one of the vendor's employees (in actuality the fraudster), requesting to update the vendor's electronic payment information. The DPW staffer attached the supposed employee's email, as well as the Form 700 and voided check image provided by the fraudster.⁶

⁵ Additional communications took place between the vendor, DPW, and the CO to identify which payments due to the vendor had not been received.

⁶ The DPW employee sending this email copied the fraudster's email address in the distribution of this message.

Actual Vendor Identified the Fraud

On the afternoon of October 24, 2019, the vendor's true representative replied to DPW and the CO:

STOP all payments to that [name of bank] Account – that is a fraudulent account – that is not [name of vendor employee]'s email address.

In a subsequent email, the vendor noted that the impersonated employee was not, in any case, authorized to change bank account information.

CO Notified the NCPD

On October 24, 2019 the Fiscal Officer notified the Deputy Comptroller/Chief Counsel (Deputy Comptroller) of the fraud, including that eight vendor payments totaling \$710,955.92 had gone into a bank account under the control of a fraudster.

Also that day, the CO contacted the NCPD and the lead detective assigned to investigate the matter met with the Deputy Comptroller. The detective told OIG that, in this meeting, the Deputy Comptroller explained that approximately \$710,000 in payments intended for a vendor had been diverted to a fraudster's bank account, transferred in eight transactions made between early September and mid-October 2019. NCPD commenced its investigation.

The County Recovered all Diverted Funds

As noted, the total amount of funds diverted to the fraudster's account was \$710,955.92. When the bank restricted (froze) the fraudster's account, it contained a balance of \$608,606.92. Employees of the Nassau County Treasurer's Office were in contact with the bank and worked to recover the frozen funds. On November 7, 2019, the bank sent the County \$608,285.31 in funds from the frozen account.⁷ The bank recovered an additional \$321.41 on November 19, 2019, which it sent to the Treasurer's Office.

⁷ A check in this amount was mailed by the Treasurer to the true vendor, on November 14, 2019.

Subsequent to this, the lead NCPD detective was able to identify additional bank accounts which had received transfers from the now frozen account, and he caused those accounts to be frozen by their respective financial institutions as well. As a result of these freezes, Nassau County was able to recover the remaining \$102,349.20. This amount was sent to the Treasurer's Office by the Nassau County District Attorney's Civil Forfeiture Unit on January 2, 2020.⁸

CO Conducted a Look Back Review; Confirmed the Validity of Some Vendor Change Requests

After the fraud came to light, the CO in 2019 performed a review (look back) of the Forms 700 processed during the period of January 2019 through September 2019. CO staff telephoned selected vendors to verify the changes requested on those forms. While this action reportedly did not identify any discrepancies, the CO did not document the results or specifics of its review.⁹

CO Requested Post-Incident Forensic Review from New York State

In February 2020, the CO contacted the New York State Division of Homeland Security and Emergency Services (DHSES) to request a "forensic review" of the fraud incident. The CO provided DHSES with three emails received from the fraudster. A member of DHSES's Cyber Incident Response Team replied that, based on an analysis of email headers, these emails came from a domain and IP address that had been listed on an abuse tracking site as associated with phishing and scams. They also found that the fake vendor domain created for this fraud was registered on September 1, 2019 (the day before the fraudster sent the first email request).

CO Staff Given Fraud-Related Training

On February 13 and 14, 2020, two presentations from consultants concerning cybersecurity were emailed to VCD staff. On February 20, 2020, VCD supervisors attended a

⁸ On January 6, 2020, a check was issued by the Treasurer's Office to the vendor in the amount of \$102,670.61, the outstanding balance owed by the County to the vendor.

⁹ The only known documentation resulting from the look-back consisted of 12 emails that were sent to vendors who could not be reached via telephone.

Government Finance Officers Association (GFOA)¹⁰ webinar that addressed such topics as vendor payment fraud.¹¹ On March 2, 2020, four or five VCD staff also attended a cybersecurity training presentation delivered by the County's bank, hosted by the Treasurer's Office. In addition, CO staff participated in online cybersecurity awareness training required for all County employees.¹²

¹⁰ Founded in 1906, the GFOA represents public finance officials throughout the United States and Canada. GFOA's mission is to advance excellence in public finance.

¹¹ According to a CO training summary, all VCD staff received copies of the GFOA training presentation.

¹² This training, provided by SANS, was implemented in February 2019. Although the training was administered Countywide after the fraud incident, DIT management informed OIG that it had already been procured and scheduled prior to the incident.

Conclusions

CO was the Victim of a Vendor Impostor Fraud Scheme

Vendor Impostor Fraud (also known as Vendor Impersonation Fraud) (VIF) occurs when a fraudster pretends to be a vendor in order to defraud private parties, businesses, or government entities. NACHA,¹³ the electronic payments association, describes it as follows:

In instances of VIF, fraudsters impersonate a legitimate vendor or contractor, and contact businesses or public-sector entities requesting to change payment account information. Contact can come in the form of an email, telephone call, fax, or even a letter in the mail. In each case, the fraudster requests that account information payment be changed to an account controlled by the fraudster, so that when an invoice is received, the entity processes a payment to the fraudster, resulting in a loss to the entity. Social engineering techniques have grown more sophisticated over time.

Fraudsters may create email addresses that are similar to the actual email address making it difficult to spot. Written correspondence may appear to be printed on legitimate letterhead or stationery.

Although victims of these scams range from small businesses to large corporations, any business entity could be the target of this form of social engineering. In particular, public sector entities seem to be targeted because their contracting information is typically a matter of public record. Fraudsters use information from such public records to impersonate legitimate contractors more convincingly.¹⁴


¹³ Previously known as the National Automated Clearinghouse Association, NACHA is a non-profit association funded by the financial institutions that use its network.

¹⁴ Accessed at: <https://www.nacha.org/sites/default/files/2019-04/NACHABECVIF.pdf>

Fraud Incident Did Not Compromise County's IT Infrastructure

The subject fraud incident did not disrupt, disable or compromise the County's IT infrastructure.

The Commissioner of the Department of Information Technology (DIT) informed OIG that the CO did not notify her department of the fraud incident. However, DIT does not view the incident as a "cyber-attack" or "breach event" affecting the County's IT infrastructure¹⁵ as specified in Nassau County's Local Law 15 of 2019.¹⁶ DIT's Manager of Computer Operations told OIG that while an email could conceivably constitute an attack on IT infrastructure, depending on the circumstances and the content of the email, in this instance the fraudulent email was neither an attack nor a breach event. Moreover, DIT



As such, the subject incident was not a "cyber-attack," as the term is commonly defined in the technological sense. The Committee on National Security Systems defines a cyber-attack as: "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information."¹⁷

¹⁵ DIT's Manager of Computer Operations defines IT infrastructure as "every computer, server, and network connected device on the County's internal network."

¹⁶ This law, codified in section 2151(m) of the Nassau County Charter, tasks DIT with performing certain actions, including notifying the legislature "within seventy-two (72) hours of a breach event or cyberattack on Nassau County's information technology infrastructure." The law does not require other County entities such as the CO to notify DIT of such adverse events.

¹⁷ Accessed at:

https://www.dni.gov/files/NCSC/documents/nittf/CNSSI-4009_National_Information_Assurance.pdf

According to Cisco, “A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Usually, the attacker seeks some type of benefit from disrupting the victim’s network.”¹⁸

CSO Online¹⁹ further defines the term cyber-attack as

an attack launched from one or more computers against another computer, multiple computers or networks. Cyber-attacks can be broken down into two broad types: attacks where the goal is to disable the target computer or knock it offline, or attacks where the goal is to get access to the target computer's data and perhaps gain admin[istrative] privileges on it.²⁰

Based on definitions such as these, the subject fraud incident was not a cyber-attack. Although the fraudster employed the electronic medium of email to carry out this fraud, the email itself did not carry malicious code or links that could compromise or tamper with the County’s networks or applications. Rather, the incident simply entailed the use of email messaging by an impostor to mislead the CO into making an otherwise routine data entry to change the banking information on file for a vendor.

The use of an email message to deceive a County employee is consistent with definitions of social engineering. For example, according to the Federal Bureau of Investigation, “Social engineering is the use of deception, through manipulation of human behavior, to target and manipulate you into divulging confidential or personal information and using it for fraudulent purposes.”²¹ DIT’s Manager of Computer Operations told OIG that, from a technical standpoint, there is nothing that can be done to protect against user error or misinterpretation, and the only way to fight emails like the one in this case is via the training of staff.

¹⁸ Accessed at: <https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html>. Cisco is a major corporation specializing in IT, networking, and cybersecurity solutions.

¹⁹ CSO Online is a web magazine provided by IDG Communications, which “provides news, analysis and research on security and risk management.” Source: <https://www.csoonline.com>

²⁰ Accessed at: <https://www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-show-disturbing-trends.html>

²¹ Accessed at: <https://www.fbi.gov/video-repository/protected-voices-social-engineering-083018.mp4/view>

In any event, the CO advised OIG that the CO has contracted an independent auditing firm to assist, among other things, in an assessment of the CO's cybersecurity needs.

The Bank Froze the Fraudster's Account on its Own Initiative

As noted earlier, the account under the fraudster's control was restricted after another bank notified the County's bank that an unrelated transaction associated with this account was fraudulent. Thus, the basis for the bank's freeze was separate and apart from the Nassau County incident.

The Bank's Independent Action Prevented the Fraudulent Transfer of \$1.384 Million

Had the bank not taken the step of freezing the account, three payments approved by the CO, totaling \$1,384,858, would have been transferred into the account under the fraudster's control.

The Vendor Detected the Fraud

The CO realized that the vendor's banking information had been fraudulently changed when it was so alerted by the vendor on October 24, 2019. The vendor detected that: 1) the bank account information on the Form 700 forwarded by DPW was not that of the company's account; and 2) the email address used by the fraudster was not the real email address of the impersonated vendor employee. The vendor brought these discrepancies to the attention of DPW and the CO on October 24, 2019. At the time that the vendor raised the alarm, the CO had authorized 11 payments, totaling \$2,095,813.92, to the fraudster's bank account.

The CO's Look Back Verification was Partial, Extent is Unclear

The CO conducted a look back review and verified Form 700 changes made by some of the County's vendors. The CO advised OIG that it reviewed all change requests submitted between January 1, 2019 and September 30, 2019. The Deputy Comptroller advised OIG that in the course of this review CO staff checked Forms 700 for any red flags, such as questionable email addresses, and found none. CO staff then telephoned selected vendors to verify their changes. The vendors were selected for verification because they received frequent high dollar payments, received payment via multiple payment methods, or had added or changed banking information during the review period.

The CO was not able, however, to provide a report summarizing its look back or documentation reflecting which vendors were contacted for verification, beyond 12 vendors who were sent emails.²²

Lacking the specifics of the verifications, OIG was not able to ascertain the percentage of vendors who were contacted for verification. However, the CO advised OIG that it did not detect any other fraud attempts, and the CO has not reported to OIG any other instances of payments that were fraudulently diverted.

Controls at the Time of the Incident

CO's Then-Existing Internal Controls Were Ineffective in Preventing the Subject Fraud; Were Not Consistent with Recommended Mitigation Strategies

It is apparent that the CO's internal controls at the time of the subject incident did not prevent the fraudulent change of banking information, and consequent diversion of multiple payments.

The Fiscal Officer informed OIG that the CO's controls in place at the time were designed for the purpose of identifying and resolving errors in the transcription of bank account and tax identification numbers.

At the time of the incident, the CO required submission of the following to process a request to change vendor information:

- A completed Form 700
- A voided check or a bank letter showing the bank account number to which payments were to be routed.
- A valid tax identification number, verified using an online IRS lookup tool.

²² Emails were sent to 12 vendors who could not be reached by telephone.

The Government Finance Officers Association (GFOA), whose mission is to advance excellence in public finance, recommends various measures to reduce the susceptibility of governmental entities to vendor impostor fraud.²³ These involve specific steps to confirm the legitimacy of vendor payment information change requests. Prior to October 2019 however, CO procedures did not incorporate these GFOA recommended risk mitigation strategies. For example, VCD staff were not required to verify that the submitter of the Form 700 was indeed an authorized representative of the true vendor. Additionally, there was no requirement that the vendors provide as confirmation their original banking information.

Pre-Incident Controls Prevented but Did Not at that Time Detect Another Fraud Attempt

In an apparently unrelated instance, on September 25, 2019, the CO was emailed a Form 700 requesting a change of a vendor's banking information for receipt of ACH payments. In accordance with a written instruction issued in 2018 by the Fiscal Officer, a VCD employee followed up by requesting that the submitter provide a voided check or bank letter. There was no response. Despite two follow-up attempts, communications from that party apparently ceased. The submitted Form 700 was retained on file but the change was not entered in NIFS. As will be discussed below, in December 2019 the actual vendor notified the CO that the September 2019 attempt to alter its banking information was not legitimate.

It is therefore possible, although not certain, that the VCD's request to provide a voided check/bank letter dissuaded a would-be fraudster from further communication with the CO. In any event, had the requirement for a voided check/bank letter not then existed, the CO presumably would have processed the change. OIG concludes, however, that the CO

²³ Accessed at: <https://www.gfoa.org/materials/electronic-vendor-fraud>

did not recognize the fraudulent nature of the September change request until the vendor so alerted the CO in December 2019.

Vendor Claims Division Staff Were Not Trained to Detect Vendor Impostor Fraud; Red Flag Missed

OIG found no evidence that VCD staff had received training pre-incident to detect vendor impostor fraud attempts. When asked whether VCD employees received any fraud awareness training prior to September 2019, the Fiscal Officer related that in August 2019 some VCD staff attended a training seminar offered by the New York State Comptroller's Office. This training focused on the three elements of vendor claims auditing — legality, correctness, and regularity of claims processed. While the training addressed fraud in the context of processing or auditing claims submitted by vendors, it did not address detecting fraud in connection with spurious emails, vendor impersonation, or the changing of banking information.²⁴

In the context of fraud detection, a red flag is an indicator that additional scrutiny or caution may be warranted. The emails and attachment that VCD staff received from the fraudster contained discrepancies that a trained eye might recognize as red flags. The most prominent of these was a “lookalike” domain at the end of the email address. As conveyed in post-incident training conducted by the County's bank:

Fraudsters purchase/register a domain closely resembling that of a legitimate company, then set up a related email account to target the victim company. Victim companies' employees often do not notice the difference between their legitimate corporate domain and the lookalike, which is very similar visually.

The fraudster sent the email using a newly created email address designed to closely mimic the legitimate vendor's email address. Specifically, the fraudster used the top-level domain, “.org,” while the legitimate vendor used “.com.” While VCD employees would not necessarily be expected to know the legitimate email domain of each County vendor, the signature portion in the fraudster email used the legitimate vendor's “.com” domain,

²⁴ Improving the Effectiveness of Your Claims Auditing Process, accessed at <https://www.osc.state.ny.us/sites/default/files/local-government/documents/pdf/2019-01/claimsauditing.pdf>

which does not match the domain of the fraudster's email address. This is a visible inconsistency. Anti-fraud training sessions commonly note that an internal inconsistency between the address the email was sent from and the web address in the signature portion is a red flag of impostor fraud.²⁵

VCD staff did not detect this red flag, possibly because they had not been trained to recognize it. Although providing VCD staff with such fraud awareness training would not have guaranteed red flag recognition, it would have equipped them with knowledge increasing the chance that they could detect a fraud attempt.

Accounting Division Staffer Was Not Trained in Significance of ACH Return Code; Red Flag Missed

As noted, on October 22, 2019, the bank provided the CO with an ACH Return Report notifying the County that three ACH transfers initiated on October 18, 2019, totaling \$1,384,858, had been rejected, with the return code of "R16-Account Frozen." According to NACHA's Operating Rules and Guidelines, the R16-Account Frozen code denotes, "Access to the account is restricted due to specific action taken by the RDFI [Receiving Depository Financial Institution] or by legal action."²⁶ The R16 return code can represent account restrictions imposed for a number of reasons that would be of potential concern to the County, such as illegal activity, tax liens, and judgments.²⁷

²⁵ OIG is aware that an entity may use different domains for web pages and email for entirely legitimate purposes. As with all red flags, such a discrepancy does not guarantee something nefarious. It does, however, indicate that further scrutiny is warranted.

The fraudster's email contained other, more subtle red flags. On the voided check image attached to the email, the name and address of the vendor on the check are slightly out of alignment with the rest of the print on the check, and therefore appears to have been superimposed on the check image. In addition, the job title shown for the vendor's employee is incorrect.

²⁶ Accessed at: <https://www.firstmid.com/wp-content/uploads/2014/02/2013-Corporate-Rules-and-Guidelines.pdf>

²⁷ PaySimple, a company that facilitates electronic payments for businesses, advises entities encountering the R16-Account Frozen code that, "This return code should be a red-flag for your business. If you see this code, be certain to do your due diligence around verifying the identity of your customer." Accessed at:

https://paysimple.com/help/Zions/ps30/a2-ach-return-codes/Directory_of_ACH_Return_Codes.htm

The Specialist who processed the subject ACH return told OIG that, while ACH returns happen on occasion, she could not recall ever receiving another ACH return notification with the R16-Account Frozen code. Rather, ACH returns more commonly occur because the receiving bank account was closed, or there was an error in the account/routing numbers. The Specialist also told OIG that the dollar amount of the rejected ACH payment in the subject incident was multitudes higher than the typical ACH rejection amount, which she estimated as ranging between \$50 and \$50,000.

The Specialist told OIG that she had not been provided guidance as to the significance of the ACH return codes, nor as to when to notify management of an ACH rejection. The Specialist told OIG she processed all ACH returns in the same manner, regardless of reason code, and she had not been directed to notify management of any of the rejections.

Accordingly, the Specialist followed the usual practice in responding to the subject ACH return, despite the atypical reason code and unusually high amount of the returned funds. Specifically, on October 23, 2019, she asked the user department (DPW) to contact their vendor and have it complete a new Form 700.²⁸ She did not escalate the matter of the ACH return, i.e., she did not notify anyone above her in the CO of the ACH rejection.

Controls Implemented After the Incident

CO Implemented Anti-Fraud Controls in the Wake of the Fraud Incident

Post-incident, the CO implemented new controls designed to guard against other vendor impostor attempts. These controls entailed the following enhancements to the Form 700 process:

- Requiring follow-up telephone contact with a vendor representative who is neither listed on nor submitting the Form 700 and its accompanying documents.

²⁸ The Deputy Comptroller explained that the purpose of completing a new form 700 is two-fold: to ensure the vendor's banking information is accurate going forward, and to verify the address to which a manual check can be mailed to replace the rejected ACH payment(s). A manual check would be used because NIFS would disallow a second attempt to send payment via ACH as a duplicate payment.

- Modifying the Form 700 to require, in the case of changes to banking information, both the original and new banking information.
- Sending confirmation emails to known vendor email addresses after changes are made.

These measures incorporated the following fraud risk mitigation strategies recommended by the GFOA:

- Confirm emailed change requests by telephone.²⁹
- Require both old and new banking information from vendor.
- Contact vendor using established contact information.³⁰

OIG concludes that the CO's new controls lessen the likelihood of another vendor impostor fraud being successfully perpetrated.

OIG reviewed a sample of 50 vendor information change requests submitted from January 1, 2020 through June 30, 2020³¹ and was able to verify that the CO had implemented, and its staff was following, these enhanced Form 700 process steps:

- Use of vendor contact control sheet to guide and document vendor verification contacts.
- Follow-up telephone contact with a vendor representative who is not named on the Form 700.
- Use of new Forms 700 requiring both original and new banking information.
- Dispatch of confirming emails after vendor information changes.

²⁹ This is also consistent with Wells Fargo's recommendation to always verify a change request through a contact method different from how the request was received. (https://global.wf.com/wp-content/uploads/2018/03/TM-3162_Impostor-Fraud-Checklist.pdf)

³⁰ Similarly, an article appearing in the January 2019 issue of Fraud Magazine, published by the Association of Certified Fraud Examiners, recommends verifying changes using established vendor contacts (Change-of-banking-details scheme defrauds quietly).

(<https://www.fraud-magazine.com/article.aspx?id=4295004197>)

³¹ This comprised a 29.7% sample of 168 requests to change vendor information submitted during this time period.

CO Made Quality Assurance Improvements to Vendor Information Management

The CO also implemented measures that, while not directly fraud-related, may be viewed as improving the overall process and increasing the likelihood that vendor payment information is accurate. These include:

- Use of a vendor contact Control Sheet to uniformly guide and track verification follow-up activities of CO staff.
- Verifications of infrequently paid vendors. Prior to approving any payments to a vendor who has not received a payment within the last three months, a representative of the VCD will contact the vendor to verify that the vendor information on file is correct. The purpose of this check is to proactively detect instances when vendors change bank accounts without notifying the County.

The CO also developed a draft written procedure that documents the workflow of Form 700 processing, as well as other functions of the VCD. However, this draft procedure has not been finalized.

Additionally, the CO advised OIG that:

- Vendor information changes will receive heightened supervisory involvement and scrutiny; the Fiscal Officer now reviews every Form 700 change request before his staff verifies and processes the request.
- The CO has assigned two full-time VCD staff members to Form 700 processing, with three additional employees designated as backups.

Appropriate Fraud Awareness Training Was Provided to VCD Staff

As noted, the CO provided two training sessions and training materials to VCD staff after the September 2019 fraud incident. OIG concludes that the two sessions were relevant to the prevention and detection of vendor impostor fraud. Training provided by the County's bank covered pertinent topics including email spoofing, vendor impersonation, and

lookalike domains. The GFOA webinar covered pertinent topics in vendor information security including payment fraud and verification of vendor information.³²

Two Other Fraud Attempts Were Unsuccessful

It should also be noted that, according to information the CO provided, two attempts at vendor impostor fraud were unsuccessful. As noted above, in September 2019, in a contemporaneous matter separate from the main subject of this report, a fraudster attempted to have a vendor's payment information changed. In this instance the fraudster did not provide a voided check or bank letter, even after the CO twice sent follow-up messages. As a result, the CO did not process the account change.³³

In December 2019, the true vendor submitted to the CO a change request, this one accompanied by a voided check. An auditor in the VCD compared the vendor's voided check to the Form 700 submitted in September and found that the account numbers did not match.³⁴ She addressed the discrepancy by emailing the actual vendor to request it submit a new Form 700. In a telephone conversation with the vendor, the auditor learned that the September request had not been legitimate; thus, the fraud attempt was revealed.³⁵ The CO did not, however, report to NCPD this fraudulent attempt to redirect County payments.

In a second, apparently unrelated matter, on September 8, 2020, when the new controls described above were in place, a person posing as the employee of a County vendor emailed the VCD requesting a "vendor ACH/EBT form." The Deputy Comptroller advised OIG that the Fiscal Officer noticed that the sender's email domain was ".net," while the true vendor's top level domain was ".com," and that the sender provided an area code and telephone number that did not correspond to the vendor's main office. OIG was informed that the Fiscal Officer, suspecting this might not be a legitimate request,

³² Additionally, after the inception of our review, the CO began periodically emailing a cybersecurity newsletter to its employees. It was explained to OIG that these newsletters form part of the CO's training efforts. The issues of the newsletter reviewed by OIG largely address consumer and personal computing concerns rather than threats facing the organization.

³³ As noted earlier, the requirement for providing a voided check or bank letter was part of the controls that existed in September 2019. It is possible, though not certain, that the lack of further action by the fraudster was attributable to the requirement for a voided check or bank letter.

³⁴ The employee's step of comparing a new request to a prior submission went beyond what was required by the new procedure.

³⁵ The vendor expressed the belief that its email had been somehow compromised.

telephoned the actual employee impersonated by the fraudster and was told that the vendor had not submitted any such request. The CO then notified the NCPD and OIG of the incident.

CO's Reporting of Vendor Impostor Fraud Attempts Has Been Inconsistent

While the CO has twice reported vendor impostor fraud schemes to NCPD, in October 2019 and September 2020,³⁶ it did not notify NCPD of the December 2019 fraud attempt discovery even though that matter too was an apparent attempt to defraud the CO into diverting payments to an unauthorized account.³⁷ OIG notes that even attempts to commit crimes are of concern and may constitute criminal conduct in violation of the Penal Law.

OIG concludes that the CO did not consistently ensure that NCPD was notified when the CO had reason to believe that a vendor impostor fraud pertaining to County funds may have been attempted.

CO Lacks a Comprehensive Fraud Risk Assessment

While new controls implemented by the CO follow a number of recommended strategies for preventing the type of fraud committed in early September 2019, that is but one fraud scheme; organizations controlling or expending funds may be susceptible to other types of fraud as well. Proactively identifying the range of fraud schemes which pose potential threats to the CO and County funds may be accomplished via the performance of comprehensive fraud risk assessments. According to the Fraud Examiner's Manual, published by the Association of Certified Fraud Examiners (ACFE), the purpose of a fraud risk assessment is to "help an organization recognize what makes it most vulnerable to fraud. Through a fraud risk assessment, the organization is able to identify where fraud is most likely to occur, enabling proactive measures to be considered and implemented to reduce the chance that it could happen."³⁸

³⁶ In addition to NCPD, the CO notified OIG of the September 2020 fraud attempt. The CO did not notify OIG of either of the two preceding incidents.

³⁷ The Comptroller related the December 2019 discovery to the Finance Committee.

³⁸ Association of Certified Fraud Examiners. (2012). *Fraud Examiner's Manual* (U.S. Edition). Austin TX: ACFE., p. 4.703.

Similarly, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) advises that: "The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and

OIG was advised that to the knowledge of the Deputy Comptroller and Fiscal Officer, no comprehensive fraud risk assessment of the CO had been recently conducted, i.e., at least under the current administration.

Following the inception of this review, OIG was advised that the CO has contracted an independent auditing firm to assist, among other things, in an assessment of the CO's cybersecurity needs. The Deputy Comptroller advised OIG that this firm's scope of work will include identifying fraud risks to the CO. The scope of work shown to OIG during the review clearly reflected appropriate targeting of potential fraud schemes involving social engineering, but as we noted in our draft report the extent to which other risk areas would be addressed was less clear. In their response to OIG's draft report, the CO informed OIG that it will conduct a comprehensive fraud risk assessment and that it has retained a consultant to perform an internal control and fraud risk assessment of all procedures across all Divisions. The complete details of the CO's response appear in appendices A and B.

risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks. (COSO: "Fraud Risk Management Guide Executive Summary," accessed at <https://www.coso.org/Documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf>)

Recommendations

While OIG concludes that the CO's new controls lessen the likelihood that another vendor impostor fraud will be successfully perpetrated, OIG recommends that the CO take the following additional actions to strengthen its control environment:

Further Strengthen Controls Through Periodic, Comprehensive Fraud Risk Assessments

Fraud risks are not limited to the one type of scheme that is the subject of this review. Proactive steps to identify and mitigate other types of fraud can reduce the need to deal with adverse impacts after the fact. OIG believes that it is beneficial to conduct comprehensive fraud risk assessments to guide management as to where additional controls are warranted. As noted, the Deputy Comptroller advised that the CO has contracted an independent auditing firm to, in part, identify fraud risks to the CO. OIG recommends that the CO ensure that this exercise comprehensively identifies the full range of fraud risks. OIG also recommends that comprehensive fraud risk assessments be conducted periodically, including when there is a significant change in the control environment.

The CO's response to this recommendation in OIG's draft report stated in part that "[t]his is being done." The CO advised in part that it has retained a consultant to conduct an internal control and fraud risk assessment of all procedures across all Divisions. Their full response, appearing in appendices A and B, elaborates on their efforts.

Provide Fraud Awareness Training for VCD staff on a Recurring Basis

CO staff will be more likely to recognize red flags and apply the appropriate level of scrutiny if they are regularly trained to spot such indicators. If the CO has not already made plans to do so, OIG recommends that the CO continue to provide formal anti-fraud training to VCD staff such as that delivered in February 2020. As the effectiveness of such training will depend in part upon its recency, such training should be given at regular intervals (e.g., annually). It is recommended that such training address fraud prevention, fraud detection, and the prompt reporting of suspicious activity. Findings emerging from fraud risk assessments can help to focus training on relevant topics.

The CO's response to this recommendation in OIG's draft report stated in part that "[t]his has been done and is being done on an on-going basis." Their full response, appearing in appendices A and B, elaborates on their efforts.

Train Accounting Division Staff on Significance of ACH Return Reason Codes

The CO should provide training to Accounting Division staff responsible for receiving and responding to ACH rejection notifications regarding the significance of the ACH R16 return code and any other code that may signify potential risk exposure for the County. The training should include guidance as to when and to whom in management ACH rejection reports should be escalated.

The CO's response to this recommendation in OIG's draft report stated in part that "[t]his has been completed." Their full response, appearing in appendices A and B, elaborates on their efforts.

Expedite Issuance of Pending Written Procedure for Vendor Information Change Processing

As of the writing of this report, the Form 700 processing procedure remains in draft form and, according to the Fiscal Officer, is not yet available to guide staff. Given the importance of the new anti-fraud controls built into this procedure and desirability of having staff implement those controls, the CO should finalize and promulgate the procedure as soon as possible.

The CO's response to this recommendation in OIG's draft report stated in part that "[t]his is being done." Their full response, appearing in appendices A and B, elaborates on their efforts.

Ensure Consistent Reporting of Fraud Attempts

The CO should ensure that it consistently notifies appropriate law enforcement authorities, such as NCPD, when it has reason to believe that a vendor impostor scheme or other fraud pertaining to County funds has been committed or attempted, subject to mutually agreed reporting protocols between the Comptroller's Office and such law enforcement agencies.

The CO's response to the draft version of this recommendation stated in part that this was completed and that the CO "will continue to consistently convey confirmed instances of fraud and illicit activity to law enforcement." Their full response appears in appendices A and B.

- # -

APPENDIX A

Comptroller's Office Response, with OIG's Follow-up Comments

Below is the content of the Comptroller's Office's (CO's) written response to this report, accompanied by OIG's comments added in **blue bolded print**. Note that Appendix B contains the CO's response letter as received, on its original letterhead.

Hon. Jack Schnirman

Nassau County Comptroller

OFFICE OF THE NASSAU COUNTY COMPTROLLER
240 Old Country Road Mineola, New York 11501
Tel: (516) 571-2386 Fax: (516) 571-5900
nccomptroller@nassaucountyny.gov

November 5, 2020

Jodi Franzese, Inspector General
Nassau County Office of the Inspector General
One West Street
Mineola, NY 11501

Dear Inspector General Franzese:

In accordance with §191 of the Nassau County Charter, the Office of the Nassau County Comptroller herein submits its comments with respect to your draft "Review of 2019 Vendor Imposter Fraud Incident."

Reform and Collaboration

Since the appointment of the Inspector General (IG) in December of 2018, the Office of the Nassau County Comptroller (Comptroller's Office or Office) has worked collaboratively with the Office of the Inspector General (OIG) to reform the County. Many of these collaborative reforms have been to Nassau County's (County) contracting and procurement processes, which is of "particular" concern to the OIG; "(t)here is hereby established an independent office of the Inspector General which is created in order to provide increased accountability and oversight of County operations, to detect and prevent waste, fraud, abuse and illegal acts in programs administered or financed by the County, *particularly the County's contracting and procurement processes*, to promote transparency, efficiency and integrity in the County contracting and procurement process" [Nassau County Charter, Article 1-C §185, emphasis added]. Together this Office and the OIG have contributed and continues to contribute to reforming the County Procurement Policy, procurement procedures, solicitation tracking, the disclosure process, and a variety of other issues that make our County government more transparent and accountable.

Indeed, the necessity for collaboration between the OIG and the Office of the Comptroller is recognized by the County Charter, which requires that all reports, such as the one this Office is commenting on herein, "shall be furnished to the County Executive, *and the County Comptroller* as well as the Presiding Officer and the Minority Leader of the County Legislature" [Nassau County Charter, Article 1-C §192(1), emphasis added]. It is of no surprise then that the exchanges between

the OIG and this Office during the review process here served both to improve upon the reforms this Office has already implemented since 2018 and to develop the OIG's understanding of many of the County's processes, which in turn will assist the OIG in its overall reform goals.

The establishment of the IG's Office was a major reform for Nassau County. In the Nassau County District Attorney's July 2015 "Special Report on the Nassau County Contracting Process" it was specifically recommended that "[t]he Legislature should modify the County Charter to eliminate the position of Commissioner of Investigations due to its history of ineffectiveness, and replace it with an independent and adequately staffed County Inspector General, appointed by the County Executive and confirmed by a supermajority of the County Legislature" [Section V(8)].

It is with this reform objective in mind and in furtherance of collaboration and good government, that this Office has welcomed the IG's review of its procedures and controls regarding vendor payment information processing (vendor registration) and the reported fraud incident of late 2019.

Purpose

Presumably in furtherance of independence, the OIG is empowered to initiate audits, investigations, inspections, examinations and reviews on its own initiative. The OIG is supervised by the County Legislature- "The County Legislature shall create a legislative committee within the County Legislature for the purpose of maintaining general supervision of and liaison with the Office of the Inspector General" [Nassau County Charter, Article 1-C §189(2)] - and its activities are bi-annually reviewed by Nassau County Legislature - "The Inspector General shall meet with representatives of the Majority and Minority delegation of the Nassau County Legislature every six months to review the previous six month's activities and the Inspector General's plans and objectives for the upcoming six months" [Nassau County Charter, Article 1-C §192(2)]. It is clear from their report, and from communications with the OIG throughout this review, that the IG initiated this review in response to a letter from the Deputy Presiding Officer of the Nassau County Legislature and that the IG would not have independently initiated this review but for the insistence of the Legislature.

OIG Comment:

While the OIG may receive requests from entities, such as the Legislature, County Executive or County Comptroller, to conduct reviews or other oversight activities, the decision in each instance as to whether in fact to grant such request is wholly within the discretion and independent judgment of the Inspector General, as is the manner in which the OIG conducts the activities it chooses to undertake. It is the Inspector General who independently makes these decisions. In this instance, the safeguards for the County's funds are squarely within the OIG's appropriate areas of concern. Moreover, not only did the Inspector General view the subject of our report as a fully legitimate and compelling topic for OIG oversight, that the OIG had an interest in the matter pre-dating the request is evident from the fact that the Inspector General (as well as members of her staff) observed the Finance Committee hearing, two days earlier, on her own initiative.

The Inspector General takes seriously the language in Section 185 of the Charter “that no interference or influence external to the Office of the Inspector General compromises or undermines the integrity, independence, fairness and objectivity of the Inspector General in fulfilling the statutory duties of the office or deters the Inspector General from zealously performing such duties.” If the Comptroller’s comments are meant to suggest that the OIG did not exercise independence, and that its review is thereby tainted, the OIG must disagree in the strongest terms.

Transparency

The Nassau County Comptroller is committed to transparency and reform. One cannot be achieved without the other. At the time the events subject to this review took place in late 2019, municipalities throughout the Country were increasingly under attack by newly developing threats using technology, including phishing and ransomware incidents. As such in the interest of transparency, to assist other municipalities in dealing with these developing threats, this Office along with the Nassau County Police Department, made this matter public. This action was frankly, antithetical to a County government that has shown historically to be susceptible to cover-ups and corruption. As a result of these actions, those in County government and a number of municipalities had been forewarned to implement measures (as did our Office) to combat such fraud, the public at large was further educate about the nature of such frauds and the IG was asked by the Legislature to conduct this welcomed review. In February of 2020, Suffolk County initiated a cybersecurity project. All of these are positive actions which foster collaboration, cooperation, good government and reform.

Note as to the OIG Recommendations:

As noted above, the OIG is required to publish its reports to, amongst others, the County Comptroller. To date our Office has not received any other OIG reports of any reviews of any other office, entity or department. Based upon seeing no previous such reports and based upon representation made by the OIG during the course of their review process, all indications are that this is the first such “review” conducted by the first ever County IG. Our Office has been cooperative with this review and indeed, as the first Office subject to such a review has been cooperatively discussing best practices for conduct of such reviews as both the IG, her staff and our Office have much experience in conducting reviews, investigations and audits.

As also noted above, it is clear the OIG would not have independently initiated this review. Given the cooperative roles that the OIG and the Comptroller’s Office play, it seems to be a poor use of OIG resources to make such formal recommendations. It is clear that the OIG could easily have cooperatively and collaboratively reviewed and informed our Office of any control gaps they identified in their review and of any actions they concluded we should take to improve our such controls. The IG is empowered to determine if it is or is not appropriate to publish and deliver a report or recommendation [Nassau County Charter, Article 1-C §191] and in the alternative to “recommend remedial actions and may provide prevention and training services to County officers, officials, employees, and any other persons covered by this Article....[t]he Inspector General may follow up to determine whether recommended remedial actions have been taken” [Nassau County Charter, Article 1-C §187(12)].

OIG Comment:

The OIG reiterates that the decision whether and in what manner to initiate and conduct a review is wholly within the discretion and independent judgment of the Inspector General, and that in any event, OIG's interest in the subject topic preceded the request it received. Likewise, the OIG independently determines when and to whom its reports are issued, consistent with its understanding of its mission and applicable law. OIG does not understand the relevance to this review of the Comptroller's comments about other reports of the OIG.

Points of Clarification

- The Office of the Comptroller AUDITS AND APPROVES claims for payment.
- The County Treasurer signs the checks.
- Vendors may choose to permit payments to be made by check.
- Vendors may choose to permit payments made by electronic payment (Automatic Clearing House or ACH).
- The Office of the Comptroller maintains the various vendor payment information in the County financial system for each vendor, such as:
 - where to send a check if a claim is being paid by check
 - bank account(s) information if payment is being made by electronic payment.
- If the vendor has multiple payment methods in the financial system, they will select which method of payment should be used for each claim when the claim is submitted for review.

► COMMENTS ON THE OIG RECOMMENDATIONS

Note: the report recommendations are not numbered as such our responses cannot be correlated by number.

•OIG RECOMMENDATION

Further Strengthen Controls Through Periodic, Comprehensive Fraud Risk Assessments

COMPTROLLER'S OFFICE COMMENTS:

This is being done: Our Office is in the midst of this process. The Comptroller's Office has retained a consultant to conduct an internal control and risk assessment which includes a gap analysis and recommendation for mitigation including the areas of vendor registration fraud and cybersecurity. Our Office will review recommendations for any procedural changes to mitigate any identified gap in the risk analysis, including the development within our Office of a Security Awareness Program, or even working with the County Information Technology Department (IT) to implement this Countywide. We have been advised that this is a first and necessary step in conducting any such assessment. See below for details.

•OIG RECOMMENDATION: Provide Fraud Awareness Training for VCD staff on a recurrent

basis

COMPTROLLER'S OFFICE COMMENTS:

This has been done and is being done on an on-going basis: The Comptroller's Office staff had received training prior to, and post the incident, and continues to receive such training. Our Office will work to develop within our Office a Security Awareness Program. See below for details.

•**OIG RECOMMENDATION:** Train Accounting Division Staff on Significance of ACH Return Reason Codes

COMPTROLLER'S OFFICE COMMENTS:

This has been completed: The Comptroller's Office staff has received such training. The staff acted in accordance with all recommended guidance, including the OIG / National Automated Clearing House Association (NACHA) guidance for rejections noted in the OIG review report. The staff took the necessary actions required by the constraints of the County financial system, which resulted in recovery of all diverted funds. All ACH rejections are being escalated to the Division Head and the Deputy Comptroller level for review. See below for details.

•**OIG RECOMMENDATION:** Expedite Issuance of Pending Written Procedures for Vendor Information Change Processing

COMPTROLLER'S OFFICE COMMENTS:

This is being done: The Comptroller's Office has obtained a consultant to conduct control review, risk assessment and gap analysis of all our procedures, including the vendor registration process. Final publication will be completed once our Office has been able to incorporate any procedural changes effectuated as a result of this review into these procedures. See below for details.

•**OIG RECOMMENDATION:** Ensure Consistent Reporting of All Fraud Attempts

OIG Comment:

The draft recommendation has been reworded to: “Ensure Consistent Reporting of Fraud Attempts.”

COMPTROLLER'S OFFICE COMMENTS:

Completed: The Comptroller's Office has consistently reported all known incidents of fraud since the incident under review that was the subject of the OIG report. See below for details.

► **COMMENTS ON EXECUTIVE SUMMARY, FINDING AND CONCLUSIONS**

Note: the report findings and conclusions are not numbered, as such our responses cannot be correlated by number.

WITH RESPECT TO:

•OIG Executive Summary: "OIG further determined that the internal controls the CO had in place at the time for the vendor information change process were not effective in preventing the fraud scheme and that its staff was not trained to detect such fraud."

•OIG Conclusion: "CO's Then-Existing Controls Were Ineffective in Preventing the Subject Fraud: Were Not Consistent with Recommended Mitigations Strategies."

•OIG Conclusion: "Pre-Incident Controls Thwarted but Did Not at the Time Detect Another Fraud Attempt."

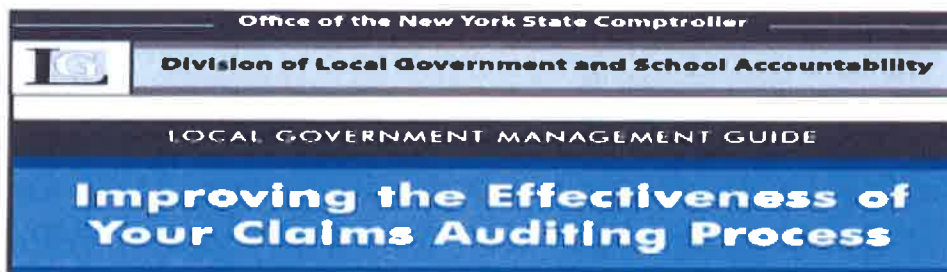
COMPTROLLER'S OFFICE COMMENTS:

•The Comptroller's Office has been improving controls over the vendor registration process based upon Governmental Finance Officers Association (GFOA) and other guidance since January of 2018, immediately upon the new Comptroller taking Office. These additional controls included:

- (1) requiring verification of bank account number in the form of either a voided check or a bank account confirmation letter;
- (2) requiring dual verification within the Claims Division of changes made to a vendor's profile in the financial system;
- (3) requiring a verification of Vendor Tax Identification Numbers (TINs) prior to making entry into NIFS - utilizing the IRS' free application;
- (4) and deactivating the ability of a vendor to receive a payment if this verification fails.

•These new controls were implemented prior to the incident subject to the OIG review and had thwarted a similar incident - which the OIG has acknowledged.

•The Comptroller's Office provided the OIG with materials demonstrating that the Vendor Claim Division was trained on electronic vendor fraud prior the incident, including:



Red Flags

Claims with certain characteristics may have a higher risk of error or fraud. Officials should use common sense and reasonable skepticism when any claim appears to be out of the ordinary. Even when all required documentation is submitted, remain skeptical, especially of claims that are not routine. In today's electronic environment, anyone with a computer and printer may be capable of replicating and manipulating information to produce false documentation. Particular attention should be paid to claims with the following characteristics:

- Missing documents
- Unavailability of original documents
- Recurring identical amounts from the same vendor
- Multiple remittance addresses for the same vendor
- Inconsistent, vague, or implausible responses arising from inquiries or analytical procedures
- Excessive voids or credits
- New vendors, especially if payment goes to a post office (PO) box
- Items purchased that are not clearly identified
- Goods delivered outside of a central location or to an unusual delivery point
- Credit card charges with no original receipts attached
- Travel and conference claims
- Alterations or questionable handwriting on documents
- Duplication
- Payments to a vendor that have increased dramatically for no apparent reason
- Payments to vendors for construction work not certified as completed by your architect or engineer
- Unusual delays in providing requested information
- Tips or complaints about possible fraud.

•In concluding that our Office's controls were not consistent with then recommended mitigation strategies, the OIG relies upon a GFOA citation to <https://www.gfoa.org/materials/electronic-vendor-fraud> presumably found by the OIG in doing open source research on the issue.

•**This guidance, it seems, was published on the GFOA website on December 2, 2019, after the incident** and after our Office has implemented these best practices safeguard and internal controls which have since been used effectively to mitigate the risk of fraud.

•The late 2019 fraud incident took place at a time when technology related schemes began affecting municipalities throughout the Country.

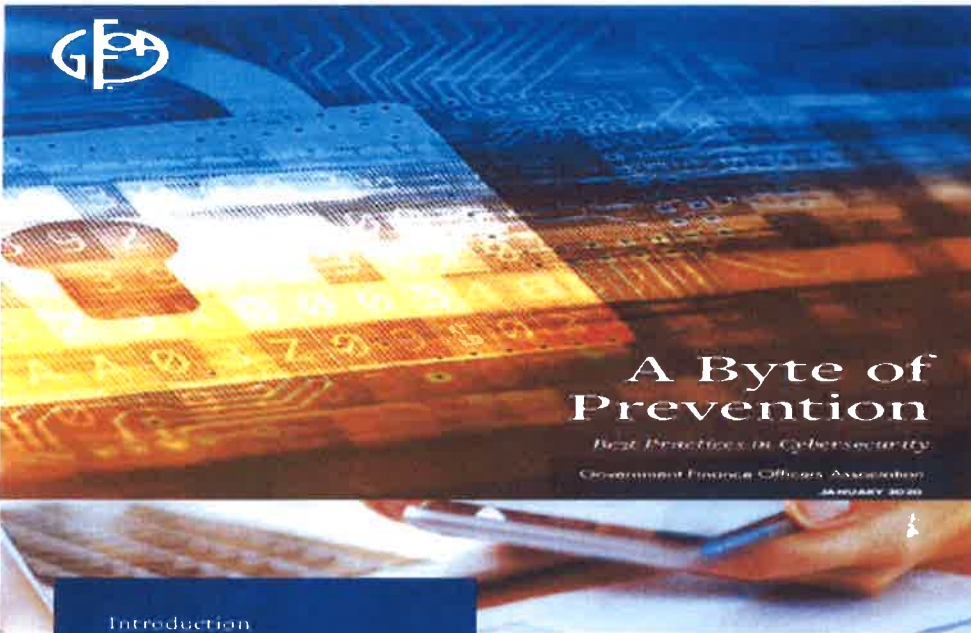
•As a response to the proliferation of such schemes, those responsible for providing guidance on governance and controls, both for-profit entities and professional advisory organizations, such as accounting firms and the GFOA began to actively focus their publication, webinars, emails, newsletters and other literature on such schemes, including electronic vendor fraud, such as these from *January 2020* and *February 2020*:

Essential Tools for Effective Payables Policies and Procedures in the Treasury Office



GOVERNMENT FINANCE OFFICERS ASSOCIATION

Webinar
February 20, 2020
1-3PM CT



Introduction

All local governments are potential targets for cybercrime, a risk that intensifies as victims increasingly pay ransoms to regain access to their hacked technologies. It can be tempting to pay up, because hacks are disruptive, damaging, and embarrassing – and expensive. As stewards of (often sensitive) public data, finance officers must understand the significance of this threat, including the large costs governments face in recovering lost data, restoring public trust, and otherwise recovering from a breach.

Finance officers can implement simple and inexpensive strategies that address people, process, and technology to protect their organizations from cyber threats without conducting a costly cybersecurity assessment. Many of the recommendations on the following pages address the weakest link in cybersecurity: the human factor.

1 | Employee Awareness

Most breaches begin with an e-mail or file attachment. Employees in the finance department are likely targets because they have frequent transactions with vendors and access to business systems. To mitigate this threat, governments should train employees to:

- Be suspicious.
- Be wary of e-mails asking them to change their usernames or passwords.
- Double-check the sender's e-mail address before opening or downloading an attachment.
- Follow the government's compliance business processes when vendors request changes to electronic payment and bank account information (e.g., accounts payable) and staff members (e.g., direct deposit). These procedures are often "out-of-band" (i.e., not done by e-mail) and are therefore likely to expose wrongful requests.
- Check the sender's website address before entering or sending sensitive data.
- Periodically check the public website haveibeenpwned.com to see if their e-mail addresses and passwords have been exposed. If so, employees should report the breach and change passwords for the accounts listed.

(Continued on page 1)

OIG Comment:

OIG did note the controls which existed in September 2019. We were informed in sum that these controls were implemented to reduce errors in vendor information. Obviously, the subject fraud occurred in September 2019 notwithstanding those controls.

We were also informed in sum that prior to September 2019 the staff was not trained to detect fraud in processing the Form 700. OIG does not minimize the importance of the staff training in August 2019, but it addressed processing or auditing claims for

payment submitted by vendors; fraud was a small part of this training and in the context of vendor claims. Unlike the subsequent training, it did not address fraud detection in connection with vendor impersonation, spurious emails, or the changing of banking information.

The GFOA advisory guidance cited by OIG was not novel and existed prior to September 2019. The GFOA Board approved the guidance two years earlier, in September 2017, GFOA delivered a webinar on the topic in November 2017, and the guidance was available on GFOA's website as early as May 2018. According to GFOA, its website later underwent an overhaul, which may be why the advisory published in 2017 may now appear to have been published in late 2019.

WITH RESPECT TO:

•OIG Executive Summary: "The bank notified the CO of the account freeze on October 22, 2019. Two day later, the CO learned, as a result of the communications from the true vendor, that the deposits had been fraudulently diverted, and the CO accordingly notified the Nassau County Police Department (NCPD)."

•OIG Finding: "Accounting Division Specialist Requested that the Actual Vendor Submit a New Form 700."

•OIG Finding: "The CO's practice in the event of an ACH return was to confirm the payee's correct address and to manually generate a paper check to replace the rejected electronic payment. On October 23, 2019, the Specialist followed this practice by emailing a blank form 700 to two employees in the Financial Services Unit of DPW."

•OIG Conclusion: "[T]he Specialist followed the usual practice in responding to the subject ACH return, despite the atypical reason code and unusually high amount of he returned funds. Specifically, on October 23, 2019, she asked the user department (DPW) to contact their vendor and have them complete a new Form 700. She did not escalate the matter of the ACH return (citation omitted)."

•OIG Conclusion "The Vendor Detected the Fraud."

•OIG Conclusion: "Accounting Division Staffer Was Not Trained in Significance of ACH Return Code: Red Flag Missed."

COMPTROLLER'S OFFICE COMMENTS:

•The OIG infers that the Accounting Systems Specialist who handled the ACH rejections was oblivious to the notion that anything unusual was happening. This notion simply lacks the appreciation for the action taken by Accounting Systems Specialist to uncover the additional diverted funds, lacks the understanding of the reasons those actions were taken (in complete disregard of the very guidance they cite), and appears to lack the appreciation of the basis for the actions taken being due to the limitations of the County financial system.

•The Accounting Systems Specialist initiated the protocol to obtain and verify an alternative form of payment. The Accounting Systems Specialist acted in accordance with all recommended guidance (including the OIG/ National Automated Clearing House Association (NACHA) guidance for rejections noted in the OIG review report), and took the necessary action required by the constraints of the County financial system, which resulted in recovery of all diverted funds.

OIG Comment:

OIG did not infer that the Accounting Systems Specialist was oblivious; rather, she informed OIG that she noticed that the ACH return code was unusual in two respects: 1) That it was an R-16 Account Frozen Code, which she did not recall seeing before, and 2) the size of the return, in excess of \$1.3 million, was far larger than typical returns. She did not, however, escalate her observations to management's attention, because she had not been instructed to handle an R-16 rejection any differently from the standard procedure for other returns, nor was she trained to understand the potential implications of the R-16 code.

While NACHA defines the code, the guidance cited is that of PaySimple.

•The OIG's own citation concerning the R-16 rejection code (see below), used to reach their conclusions, recommends that the action to take is to **obtain a different form of payment**. The citation indicates that there are *common reasons* that this rejection code is used, and it *may, on a more exceptional basis* indicate that there is suspicious activity (see below).

OIG Citation: [https://paysimple.com/help/Zions/ps30/a2-ach-return-codes/Directory of ACH_Return Codes.htm](https://paysimple.com/help/Zions/ps30/a2-ach-return-codes/Directory%20of%20ACH_Return%20Codes.htm)

R16 Account Frozen

NACHA Definition:	1) Access to the account is restricted due to specific action taken by the RDFI or by legal action; or 2) OFAC has instructed the RDFI or Gateway to return the Entry.
What it Means:	The payment cannot be honored because the account has been frozen and no transactions can be processed against it.
What to Do:	<p>Contact your customer to obtain a different form of payment. You will not be able to process transactions using this bank account until it is un-frozen.</p> <p>There are several common reasons why a bank account may be frozen, such as a civil legal dispute over an unpaid debt. However, you may also see this code if OFAC has frozen the account or the individual payment due to suspicion of terrorism-related activity. (OFAC stands for the Office of Foreign Assets Control, which is an agency of the United States Department of the Treasury under the auspices of the Under Secretary of the Treasury for Terrorism and Financial Intelligence.)</p> <p>This return code should be a red-flag for your business. If you see this code, be certain to do your due diligence around verifying the identity of your customer.</p>

•The Accounting Systems Specialist was following protocol in place by our Office and these protocols are the exact protocols indicated by the OIG that should have been followed according to their citation.

OIG Comment:

OIG acknowledged the Specialist followed the Office's protocols and does not dispute the necessity of the Specialist's actions to facilitate paying the legitimate vendor. The issue here, however, is that the Office protocol made no additional provision for the type of situation we reviewed. The Specialist told OIG that she handled all rejection reports the same way, and she never notified a supervisor of ACH rejections. OIG points out the above cited language that: "This return code should be a red-flag for your business. If you see this code, be sure to do your due diligence around verifying the identity of your customer."

•Furthermore, because the current financial system is limited and will not permit another ACH transaction for the same claim, the *County's* procedure, is to initiate a paper check transaction to be mailed to the vendor to replace the rejected ACH payment. To effectuate this transaction, the County procedure is to verify the address to send such a paper check via the submission of a W9/700 Form, so that proper protocols and controls are followed verify the information before the check is sent to. The OIG demonstrated their lack of appreciation for this limitation as they only noted this in a footnote in their report.

OIG Comment:

This point was footnoted because, while the constraints of the County's financial system may well necessitate identification of an alternate means of sending payment to the legitimate vendor, those system constraints do not prevent, and should have no bearing on, exploring the reason that a frozen account report was generated. System payment constraints are irrelevant to instructing the Specialist to elevate to management an unusual occurrence like a sizeable rejection due to a frozen account.

The CO's protocol at the time sought to facilitate an alternative method of payment and obtain banking information. The protocol did not provide for flagging the unusual R16 rejection reason code for management review, even though it could potentially signal fraudulent activity or adverse legal and/or financial information about the vendor; information that might be of concern to the County. OIG notes, in any event, that the Comptroller's Office has reported that all ACH rejections are now being escalated for management review.

•In following the protocols and initiating this control, the Accounting Systems Specialist set in motion a series of events and correspondences between our Office, DPW and the Vendor which, in short order, revealed the additional diverted funds. By taking these actions, and initiating these series of email exchanges, the additional diversions were detected and all money was recovered.

•A closer look at the chain of events through these emails, indicates 24 hours and 46 minutes between our Office alerting DPW of the rejection (as per correct protocol noted above) and the Deputy Comptroller and then the Nassau County Police Department (NCPD) being notified of the confirmed fraud and diversion of the additional funds.

•During this *one* day period in which there was constant communication between the Vendor, DPW and our Office, the Vendor was put on notice, worked with the County, DPW, our Office, and other County Offices to identify the additional diversions.

•Even accounting for the time between when the Accounting System Specialist received the initial email from the bank, late in the day on October 22, 2019, to the time the Accounting System Specialist initiated the protocol by sending an email to DPW, the next morning, the time frame between the email notification and the report to the Deputy Comptroller and the NCPD is less than 48 hours.

•The OIG report agrees factually with all of the timelines concerning these email exchanges which were necessary to uncover the additionally diverted funds – although the OIG report spuriously notes only the dates of these exchanges and not the timing of these exchanges, which actually occurred over a *one* day period.

OIG Comment:

OIG's report makes clear that the events in question spanned a short period of time, October 22 through October 24, 2019, and OIG did not suggest that the time was

unduly long. Moreover, as all cited communications are clearly shown as occurring in the even more compact timeframe of October 23rd through October 24th, there was nothing spurious in the OIG's recitation of events. Specific times were omitted for ease of reading. The sequence of events demonstrates that: 1) it was the vendor who recognized the presence of fraud, and 2) that once this happened on October 24th the Comptroller's Office notified NCPD the same day.

WITH RESPECT TO:

- OIG Finding: "CO Conducted a Look Back Review; Confirmed the Validity of Some Vendor Change Request."
- OIG Finding: "After the fraud came to light, the CO in 2019 performed a review (look back) of some of the Form 700 processed during the period of January through September 2019."
- OIG Conclusion: "The CO's Look Back Verification was Partial, Extent is Unclear."
- OIG Conclusion: "The CO conducted a look back review and verified Form 700 changes made to some of the County's vendors."

COMPTROLLER'S OFFICE COMMENTS:

- Simply put, the Comptroller's Office reviewed all W9/700 Forms submitted between January 2019 and the incident.
- This review implemented the recommended best practices in identifying red flags concerning electronic vendor fraud.
- None of the vendor requests and the information submitted during this period had any such red flags and there were no instances found of any entity, other than the actual vendor, having submitted the W9/700 Form.
- In addition, to the above review, which had negative results for red flags, the Office additionally verified selected vendors with frequent high dollar payments, vendors with multiply suffixes in the financial system (multiple payment methods) and/or vendors who were adding or changing banking information during the period (as opposed to a change of address or other information).
- This process overlapped with the implementation of a three month look back period for payment approvals, requiring that any vendor payment going to a vendor who has not received a payment in the last three months, before such a payment can be approved, the vendor must be contacted to verify their payment information. The OIG was informed that as of the date of their inquiry on this matter (July 2020) the information was verified in this manner of 534 vendors, 42 of which required changes to their information which were effectuated using all of our updated procedures.

OIG Comment:

OIG corrected the draft phrasing in the second cited finding; it should have not included the words "some of." The wording of that finding now conforms to the other finding and associated conclusions.

To be clear, there is a difference between the Comptroller's Office review of the Forms 700 and the verification exercise. The former as described was essentially a screening of the forms. The Comptroller's Office informed OIG that it screened all Forms 700 received during a nine-month period in 2019. The verification activity was a validation process which entailed contacting selected vendors to confirm their changes.

According to information the Comptroller's Office provided to OIG (and confirmed in its comments above), of the total population reviewed (screened), only in selected instances did the Comptroller's Office take the additional step of verifying with the vendor the changes reflected on the forms. OIG did not question that this was done but noted that only a subset of the total population was verified. As the Comptroller's Office was not able to provide the OIG with a list of the vendors contacted for verification during its lookback, the extent of that verification process remains unclear.

The Comptroller's Office commented to the effect that there was an overlapping verification of 534 vendors who had not received payment in the prior three months. Again, OIG does not question this, but would point out that, to our understanding: (1) the extent of overlap of the two processes is unknown to OIG; (2) the three month no-payment lookback was a separate exercise, rather than being part of the nine month lookback; and (3) the three month exercise was differently focused, i.e., revealing vendors who had changed their banking information without notifying the County (found to be 42), rather than confirming the prior requests of vendors who had wanted the County to change their banking information.

WITH RESPECT TO:

•OIG Conclusion: "CO's Reporting of Fraud Attempts Has Been Inconsistent."

OIG Comment:

The draft wording of this conclusion has been revised to read: "CO's Reporting of Vendor Impostor Fraud Attempts Has Been Inconsistent."

•OIG Conclusion: "OIG notes that even attempts to commit crimes are of concern and may constitute criminal conduct in violation of the Penal Law."

•OIG Conclusion: "OIG concludes that the Comptroller has not consistently ensured that proper authorities were promptly notified when the CO has reason to believe that a fraud pertaining to County funds may have been committed or attempted."

OIG Comment:

The draft wording of this conclusion has been revised to read: "OIG concludes that the Comptroller did not consistently ensure that NCPD was notified when the CO had reason to believe that a Vendor Imposter Fraud may have been attempted."

COMPTROLLER'S OFFICE COMMENTS:

•The Comptroller's Office has worked with and continues to work with our partners in law enforcement to report instances of fraud or other possible illicit activities concerning the County. The Office regularly transmits such findings to law enforcement, including the Nassau County District Attorney's Office and the Office of the New York State Attorney General. The Comptroller's Office is an investigative body which has and will continue to consistently convey confirmed instances of fraud and illicit activity to law enforcement.

•There were two attempts in September of 2019. One early in September of 2019 resulted in the matter which is the subject of the OIG review and other later in September of 2019. As noted by the OIG, the Comptroller's Office controls in place at the time thwarted the late September 2019 incident; it was revealed that the request of the fraudster was not processed because the fraudster never follow-up in submitting a cancelled check. The additional controls put in place by this Office after September of 2019 then detected the earlier attempt by the fraudulent vendor when the actual vendor sought to update their vendor information. As such, the controls put in place by this Office did both thwart and detect this incident.

•As noted above, the Comptroller's Office has continually improved, and will continue to, improve, controls based upon GFOA and best practice guidance. As these best practices changed, and in response to the incident subject to the OIG review, we developed our controls. As such there was a lag in time, which clearly would not happen with the new controls in place, between the thwarting of the later September 2019 incident and the detection of the incident. Given the delay between the thwarting of the incident and the identification there would be little value starting an official NCPD investigation into the matter. Nevertheless, the NCPD was aware of the incident. It is not clear from the OIG if in reaching their conclusion the OIG confirmed with the NCPD if the NCPD had a record this incident.

•The OIG writes that "even attempts to commit crimes are of concern and may constitute criminal conduct in violation of the Penal Law." It is noted that during the January 22, 2020 Finance Committee hearing on this matter, the IT Department reported that "last week we actively blocked 1,100 phishing attempts into the county." Is the IG requiring a report be made for each and every phishing attempt? 1,100 per week equates to over 57,000 attempts per year. Has the OIG discussed their requirement with the NCPD? Perhaps the OIG is imposing such a requirement because the Nassau County Charter, Section 187(5) requires that "[w]here the Inspector General suspects a possible criminal violation of any state, federal, or local law, he or she *shall forthwith notify the*

appropriate law enforcement agencies [emphasis added]. Has the OIG, given their broad investigatory authority and authority to "receive, review, and investigate any complaints regarding any County-funded projects, programs, contracts, purchase orders, agreements or transactions, and all other activities, or operations of the County Executive and County agencies" [Nassau County Charter, Section 187(5)], "suspected" and reported numerous criminal violations?

OIG Comment:

OIG was informed that NCPD had no record of receiving a notification of the second September 2019 incident; additionally the Deputy Comptroller/Chief Counsel told OIG that to his knowledge his office had not reported it to NCPD, which is apparently confirmed by the above statement that, "Given the delay between the thwarting of the incident and the identification there would be little value starting an official NCPD investigation into the matter."

To be clear, OIG did not impose requirements; it only made recommendations, which the Comptroller's Office is free to accept in whole or in part, or disregard, as it chooses.

To recap, we observed that the Comptroller's Office, when faced with three roughly similar attempts to fraudulently divert County payments during 2019-2020, timely notified NCPD in two of the three instances. OIG has modified the draft wording of its conclusions to more closely reflect that it is specifically referring to the reporting of Vendor Imposter Fraud attempts.

The universe of such instances known to OIG is 3, not 1,100 or 57,000. OIG did not recommend or imply that all phishing attempts blocked by DIT be reported to law enforcement. Our reference to attempted crimes was intended to help convey that attempts to defraud the County, although unsuccessful, should also be of concern. In consideration of the Comptroller's Office comments, OIG has modified the draft wording of its notification recommendation to "... when it has reason to believe that a vendor impostor scheme or other fraud pertaining to County funds has been committed or attempted, subject to a mutually agreed reporting protocol ..."

OIG does not understand the reference, or pertinence to our conclusions and recommendation, of the Comptroller's Office self-description as an "investigative body." In any event, our recommendation was driven by what we found, not by any extraneous considerations, such as the law enforcement notification provision applicable to OIG. OIG does not understand the purpose of referencing that extraneous provision, nor the purpose of the Comptroller's Office then posing a question about the operations of the OIG.

WITH RESPECT TO:

- OIG Conclusion: "CO Lacks Comprehensive Fraud Risk Assessment"

COMPTROLLER'S OFFICE COMMENTS:

•The Comptroller's Office will conduct a comprehensive fraud risk assessment. The Comptroller's Office has retained a consultant to conduct an internal control and risk assessment of all our procedures across all Divisions, which includes a gap analysis and recommendation for mitigation including the areas of vendor registration fraud and cybersecurity. Our Office will review recommendations for any procedural changes to mitigate any identified gap in the risks analysis, including the development within our Office of a Security Awareness Program.

•This review being undertaken by the Comptroller's Office comprehensively includes all Divisions, going beyond the scope of the incident subject to the OIG report. As such, our Office is in the process of undertaking a deep-dive review of our processes and controls using an internal control assessment which is a first and necessary step toward a comprehensive fraud risk assessment.

Respectfully Submitted,

[SIGNATURE]

Jeffrey R. Schoen
Deputy Comptroller/Chief Counsel

CC: Hon. Jack Schnirman, Nassau County Comptroller

APPENDIX B

Comptroller's Office Response, as Submitted

Hon. Jack Schnirman
Nassau County Comptroller



OFFICE OF THE NASSAU COUNTY COMPTROLLER

240 Old Country Road
Mineola, New York 11501
Tel: (516) 571-2386 Fax: (516) 571-5900
nccomptroller@nassaucountyny.gov

November 5, 2020

Jodi Franzese, Inspector General
Nassau County Office of the Inspector General
One West Street,
Mineola, NY 11501

Dear Inspector General Franzese:

In accordance with §191 of the Nassau County Charter, the Office of the Nassau County Comptroller herein submits its comments with respect to your draft "Review of 2019 Vendor Imposter Fraud Incident."

Reform and Collaboration

Since the appointment of the Inspector General (IG) in December of 2018, the Office of the Nassau County Comptroller (Comptroller's Office or Office) has worked collaboratively with the Office of the Inspector General (OIG) to reform the County. Many of these collaborative reforms have been to Nassau County's (County) contracting and procurement processes, which is of "particular" concern to the OIG; "[t]here is hereby established an independent office of the Inspector General which is created in order to provide increased accountability and oversight of County operations, to detect and prevent waste, fraud, abuse and illegal acts in programs administered or financed by the County, *particularly the County's contracting and procurement processes*, to promote transparency, efficiency and integrity in the County contracting and procurement process" [Nassau County Charter, Article 1-C §185, emphasis added]. Together this Office and the OIG have contributed and continues to contribute to reforming the County Procurement Policy, procurement procedures, solicitation tracking, the disclosure process, and a variety of other issues that make our County government more transparent and accountable.

Indeed, the necessity for collaboration between the OIG and the Office of the Comptroller is recognized by the County Charter, which requires that all reports, such as the one this Office is commenting on herein, "shall be furnished to the County Executive, *and the County Comptroller* as well as the Presiding Officer and the Minority Leader of the County Legislature" [Nassau County Charter, Article 1-C §192(1), emphasis added]. It is of no surprise then that the exchanges between the OIG and this Office during the review process here served both to improve upon the reforms this Office has already implemented since 2018 and to develop the OIG's understanding of many of the County's processes, which in turn will assist the OIG in its overall reform goals.

OFFICE OF THE COMPTROLLER

240 Old Country Road • Mineola, New York 11501

Tel: (516) 571-2386 • Fax: (516) 571-5900 • nccomptroller@nassaucountyny.gov

The establishment of the IG's Office was a major reform for Nassau County. In the Nassau County District Attorney's July 2015 "Special Report on the Nassau County Contracting Process" it was specifically recommended that "[t]he Legislature should modify the County Charter to eliminate the position of Commissioner of Investigations due to its history of ineffectiveness, and replace it with an independent and adequately staffed County Inspector General, appointed by the County Executive and confirmed by a supermajority of the County Legislature" [Section V(8)].

It is with this reform objective in mind and in furtherance of collaboration and good government, that this Office has welcomed the IG's review of its procedures and controls regarding vendor payment information processing (vendor registration) and the reported fraud incident of late 2019.

Purpose

Presumably in furtherance of independence, the OIG is empowered to initiate audits, investigations, inspections, examinations and reviews on its own initiative. The OIG is supervised by the County Legislature- "The County Legislature shall create a legislative committee within the County Legislature for the purpose of maintaining general supervision of and liaison with the Office of the Inspector General" [Nassau County Charter, Article 1-C §189(2)] - and its activities are bi-annually reviewed by Nassau County Legislature - "The Inspector General shall meet with representatives of the Majority and Minority delegation of the Nassau County Legislature every six months to review the previous six month's activities and the Inspector General's plans and objectives for the upcoming six months" [Nassau County Charter, Article 1-C §192(2)]. It is clear from their report, and from communications with the OIG throughout this review, that the IG initiated this review in response to a letter from the Deputy Presiding Office of the Nassau County Legislature and that the IG would not have independently initiated this review but for the insistence of the Legislature.

Transparency

The Nassau County Comptroller is committed to transparency and reform. One cannot be achieved without the other. At the time the events subject to this review took place in late 2019, municipalities throughout the Country were increasingly under attack by newly developing threats using technology, including phishing and ransomware incidents. As such in the interest of transparency, to assist other municipalities in dealing with these developing threats, this Office along with the Nassau County Police Department, made this matter public. This action was frankly, antithetical to a County government that has shown historically to be susceptible to cover-ups and corruption. As a result of these actions, those in County government and a number of municipalities had been forewarned to implement measures (as did our Office) to combat such fraud, the public at large was further educate about the nature of such frauds and the IG was asked by the Legislature to conduct this welcomed review. In February of 2020, Suffolk County initiated a cybersecurity project. All of these are positive actions which foster collaboration, cooperation, good government and reform.

Note as to the OIG Recommendations:

As noted above, the OIG is required to publish its reports to, amongst others, the County Comptroller. To date our Office has not received any other OIG reports of any reviews of any other office, entity or department. Based upon seeing no previous such reports and based upon representation made by the OIG during the course of their review process, all indications are that this is the first such “review” conducted by the first ever County IG. Our Office has been cooperative with this review and indeed, as the first Office subject to such a review has been cooperatively discussing best practices for conduct of such reviews as both the IG, her staff and our Office have much experience in conducting reviews, investigations and audits.

As also noted above, it is clear the OIG would not have independently initiated this review. Given the cooperative roles that the OIG and the Comptroller’s Office play, it seems to be a poor use of OIG resources to make such formal recommendations. It is clear that the OIG could easily have cooperatively and collaboratively reviewed and informed our Office of any control gaps they identified in their review and of any actions they concluded we should take to improve our such controls. The IG is empowered to determine if it is or is not appropriate to publish and deliver a report or recommendation [Nassau County Charter, Article 1-C §191] and in the alternative to “recommend remedial actions and may provide prevention and training services to County officers, officials, employees, and any other persons covered by this Article...[t]he Inspector General may follow up to determine whether recommended remedial actions have been taken” [Nassau County Charter, Article 1-C §187(12)].

Points of Clarification

- The Office of the Comptroller AUDITS AND APPROVES claims for payment.
- The County Treasurer signs the checks.
- Vendors may choose to permit payments to be made by check.
- Vendors may choose to permit payments made by electronic payment (Automatic Clearing House or ACH).
- The Office of the Comptroller maintains the various vendor payment information in the County financial system for each vendor, such as:
 - where to send a check if a claim is being paid by check
 - bank account(s) information if payment is being made by electronic payment.
- If the vendor has multiple payment methods in the financial system, they will select which method of payment should be used for each claim when the claim is submitted for review.

► **COMMENTS ON THE OIG RECOMMENDATIONS**

Note: the report recommendations are not numbered as such our responses cannot be correlated by number.

• **OIG RECOMMENDATION**

Further Strengthen Controls Through Periodic, Comprehensive Fraud Risk Assessments

COMPTROLLER'S OFFICE COMMENTS:

This is being done: Our Office is in the midst of this process. The Comptroller's Office has retained a consultant to conduct an internal control and risk assessment which includes a gap analysis and recommendation for mitigation including the areas of vendor registration fraud and cybersecurity. Our Office will review recommendations for any procedural changes to mitigate any identified gap in the risk analysis, including the development within our Office of a Security Awareness Program, or even working with the County Information Technology Department (IT) to implement this Countywide. We have been advised that this is a first and necessary step in conducting any such assessment. See below for details.

• **OIG RECOMMENDATION:** Provide Fraud Awareness Training for VCD staff on a recurrent basis

COMPTROLLER'S OFFICE COMMENTS:

This has been done and is being done on an on-going basis: The Comptroller's Office staff had received training prior to, and post the incident, and continues to receive such training. Our Office will work to develop within our Office a Security Awareness Program. See below for details.

• **OIG RECOMMENDATION:** Train Accounting Division Staff on Significance of ACH Return Reason Codes

COMPTROLLER'S OFFICE COMMENTS:

This has been completed: The Comptroller's Office staff has received such training. The staff acted in accordance with all recommended guidance, including the OIG / National Automated Clearing House Association (NACHA) guidance for rejections noted in the OIG review report. The staff took the necessary actions required by the constraints of the County financial system, which resulted in recovery of all diverted funds. All ACH rejections are being escalated to the Division Head and the Deputy Comptroller level for review. See below for details.

•**OIG RECOMMENDATION:** Expedite Issuance of Pending Written Procedures for Vendor Information Change Processing

COMPTROLLER'S OFFICE COMMENTS:

This is being done: The Comptroller's Office has obtained a consultant to conduct control review, risk assessment and gap analysis of all our procedures, including the vendor registration process. Final publication will be completed once our Office has been able to incorporate any procedural changes effectuated as a result of this review into these procedures. See below for details.

•**OIG RECOMMENDATION:** Ensure Consistent Reporting of All Fraud Attempts

COMPTROLLER'S OFFICE COMMENTS:

Competed: The Comptroller's Office has consistently reported all known incidents of fraud since the incident under review that was the subject of the OIG report. See below for details.

► **COMMENTS ON EXECUTIVE SUMMARY, FINDING AND CONCLUSIONS**

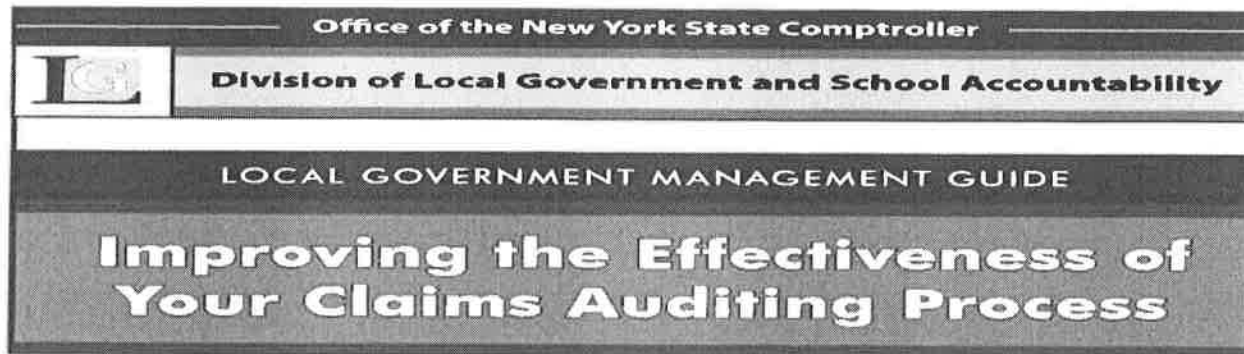
Note: the report findings and conclusions are not numbered, as such our responses cannot be correlated by number.

WITH RESPECT TO:

- OIG Executive Summary: “OIG further determined that the internal controls the CO had in place at the time for the vendor information change process were not effective in preventing the fraud scheme and that its staff was not trained to detect such fraud.”
- OIG Conclusion: “CO’s Then-Existing Controls Were Ineffective in Preventing the Subject Fraud: Were Not Consistent with Recommended Mitigations Strategies.”
- OIG Conclusion: “Pre-Incident Controls Thwarted but Did Not at the Time Detect Another Fraud Attempt.”

COMPTROLLER’S OFFICE COMMENTS:

- The Comptroller’s Office has been improving controls over the vendor registration process based upon Governmental Finance Officers Association (GFOA) and other guidance since January of 2018, immediately upon the new Comptroller taking Office. These additional controls included:
 - (1) requiring verification of bank account number in the form of either a voided check or a bank account confirmation letter;
 - (2) requiring dual verification within the Claims Division of changes made to a vendor’s profile in the financial system;
 - (3) requiring a verification of Vendor Tax Identification Numbers (TINs) prior to making entry into NIFS – utilizing the IRS’ free application;
 - (4) and deactivating the ability of a vendor to receive a payment if this verification fails.
- These new controls were implemented prior to the incident subject to the OIG review and had thwarted a similar incident – which the OIG has acknowledged.
- The Comptroller’s Office provided the OIG with materials demonstrating that the Vendor Claim Division *was* trained on electronic vendor fraud prior the incident, including:



Red Flags

Claims with certain characteristics may have a higher risk of error or fraud. Officials should use common sense and reasonable skepticism when any claim appears to be out of the ordinary. Even when all required documentation is submitted, remain skeptical, especially of claims that are not routine. In today's electronic environment, anyone with a computer and printer may be capable of replicating and manipulating information to produce false documentation. Particular attention should be paid to claims with the following characteristics:

- Missing documents
- Unavailability of original documents
- Recurring identical amounts from the same vendor
- Multiple remittance addresses for the same vendor
- Inconsistent, vague, or implausible responses arising from inquiries or analytical procedures
- Excessive voids or credits
- New vendors, especially if payment goes to a post office (PO) box
- Items purchased that are not clearly identified
- Goods delivered outside of a central location or to an unusual delivery point
- Credit card charges with no original receipts attached
- Travel and conference claims
- Alterations or questionable handwriting on documents
- Duplications
- Payments to a vendor that have increased dramatically for no apparent reason
- Payments to vendors for construction work not certified as completed by your architect or engineer
- Unusual delays in providing requested information
- Tips or complaints about possible fraud.

•In concluding that our Office's controls were not consistent with then recommended mitigation strategies, the OIG relies upon a GFOA citation to <https://www.gfoa.org/materials/electronic-vendor-fraud> presumably found by the OIG in doing open source research on the issue.

•**This guidance, it seems, was published on the GFOA website on December 2, 2019, after the incident** and after our Office has implemented these best practices safeguard and internal controls which have since been used effectively to mitigate the risk of fraud.

•The late 2019 fraud incident took place at a time when technology related schemes began affecting municipalities throughout the Country.

•As a response to the proliferation of such schemes, those responsible for providing guidance on governance and controls, both for-profit entities and professional advisory organizations, such as accounting firms and the GFOA began to actively focus their publication, webinars, emails, newsletters and other literature on such schemes, including electronic vendor fraud, such as these from *January 2020* and *February 2020*:

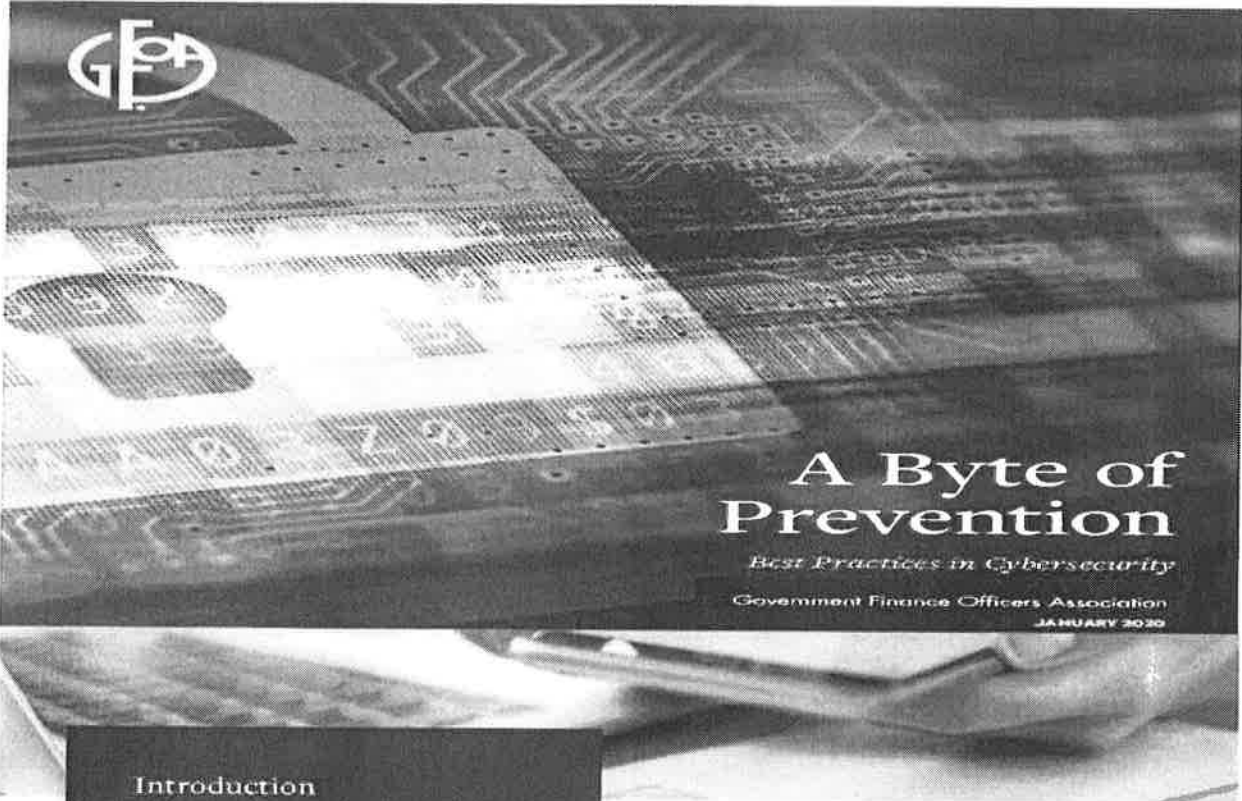
Essential Tools for Effective Payables Policies and Procedures in the Treasury Office



 GOVERNMENT FINANCE OFFICERS ASSOCIATION

Webinar
February 20, 2020
1-3PM CT

1



Introduction

All local governments are potential targets for cybercrime, a risk that intensifies as victims increasingly pay ransoms to regain access to their hijacked technologies. It can be tempting to pay up because hacks are disruptive, damaging, and embarrassing – and expensive. As stewards of (often sensitive) public data, finance officers must understand the significance of this threat, including the large costs governments face in recovering lost data, restoring public trust, and otherwise recovering from a breach.

Finance officers can implement simple and inexpensive strategies that address people, process, and technology to protect their organizations from cyber threats without conducting a costly cybersecurity assessment. Many of the recommendations on the following pages address the weakest link in cybersecurity: the human factor.

1 | Employee Awareness

Most breaches begin with an e-mail or file attachment. Employees in the finance department are likely targets because they have frequent transactions with vendors and access to business systems. To mitigate this threat, governments should train employees to:

- Be suspicious.
- Be wary of e-mails asking them to change their usernames or passwords.
- Double-check the sender's e-mail address before opening or downloading an attachment.
- Follow the government's compliance business processes when vendors request changes to electronic payment and bank account information (e.g., accounts payable) and staff members (e.g., direct deposit). These procedures are often "out-of-band" (i.e., not done by e-mail) and are therefore likely to expose wrongful requests.
- Check the vendor's website address before entering or sending sensitive data.
- Periodically check the public website haveibeenpwned.com to see if their e-mail addresses and passwords have been exposed. If so, employees should report the breach and change passwords for the accounts listed.

Continued on page 3

WITH RESPECT TO:

- OIG Executive Summary: “The bank notified the CO of the account freeze on October 22, 2019. Two day later, the CO learned, as a result of the communications from the true vendor, that the deposits had been fraudulently diverted, and the CO accordingly notified the Nassau County Police Department (NCPD).”

- OIG Finding: “Accounting Division Specialist Requested that the Actual Vendor Submit a New Form 700.”

- OIG Finding: “The CO’s practice in the event of an ACH return was to confirm the payee’s correct address and to manually generate a paper check to replace the rejected electronic payment. On October 23, 2019, the Specialist followed this practice by emailing a blank form 700 to two employees in the Financial Services Unit of DPW.”

- OIG Conclusion: “[T]he Specialist followed the usual practice in responding to the subject ACH return, despite the atypical reason code and unusually high amount of he returned funds. Specifically, on October 23, 2019, she asked the user department (DPW) to contact their vendor and have them complete a new Form 700. She did not escalate the matter of the ACH return (citation omitted).”

- OIG Conclusion “The Vendor Detected the Fraud.”

- OIG Conclusion: “Accounting Division Staffer Was Not Trained in Significance of ACH Return Code: Red Flag Missed.”

COMPTROLLER’S OFFICE COMMENTS:

- The OIG infers that the Accounting Systems Specialist who handled the ACH rejections was oblivious to the notion that anything unusual was happening. This notion simply lacks the appreciation for the action taken by Accounting Systems Specialist to uncover the additional diverted funds, lacks the understanding of the reasons those actions were taken (in complete disregard of the very guidance they cite), and appears to lack the appreciation of the basis for the actions taken being due to the limitations of the County financial system.

- The Accounting Systems Specialist initiated the protocol to obtain and verify an alternative form of payment. The Accounting Systems Specialist acted in accordance with all recommended guidance (including the OIG/ National Automated Clearing House Association (NACHA) guidance for rejections noted in the OIG review report), and took the necessary action required by the constraints of the County financial system, which resulted in recovery of all diverted funds.

•The OIG’s own citation concerning the R-16 rejection code (see below), used to reach their conclusions, recommends that the action to take is to **obtain a different form of payment**. The citation indicates that there are *common reasons* that this rejection code is used, and it *may, on a more exceptional basis* indicate that there is suspicious activity (see below).

OIG Citation: [https://paysimple.com/help/Zions/ps30/a2-ach-return-codes/Directory of ACH Return Codes.htm](https://paysimple.com/help/Zions/ps30/a2-ach-return-codes/Directory%20of%20ACH%20Return%20Codes.htm)

R16 Account Frozen

NACHA Definition:	1) Access to the account is restricted due to specific action taken by the RDFI or by legal action; or 2) OFAC has instructed the RDFI or Gateway to return the Entry.
What it Means:	The payment cannot be honored because the account has been frozen and no transactions can be processed against it.
What to Do:	<p>Contact your customer to obtain a different form of payment. You will not be able to process transactions using this bank account until it is un-frozen.</p> <p>There are several common reasons why a bank account may be frozen, such as a civil legal dispute over an unpaid debt. However, you may also see this code if OFAC has frozen the account or the individual payment due to suspicion of terrorism-related activity. (OFAC stands for the Office of Foreign Assets Control, which is an agency of the United States Department of the Treasury under the auspices of the Under Secretary of the Treasury for Terrorism and Financial Intelligence.)</p> <p>This return code should be a red-flag for your business. If you see this code, be certain to do your due diligence around verifying the identity of your customer.</p>

•The Accounting Systems Specialist was following protocol in place by our Office and these protocols are the exact protocols indicated by the OIG that should have been followed according to their citation.

•Furthermore, because the current financial system is limited and will not permit another ACH transaction for the same claim, the *County’s* procedure, is to initiate a paper check transaction to be mailed to the vendor to replace the rejected ACH payment. To effectuate this transaction, the County procedure is to verify the address to send such a paper check via the submission of a W9/700 Form, so that proper protocols and controls are followed verify the information before the check is sent to. The OIG demonstrated their lack of appreciation for this limitation as they only noted this in a footnote in their report.

OFFICE OF THE COMPTROLLER

240 Old Country Road • Mineola, New York 11501

Tel: (516) 571-2386 • Fax: (516) 571-5900 • nccomptroller@nassaucountyny.gov

- In following the protocols and initiating this control, the Accounting Systems Specialist set in motion a series of events and correspondences between our Office, DPW and the Vendor which, in short order, revealed the additional diverted funds. By taking these actions, and initiating these series of email exchanges, the additional diversions were detected and all money was recovered.
- A closer look at the chain of events through these emails, indicates 24 hours and 46 minutes between our Office alerting DPW of the rejection (as per correct protocol noted above) and the Deputy Comptroller and then the Nassau County Police Department (NCPD) being notified of the confirmed fraud and diversion of the additional funds.
- During this *one* day period in which there was constant communication between the Vendor, DPW and our Office, the Vendor was put on notice, worked with the County, DPW, our Office, and other County Offices to identify the additional diversions.
- Even accounting for the time between when the Accounting System Specialist received the initial email from the bank, late in the day on October 22, 2019, to the time the Accounting System Specialist initiated the protocol by sending an email to DPW, the next morning, the time frame between the email notification and the report to the Deputy Comptroller and the NCPD is less than 48 hours.
- The OIG report agrees factually with all of the timelines concerning these email exchanges which were necessary to uncover the additionally diverted funds – although the OIG report spuriously notes only the dates of these exchanges and not the timing of these exchanges, which actually occurred over a *one* day period.

WITH RESPECT TO:

- OIG Finding: “CO Conducted a Look Back Review; Confirmed the Validity of Some Vendor Change Request.”
- OIG Finding: “After the fraud came to light, the CO in 2019 performed a review (look back) of some of the Form 700 processed during the period of January through September 2019.”
- OIG Conclusion: “The CO’s Look Back Verification was Partial, Extent is Unclear.”
- OIG Conclusion: “The CO conducted a look back review and verified Form 700 changes made to some of the County’s vendors.”

COMPTROLLER'S OFFICE COMMENTS:

- Simply put, the Comptroller's Office reviewed all W9/700 Forms submitted between January 2019 and the incident.
- This review implemented the recommended best practices in identifying red flags concerning electronic vendor fraud.
- None of the vendor requests and the information submitted during this period had any such red flags and there were no instances found of any entity, other than the actual vendor, having submitted the W9/700 Form.
- In addition, to the above review, which had negative results for red flags, the Office additionally verified selected vendors with frequent high dollar payments, vendors with multiply suffixes in the financial system (multiple payment methods) and/or vendors who were adding or changing banking information during the period (as opposed to a change of address or other information).
- This process overlapped with the implementation of a three month look back period for payment approvals, requiring that any vendor payment going to a vendor who has not received a payment in the last three months, before such a payment can be approved, the vendor must be contacted to verify their payment information. The OIG was informed that as of the date of their inquiry on this matter (July 2020) the information was verified in this manner of 534 vendors, 42 of which required changes to their information which were effectuated using all of our updated procedures.

WITH RESPECT TO:

- OIG Conclusion: "CO's Reporting of Fraud Attempts Has Been Inconsistent."
- OIG Conclusion: "OIG notes that even attempts to commit crimes are of concern and may constitute criminal conduct in violation of the Penal Law."
- OIG Conclusion: "OIG concludes that the Comptroller has not consistently ensured that proper authorities were promptly notified when the CO has reason to believe that a fraud pertaining to County funds may have been committed or attempted."

COMPTROLLER'S OFFICE COMMENTS:

- The Comptroller's Office has worked with and continues to work with our partners in law enforcement to report instances of fraud or other possible illicit activities concerning the County. The Office regularly transmits such findings to law enforcement, including the Nassau County District Attorney's Office and the Office of the New York State Attorney General. The Comptroller's Office is an investigative body which has and will continue to consistently convey confirmed instances of fraud and illicit activity to law enforcement.

OFFICE OF THE COMPTROLLER

240 Old Country Road • Mineola, New York 11501

Tel: (516) 571-2386 • Fax: (516) 571-5900 • nccomptroller@nassaucountyny.gov

•There were two attempts in September of 2019. One early in September of 2019 resulted in the matter which is the subject of the OIG review and other later in September of 2019. As noted by the OIG, the Comptroller's Office controls in place at the time thwarted the late September 2019 incident; it was revealed that the request of the fraudster was not processed because the fraudster never follow-up in submitting a cancelled check. The additional controls put in place by this Office after September of 2019 then detected the earlier attempt by the fraudulent vendor when the actual vendor sought to update their vendor information. As such, the controls put in place by this Office did both thwart and detect this incident.

•As noted above, the Comptroller's Office has continually improved, and will continue to, improve, controls based upon GFOA and best practice guidance. As these best practices changed, and in response to the incident subject to the OIG review, we developed our controls. As such there was a lag in time, which clearly would not happen with the new controls in place, between the thwarting of the later September 2019 incident and the detection of the incident. Given the delay between the thwarting of the incident and the identification there would be little value starting an official NCPD investigation into the matter. Nevertheless, the NCPD was aware of the incident. It is not clear from the OIG if in reaching their conclusion the OIG confirmed with the NCPD if the NCPD had a record this incident.

•The OIG writes that "even attempts to commit crimes are of concern and may constitute criminal conduct in violation of the Penal Law." It is noted that during the January 22, 2020 Finance Committee hearing on this matter, the IT Department reported that "last week we actively blocked 1,100 phishing attempts into the county." Is the IG requiring a report be made for each and every phishing attempt? 1,100 per week equates to over 57,000 attempts per year. Has the OIG discussed their requirement with the NCPD? Perhaps the OIG is imposing such a requirement because the Nassau County Charter, Section 187(5) requires that "[w]here the Inspector General suspects a possible criminal violation of any state, federal, or local law, he or she *shall forthwith notify the appropriate law enforcement agencies* [emphasis added]. Has the OIG, given their broad investigatory authority and authority to "receive, review, and investigate any complaints regarding any County-funded projects, programs, contracts, purchase orders, agreements or transactions, and all other activities, or operations of the County Executive and County agencies" [Nassau County Charter, Section 187(5)], "suspected" and reported numerous criminal violations?

WITH RESPECT TO:

•OIG Conclusion: “CO Lacks Comprehensive Fraud Risk Assessment”

COMPTROLLER’S OFFICE COMMENTS:

•The Comptroller’s Office will conduct a comprehensive fraud risk assessment. The Comptroller’s Office has retained a consultant to conduct an internal control and risk assessment of all our procedures across all Divisions, which includes a gap analysis and recommendation for mitigation including the areas of vendor registration fraud and cybersecurity. Our Office will review recommendations for any procedural changes to mitigate any identified gap in the risks analysis, including the development within our Office of a Security Awareness Program.

•This review being undertaken by the Comptroller’s Office comprehensively includes all Divisions, going beyond the scope of the incident subject to the OIG report. As such, our Office is in the process of undertaking a deep-dive review of our processes and controls using an internal control assessment which is a first and necessary step toward a comprehensive fraud risk assessment.

Respectfully Submitted,



Jeffrey R. Schoen
Deputy Comptroller/Chief Counsel

CC: Hon. Jack Schnirman, Nassau County Comptroller