

OFFICE OF INSPECTOR GENERAL

St. Johns County

Clerk of the Circuit Court and County Comptroller



REPORT OF INVESTIGATION #2024-0002

FAILURE TO FOLLOW STANDARD OPERATING PROCEDURES

Elizabeth Gonzalez
Interim Inspector General

February 7, 2025

Date Issued

EXECUTIVE SUMMARY

On September 28, 2023, St. Johns County Clerk of Courts and County Comptroller Brandon Patty (Clerk) reported to the St. Johns County Clerk of the Circuit Court and County Comptroller (COCC) Office of Inspector General (OIG) that a COCC Treasury Clerk may have failed to follow procedures for processing an Electronic Funds Transfer (EFT) setup request that was submitted by an individual impersonating a SJC vendor, resulting in two payments being issued to a scammer. The Clerk requested the OIG investigate whether the Treasury Clerk failed to follow the EFT setup Standard Operating Procedure; specifically, it was questioned whether the Treasury Clerk placed a telephone call to the vendor for verbal confirmation, as required. The OIG subsequently initiated an investigation.

The OIG's investigation was performed according to the Principles and Standards for Offices of Inspector General and The Florida Inspectors General Standards Manual from The Commission for Florida Law Enforcement Accreditation.

The investigation confirmed that the Treasury Clerk did not contact the vendor for verbal verification, as required by the SOP. The Treasury Clerk testified that she did not recall seeing the SOP; however, she articulated a clear understanding of various requirements outlined in the SOP that she did not adhere to and further testified that even if she had seen the SOP, she did not refer to it in performing EFT setups.

The OIG **substantiated** the allegation that the COCC Treasury Clerk failed to follow Standard Operating Procedures for processing an electronic funds transfer setup request, which resulted in payments totaling **\$1,163,795.28** to a scammer.¹

Additionally, the OIG identified internal control factors that contributed to this system failure. The OIG identified areas for improvement that should be addressed to assist in mitigating the risk of this type of incident from reoccurring. The recommendations are included at the end of this report.

In response to this incident, the Clerk reassigned the Treasury Clerk and engaged with a third-party vendor to perform the EFT setup process that had been previously assigned to the Treasury Clerk.² The Clerk's response to the investigation's findings is attached to this report.³

¹ As of January 9, 2025, of the \$1,163,795.28, the COCC recovered \$662,911.35.

² According to the vendor quote, the cost for this service was \$219,985.50 for setup and three years of licensing fees.

³ Exhibit 1

BACKGROUND

Florida offices of the Clerk and Comptroller perform a wide range of record keeping, information management, and financial administration services for Florida's judicial system and county government. In addition to serving as the Clerk of the Circuit Court, most Clerks also serve as the County Treasurer, Recorder, Auditor, Finance Officer, and Ex-Officio Clerk to the County Commission.⁴

Florida's Clerks of Court and Comptrollers have nearly 1,000 statutory responsibilities and provide critical public services to their communities. Most Clerks of Court also serve as the Comptroller within their county, acting as the Chief Financial Officer, accountant, and custodian of county funds; in St. Johns County, the Clerk serves as both.

Comptrollers play a crucial role in local government by promoting accountability, transparency and efficiency by maintaining fiscal order of the county, ensuring proper use of public funds, protecting the county's funds, and promoting transparency.⁵

In Fiscal Years 2023 and 2024, the St. Johns County Clerk of Courts and Comptroller oversaw the Board of County Commissioner's adopted budgets of \$1,550,104,053⁶ and \$1,665,664,624.⁷

The St. Johns County Clerk of the Circuit Court and County Comptroller (COCC) Finance Department is led by the Chief Financial Officer (CFO). The Finance Department is responsible for the COCC budget and St. Johns County (SJC or County) Comptroller functions (BOCC Finance).

The COCC Treasury Clerk (Treasury Clerk) in question has been employed with the COCC since September of 2000, and currently reports to the Board of County Commissioners (BOCC) Accounting Deputy Director; however, during the time of the incident in question, she reported to the BOCC Accounting Director (Director), who reports directly to the CFO. Throughout her tenure with the COCC, the Treasury Clerk has held positions such as Cash Receipt Specialist, Banking Services Specialist, and Banking Services Accountant.

According to the job specifications, the Treasury Clerk is responsible for performing accounting duties in support of the department's banking services functions. These duties include setting up Electronic Funds Transfers (EFTs) for vendors, maintaining the Accounts Payable Vendors Electronic File Transfer database, and scanning documents into PaperVision (a document management system).

The EFT Setup Standard Operating Procedure (SOP) was established on October 20, 2021, and authored by the Accounts Payable Supervisor, who was assigned the EFT responsibilities at that time. The creation date of the SOP is significant as it was authored in response to a similar fraud attempt incident that occurred in August of 2020. The SOP provided required steps that were implemented in attempt to mitigate the risk of fraudulent activities associated with the EFT setup

⁴ This information was obtained from the Florida Courts and Comptrollers web page.

⁵ This information was obtained from the Florida Courts and Comptrollers web page.

⁶ BCC Resolution No. 2022-358

⁷ BCC Resolution No. 2023-365

process. Once completed, the SOP was uploaded to the Finance Department's local computer network drive.

ALLEGATION AND FINDING

*St. Johns County Clerk of the Circuit Court and County Comptroller Treasury Clerk failed to follow Standard Operating Procedures for processing an Electronic Funds Transfer setup request, which resulted in payments to a scammer. Finding: **Substantiated***

Governing Directives

EFT Setup, Standard Operating Procedure, BOCC Finance states in pertinent part:

Step # 1: *The person designated to set up [sic] EFTs in the office is the only one to send out setup forms directly to the vendor trying to set up [sic]. The form is not to be sent to another department for them to send out. This minimizes variations of the form out there and we like to maintain that control in our office...*

Step # 3: *The company info needs to be compared to our system for the same EIN and address information. (Fund Accounting/Reference Tables/Vendor List) Then Google the company to match the address and phone information to the forms presented. Make a printout of the information found to attach to the packet.*

Step # 4: *Once all information has been received and the vendor information has been confirmed, the company will need to be contacted to make final verbal verification that they would like to set up [sic] to receive EFT payments from us and confirm the bank where funds will be sent.*

3.4. Employee Conduct and Work Rule, St. Johns County Clerk of the Circuit Court and Comptroller Employee Handbook states in pertinent part:

The Clerk & Comptroller's office requires that you are familiar with and comply with all rules and regulations in carrying out your assigned duties.

CASE INITIATION

On September 28, 2023, St. Johns County Clerk of Courts and County Comptroller Brandon Patty (Clerk) requested the OIG investigate whether a COCC Treasury Clerk failed to follow procedures for processing an EFT setup request, which was received from an individual impersonating a SJC vendor.⁸ Specifically, it was questioned as to whether the Treasury Clerk placed a telephone call to the vendor for verbal confirmation, as required by the EFT Setup SOP.

It was reported that on July 31, 2023, the EFT setup request was processed by the Treasury Clerk, submitted to the BOCC Accounting Director for review, and approved by the Director on August 2, 2023. Subsequently, the vendor's payment information was updated. On August 28, 2023, an EFT payment was issued against a legitimate invoice to a scammer in the amount of \$551,363.39; on September 26, 2023, a second payment was issued against another legitimate invoice in the amount of \$612,431.89.

⁸ The request originated from an e-mail address identical to a legitimate vendor contact e-mail address except for the domain extension as ".co" versus ".com."

On September 27, 2023, the Comptroller's office became aware that the vendor had not received payment for the invoices in question. On the same day, the sending and receiving banks were contacted and the incident was reported to the St. Johns County Sheriff's Office (SJSO) who conducted a criminal investigation.⁹ The OIG opened an investigation based on the information the Clerk provided.

RECORDS REVIEWED

The OIG reviewed the EFT Setup SOP¹⁰ and all documents associated with this EFT Setup, to include: the Electronic Fund Transfer Form and Agreement;¹¹ the W-9 Request for Taxpayer Identification Number;¹² e-mails from the fraudulent person to the Utilities Manager requesting the EFT setup;¹³ the EFT Setup Checklist;¹⁴ and the voided check.¹⁵ The review and analysis of records concluded the records were consistent with and corroborated the testimony provided throughout the investigation.

WITNESS TESTIMONY

The OIG interviewed the following witnesses under oath: Chief Financial Officer (CFO); BOCC Accounting Director (Director), Accounts Payable Supervisor (AP Supervisor); and SJC Utilities Department Manager (Utilities Manager).

Throughout the course of the investigation, all accounts of what transpired leading to the fraud event were consistent, and revealed the following facts:

On July 27, 2023, an individual impersonating a County vendor e-mailed a SJC Utilities Department Project Manager (Project Manager) requesting a change to their banking information. The Project Manager replied to the scammer that vendor payments were beyond his scope and responsibility, copying the Utilities Manager on the e-mail. On July 31, 2023, the Utilities Manager sent the EFT Agreement form to the fraudulent e-mail address and once the form was completed, the scammer e-mailed the form directly to the Treasury Clerk.

On July 31, 2023, the Treasury Clerk hand-delivered the completed EFT Agreement form and the EFT setup checklist (an internal document utilized to document the completion and supervisory review of necessary steps for EFT setups) to the Director for review. The Director reviewed the EFT setup checklist and initially rejected it because the vendor's name on the EFT Agreement form did not match the vendor's name according to the Internal Revenue Service (IRS) verification website; the name must match exactly. After resolving that issue, the checklist was ultimately approved by the Director on August 2, 2023. Subsequently, the vendor's payment information was updated in the vendor management system.

On August 28, 2023, a payment of \$551,363.39 was issued for an invoice due to the vendor; however, because the account information had been changed to the scammer's account, the

⁹ The SJSO criminal investigation has been closed without identifying any perpetrator, however, the investigation assisted in recovering a portion of the lost funds.

¹⁰ Exhibit # 2

¹¹ Exhibit # 3

¹² Exhibit # 4

¹³ Exhibit # 5

¹⁴ Exhibit # 6

¹⁵ Exhibit # 7

vendor did not receive the payment. On September 26, 2023, a second payment of \$612,431.89 was issued to the scammer's account for an additional invoice that was due to the vendor.

The fraudulent payment went unnoticed until September 27, 2023, when the Utilities Department contacted BOCC Finance to notify them that the vendor indicated they had not yet been paid, and that they had not initiated a change to their payment method information. At that point, the receiving and sending banks were notified, which halted the second payment. The first payment was reported to the St. Johns County Sheriff's Office (SJSO) for investigation.

Testimony regarding BOCC Finance Policies and Procedures:

Generally, BOCC Finance SOPs are drafted by the employee responsible for performing the function to which the SOP applies. SOPs are not required to be reviewed or approved through the supervisory chain, and there is no formal implementation process. SOPs are available to employees in a folder located in an internal computer network drive; however, employees are not required to acknowledge receipt or understanding of SOPs. In the event there is a change to an SOP, Finance employees are typically notified via e-mail.

The AP Supervisor recalled that she sent an electronic copy of the EFT SOP via e-mail to the Treasury Clerk, when the EFT duties transitioned from the AP Supervisor to the Treasury Clerk (a copy of this e-mail was provided to the OIG and confirmed the SOP was sent on October 20, 2021).

Apart from the AP Supervisor, the author of the SOP, and the CFO, the remaining individuals interviewed stated that they had never seen the SOP and had no prior knowledge of its existence. According to the Director, she had not seen the EFT Setup SOP until September 28, 2023, the day after they discovered the fraud incident. When she saw the SOP, she recalled being "upset" because had she known it existed, she would have adhered to the procedures.

After reviewing the SOP, the Director learned that the current process outlined in the SOP was not being followed; for example, the policy required that the individual assigned to complete the EFT setup process should be the only person sending out the EFT Agreement form to the requesting vendor. However, it had been common practice for the forms to be sent to vendors through the County employee project managers, which directly contradicted the first step in the SOP.

The CFO described the EFT procedure as it was outlined in the current SOP. She confirmed that once they receive the EFT Agreement form, completed and signed by an "authorized person" from the vendor, along with a voided check or bank letter to support the information provided on the form, the Treasury Clerk is supposed to conduct a Google search of the vendor's name, place a telephone call to the phone number listed in the search results, and ask for the individual who submitted the form to verify the information. This verification process is documented on the EFT setup checklist. Once the Treasury Clerk confirms and verifies as noted above, they submit the checklist along with supporting documentation, to the Director for review and approval. Once approved, the Treasury Clerk enters the account and routing information in the vendor record.

Testimony pertaining to what differed in this incident consistently identified the verification portion of the SOP, and the failure to confirm the identity of the requester, prior to updating the EFT information.

According to the SJC Utilities Manager, vendors typically initiate EFT requests or changes through their point of contact at the County, such as the assigned Project Manager. At no point were

Utilities personnel instructed **not** to send EFT Agreement forms to vendors who were requesting a change to their payment method. Prior to this incident, the Utilities Manager requested a copy of a blank EFT Agreement form through an e-mail to the Director; however, it was the Treasury Clerk who provided the form. The Utilities Manager advised that he saved a copy of the blank form to eliminate the step of having to request the form each time they received a request. This practice conflicts with Step # 1 of the EFT SOP.

- **Step # 1:** *The person designated to set up [sic] EFTs in the office is the only one to send out setup forms directly to the vendor trying to set up [sic]. The form is not to be sent to another department for them to send out. This minimizes variations of the form out there and we like to maintain that control in our office...*

In this instance, the Project Manager received the initial request from the individual impersonating a vendor and elevated the request to the Utilities Manager, who ultimately sent the EFT Agreement form to the scammer with instructions to submit the form to the Treasury Clerk, which they did.

The CFO did not believe that the Treasury Clerk adhered to the SOP; specifically, that she failed to conduct a Google search to verify the contact information as required in Step # 3 of the SOP.

- **Step # 3:** *The company info needs to be compared to our system for the same EIN and address information. (Fund Accounting/Reference Tables/Vendor List) Then Google the company to match the address and phone information to the forms presented. Make a printout of the information found attached to the packet.*

The CFO stated that it appeared that the Treasury Clerk used the e-mail thread that she (the Treasury Clerk) thought was from the vendor to the Utilities Department as verification, in lieu of contacting the vendor for verbal verification, as required in Step # 4 of the SOP.

- **Step # 4:** *Once all information has been received and the vendor information has been confirmed, the company will need to be contacted to make final verbal verification that they would like to set up [sic] to receive EFT payments from us and confirm the bank where funds will be sent.*

The voided check submitted by the scammer, as one of the required documents, was discussed during the interviews as it contained “red flags” that should have been questioned during the EFT setup process. Although the voided check submission was required as part of the EFT Agreement packet, testimony revealed the check was not examined prior to the approval of the EFT setup request.

The Director did not recall seeing the voided check, or whether it was submitted with the EFT setup checklist. Upon reviewing the voided check during her interview, she identified a spelling error, “routine” instead of “routing,” on the check. The Director indicated that she typically reviewed the checks by looking only at numbers; however, she thought the Treasury Clerk had been reviewing the documents for inconsistencies.

The CFO stated she would not have approved the EFT setup checklist in question. She stated that the Director did not receive a copy of the voided check when she approved the checklist. She confirmed there were obvious red flags on the voided check, such as spelling errors and dotted lines. The CFO asked both the Director and the Treasury Clerk whether the voided check was included in the packet submitted with the checklist for approval; the Director said it was not, the

Treasury Clerk said she did not recall seeing it in the packet; however, the packet was still approved.

SUBJECT TESTIMONY

The Treasury Clerk described her responsibilities at the time of the incident, to include the verification of changes to banking information. Processing EFT setups was part of her duties at the time of the incident.

The Treasury Clerk's account of the incident mirrored witness testimony, stating that she received an e-mail request to change a vendor's payment method information on July 31, 2023. An individual impersonating a County vendor e-mailed the Project Manager requesting a change to their banking information. The Utilities Manager e-mailed the EFT Agreement form to the scammer and once it was completed, the scammer e-mailed the form to the Treasury Clerk. Once the form was received, the Treasury Clerk completed the EFT Checklist, then submitted the checklist and form to the Director for review. Once the checklist was approved, the Treasury Clerk updated the vendor's information to reflect the information presented on the EFT Agreement form.

According to the Treasury Clerk, the EFT setup checklist was introduced as a guide to ensure the responsible party (in this case the Treasury Clerk) was completing the required steps and receiving the necessary documents to properly complete the EFT setup process.

Referring to the EFT Checklist, specifically line # 4, *how the contact information for the vendor was found*, which gives the example as, "website," and line # 5 *Contact @ Company who confirmed info*, the Treasury Clerk was asked to explain what she believed were the intentions of those lines.

The Treasury Clerk explained that the purpose of line # 4 was to verify that the company listed on the request was the actual company requesting the change, using Google. The Treasury Clerk indicated that the line was there to verify identity. She stated that in this instance, since the request was coming from an existing vendor, there was no need to research the contact information or website. Instead, she used the e-mail request from the Utilities Manager to satisfy the SOP and EFT setup checklist line # 4, which she believed was sufficient to satisfy the verification portion of the checklist.

The Treasury Clerk indicated that the intention of line # 5 was to name the person who submitted the request. The Treasury Clerk said she did not think a phone call to confirm the information was required and could not think of a time when she had ever called a vendor to verify the information. She said she did not recall whether she had ever been instructed to make verification phone calls as part of the EFT setup process. According to her, the only time a phone call was necessary was if the vendor was having issues with the process and required assistance.

The Treasury Clerk was responsible for processing EFT setups for approximately two years and stated she did not recall ever seeing the EFT Setup SOP during that time. Although other testimony and e-mail documentation indicate that the Treasury Clerk did receive a copy of the SOP, she continued to convey that she had no knowledge of the SOP and further stated that even if she had read it in the past, she did not refer to it. She indicated that she trained herself with no guidance or supervision because she did not have a manager (she mentioned having three different Managers during the period she was performing this duty).

She acknowledged that it was her responsibility to confirm that requests for bank changes were coming from legitimate sources; however, she believed that responsibility would be built into the

established process. When asked why she would not follow the established process if she was relying on the process to satisfy that responsibility, she stated she did not recall.

The Treasury Clerk indicated that to her, an SOP was built for the person who was performing the job related to that SOP and questioned whether she needed to follow an SOP that somebody else wrote. The Treasury Clerk stated that she had never written an SOP and when asked whether she would follow her own process over an SOP, she indicated that she worked on a case-by-case basis. The Treasury Clerk stated she assumed that since her work had been reviewed by various managers, and she had never been told she was doing something wrong, that everything was “okay.” She emphasized several times that her work was never questioned during the review process and stated it was never impressed upon her by management that she had to follow an SOP.

Regarding the e-mail sent from the scammer to the Treasury Clerk, the Treasury Clerk stated that although she had completed Cyber-security training, she did not notice the originating e-mail domain extension was “.co” as compared to “.com.” The Treasury Clerk further stated that even if she had noticed the “.co,” she would not have identified that as potential fraud, because of her lack of knowledge of the existence of that domain extension.

The Treasury Clerk mentioned she was responsible for verifying and inputting vendor information and questioned “where are the separation of duties?” She further stated it was not clear to her nor her various managers, who was responsible for what.

CONCLUSION

The BOCC Finance Department’s EFT Setup SOP at the time of this incident was established in response to a similar event that occurred in or about August of 2020. The AP Supervisor, formerly responsible for the EFT setups during the time of the 2020 incident, authored the SOP outlining the current EFT setup process. The EFT setup checklist was introduced as a guide to ensure the responsible party was completing the required steps outlined in the SOP and receiving the necessary documents to properly complete the EFT setup process.

Based on records and testimony, including the Treasury Clerk’s own testimony, the investigation substantiated that the Treasury Clerk failed to follow the EFT Setup SOP, and as a result, St. Johns County taxpayer dollars were compromised.

The Treasury Clerk testified that she did not recall seeing the SOP; however, she articulated a clear understanding of various requirements outlined in the SOP that she did not adhere to, and records indicated the SOP had been e-mailed directly to her. She further testified that even if she had read the SOP in the past, she did not refer to it in performing EFT setups; rather, she handled them on a case-by-case basis.

Records and testimony also confirmed that the Treasury Clerk did not contact the vendor for verbal verification and did not Google search the vendor to match the contact information, as required by the SOP. Had she completed these required steps in this instance, the procedures may have prevented the fraud.

ADDITIONAL INFORMATION

Although the Treasury Clerk’s lack of due diligence and failure to follow procedures were not disputed, there were other internal factors that contributed to this system failure. The investigation

revealed the following additional information and areas for improvement that should be addressed to assist in mitigating the risk of this type of incident from reoccurring:

- It was determined that although SOPs existed within BOCC Finance, there was no consistent or formal process by which SOPs were created, effected, maintained, distributed, or acknowledged. Staff testimony was consistent in indicating a lack of knowledge pertaining to the content or location of BOCC Finance SOPs. Additionally, the existing SOP for EFT setups included outdated information, such as the individual responsible for reviewing the EFT setups.
- There was no mechanism in place by which BOCC Finance staff authenticated that the individual who submitted the EFT Agreement form was an authorized individual to make such a request. The absence of this procedure was apparent when BOCC Finance staff, including the CFO, were asked how they confirmed the individual making a request was a person authorized to change vendor payment information; all who were interviewed stated they did not know.
- The verification process to confirm the legitimacy of a vendor request and the responsibilities to validate that the information received was accurate, fell on one individual; the same individual entered the banking information into the payment system. There was no secondary control, such as dual signature, to enhance the security and confirm the payment information was accurate and legitimate.
- The scammer utilized e-mail to request the payment method change, posing as a vendor representative. The e-mail address mirrored the actual verified e-mail of the vendor, except for the domain extension. The scammer's e-mail employed the domain extension of .co, which differed from the actual .com used by the vendor. Throughout the entire process, this variation went unnoticed.
- The Director approved the EFT setup, despite all the required documents not being included and reviewed as part of the EFT setup checklist packet. Although the Director indicated she had no knowledge of the SOP, she confirmed during her interview that a voided check was a required document to complete her review. Testimony confirmed that the voided check submitted by the scammer, as required by the EFT Agreement form, was not reviewed prior to the approval.

RESPONSES TO DRAFT FINDINGS

The Treasury Clerk was afforded the opportunity to review and respond to the draft report of investigation. The Treasury Clerk reviewed the draft report and declined the opportunity to provide a response.

The COCC Chief Technology Officer John Rundgren, serving as the Clerk's designee at the time, was afforded an opportunity to review and respond to the draft report. On behalf of the Clerk/Designee, the CFO submitted a response, which is attached to this report.

IDENTIFIED, QUESTIONED, AND AVOIDABLE COSTS

The initial voucher, V74987, was issued August 28, 2023. The total amount of the voucher was \$551,363.39. To date, the total funds recovered for Voucher V74987 are \$50,479.46. The net loss to date is \$500,883.93.

The second voucher, V75550, was issued September 26, 2023. The total amount of the voucher was \$612,431.89. The total funds recovered for Voucher V75550 are \$612,431.89. The net loss to date is \$0.00.

As of January 9, 2025, negotiations with the fraud department of the receiving bank, BMO, are continuing, per the COCC CFO. The total net loss of both vouchers to date is **\$500,883.93**.

RECOMMENDATIONS

The OIG recommends the St. Johns County Clerk of the Circuit Court and Comptroller Chief Finance Officer:

1. Develop a process for the drafting, review, approval, dissemination, and employee acknowledgement of all new and revised BOCC SOPs.
2. Consider limiting authorization to approve and effect policies to the CFO or Clerk.
3. Conduct periodic reviews of all BOCC SOPs and revise, as necessary, ensuring all staff are notified in writing of any revisions. Ensure all policies include the approver's name, effective date, review date(s), and revision dates.
4. Share SOPs with all employees and agencies, such as County staff, if/when they have an active role in a BOCC process, (program managers, grant managers, etc.).
5. Include in staff training and/or signed employee acknowledgement of SOPs that staff are prohibited from deviating from existing department standards and SOPs, without documented exceptions approved by management.
6. Review all BOCC Finance policies and procedures and determine if any revisions are needed to reflect current operating procedures.
7. Review all BOCC Finance policies and procedures and determine whether current procedures include effective controls and best practices to safeguard funds and update as necessary.
8. Establish a process and require BOCC Finance staff to independently identify and authenticate persons at each vendor who are authorized to make requests or changes to vendor profile information, including payment, financial, or contact information.
9. Update and maintain vendor management system to reflect current, accurate, and complete vendor information, to include, at minimum, names and contact information of individuals authorized to change or approve changes to vendor profile information.
10. Ensure a separation of duties between staff who manage vendor information in vendor information system and staff who release payment to the vendor.
11. Rescind previous EFT SOP and notify staff of revised EFT SOP for handling. Document staff acknowledgements of rescinded and revised policies and notify BOCC staff of changes in procedures.

The OIG recommends the St. Johns County Clerk of Courts and Comptroller:

1. Ensure all BOCC staff are provided training on fraud detection and prevention.
2. Review the findings within this report and determine whether personnel action or re-assignment of duties are deemed necessary for the Treasury Clerk, BOCC Accounting Director, or CFO.
3. Consider setting a standard for all COCC Departments and Divisions to establish SOPs relevant to their processes that are; approved by management, have documented distribution to and acknowledgement by applicable staff, are periodically reviewed and revised, as necessary, and include the title, purpose, effective date, review date(s), revision date(s), approver name, and to whom the policy applies.

Attachments:

1. Exhibit 1: Clerk's Response to Draft Report Findings
2. Exhibit 2: EFT Setup SOP
3. Exhibit 3: EFT Form and Agreement
4. Exhibit 4: W-9 Request for Taxpayer Identification Number
5. Exhibit 5: E-mails
6. Exhibit 6: EFT Setup Checklist
7. Exhibit 7: Voided Check

Exhibit 1



Brandon J. Patty

Clerk of the Circuit Court and County Comptroller | St. Johns County, Florida
4010 Lewis Speedway, St. Augustine, FL 32084
(904) 819-3600 | www.stjohnsclerk.com

August 21, 2024

Elizabeth Gonzalez, Interim Inspector General:

RE: Response to OIG Investigation Report 2024-0002

The employee in question was reassigned to other duties the day after this incident occurred. The employee is no longer involved with any tasks that relate to any type of vendor management.

As the result of this incident, Clerk Brandon Patty led the charge of finding a third-party vendor verification company. This charge was carried out by the comptroller staff, with the help of the BOCC purchasing department. The Comptroller's office now has a third-party vendor verification company in place, PaymentWorks. This third-party company not only verifies vendor banking information, but also verifies that the business is legitimate on levels that staff does not have access to. Employees no longer communicate with any vendor for account changes or makes any changes to the vendor record at the vendor's request by email nor phone. All changes must be initiated by the vendor through the platform and verified, no exceptions. In addition to this verification process, all vendor payments that have been verified are also indemnified by PaymentWorks. The Comptroller's office went live with this new verification company in March 2024. We currently have 511 vendors verified and indemnified.

In the future, management will ensure all staff receives, and further acknowledges receipt of, any procedural or policy changes in the office. Management will also ensure staff acknowledges that they understand the changes in question. Acknowledgements will be kept on file for reference.

Although this was an unfortunate incident, it allowed the Comptroller's office to uncover and correct a procedural deficiency. The vendor management process is now more streamlined and secure for the clerk's office as well as the vendors. It also provides better protection for county assets.

Sincerely,

Dwala Anderson, MBA, CGFO
Chief Financial Officer

Exhibit 2



STANDARD OPERATING PROCEDURES

DATE 10/20/2021

DEPT BOCC Finance

SOP # _____

DESCRIPTION EFT setup

PURPOSE: Describe how to setup vendors to receive EFT transactions

PREPARED BY: Donna Echegoyen

REVIEWED BY:

#	STEP
1	Person designated to setup EFTs in the office is the only one to send out setup forms directly to the vendor trying to setup. The form is not to be sent to another department for them to send out. This minimizes variations of the form out there and we like to maintain that control in our office.
2	Upon receiving the requested information (completed, signed form and a copy of a voided check or bank letter an ' <i>EFT checklist</i> ' form must be completed. NOTE- The current exceptions are for CBC and Amphitheatre vendors that are actual people and not companies.
3	The company info needs to be compared to our system for the same EIN and address information. (Fund Accounting/Reference Tables/Vendor List) Then Google the company to match the address and phone information to the forms presented. Make a printout of the information found to attach to the packet.
4	Once all information has been received and the vendor information has been confirmed, the company will need to be contacted to make final verbal verification that they would like to setup to receive EFT payments from us and confirm the bank where funds will be sent.
5	Once the verbal part has been done the packet needs to be given to Dwala with the checklist on top.
6	Once she has returned the packet to you-it will be indicated if it's Ok, or not. You will then look up the appropriate bank code located in: Fund Accounting/Reference Tables/EFT Bank Codes
7	In the bank code table, you can hit enter to show the whole list and sort by routing number or instead of looking through the list you can look up by the routing number by typing that in at the Bank Routing Number field and hitting enter.
8	Once the bank code has been found, note that on the setup paperwork.
9	Go to the vendor's record and enter their web address if they have one on the first tab of information, enter the phone # if there isn't one there already (I enter under the purchasing address so that it's visible for them as well). Go to the EFT/ACH tab and choose the appropriate Transaction Code . Checking will be 23- 2nd Checking Prenote Savings will be- 33 2nd Savings Prenote Bank Code -will be the bank code you looked up already Account number -will be the account number on their voided check or bank letter-NOT what they may have typed on the form A/P Email -will be the Email address they have provided to receive notifications at.

ANNUAL REVIEW DATE: _____

Exhibit 3

ELECTRONIC FUNDS TRANSFER FORM AND AGREEMENT

8/7/23 Acc N/P void

<small>(Official Use Only)</small>
Vendor# 122511

PART I

As a payment option, the company or individual described below ("Company") authorizes St. Johns County to initiate credit entries via electronic funds transfer ("EFT") pursuant to this Electronic Funds Transfer Form and Agreement ("EFT Agreement").

Select request type.

Type of Request		
<input type="checkbox"/> New Request	<input checked="" type="checkbox"/> Change of Information	<input type="checkbox"/> Stop EFT

Enter Company details.

Payee Information			
Company/Individual Name:	DBE Management, LLC Dba DBE UTILITY SERVICES	FEIN/SSN Number:	20-1331070
Company Address:	13387 Bryan Rd		
City, State and Zip:	Loxahatchee, FL 33470		

Enter the contact details of the Company representative authorized to manage electronic payments on behalf of Company.

Company Representative			
Name:	Cindy Galt	Main Phone #	561) 508-3708
Title:	Accounts Receivable Leader	Direct Phone #	561) 508-3708
Email:	cgalt@dbehdd.com	Fax#	

Enter banking details.

Financial Details			
Select Account Type:	<input checked="" type="checkbox"/> Checking	<input type="checkbox"/> Savings	
Bank Name:	BMO HARRIS BANK, NA BC-662	Bank Contact Phone #	(855) 259-8521
Bank Contact Name:		Account Name:	DBE Management LLC Dba DBE UTILITY SERVICES
ACH Routing #	071025661	Bank Account #	4832813285

(Due to system constraints bank account number is limited to 18 or less digits.)

ATTACH A VOIDED CHECK OR LETTER FROM YOUR BANKING FACILITY WITH ROUTING NUMBER, ACCOUNT NUMBER AND ACCOUNT TYPE.

Remittance Notification			
Are email notifications requested?	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> No	
Name:	Cindy Galt		
Email Address:	cgalt@dbehdd.com		

PART II

Company acknowledges and agrees to the following terms and conditions under which St. Johns County will initiate payments to Company:

- Company shall complete and submit a new EFT Form to St. Johns County to initiate electronic funds transfer (EFT) payments. Company shall also complete and submit a new EFT form to St. Johns County when there is any change to Company's name, legal structure, Tax ID number or banking facility. All payments to Company may be withheld or delayed until such new EFT Form is executed to the satisfaction of St. Johns County.
- St. Johns County is relying on the information provided by Company on this EFT Form. Company may change any portion of the information provided on the EFT Form by completing and submitting a new EFT Form. Any such change in Company's information must be communicated to St. Johns County no less than thirty (30) business days prior to the next EFT payment. Company shall be responsible for any loss of payment as a failure to timely communicate changed information to St. Johns County.

Exhibit 4

✓-122511

Code @ ipeda

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

Go to www.irs.gov/FormW9 for instructions and the latest information.

Print or type.
See Specific Instructions on page 3.

1 Name (as shown on your income tax return). Name is required on this line; do not leave this line blank.
DBE MANAGEMENT LLC

2 Business name/disregarded entity name, if different from above.
DBE UTILITY SERVICES

3 Check appropriate box for federal tax classification of the person whose name is entered on line 1. Check only one of the following seven boxes.

Individual/sole proprietor or single-member LLC

C Corporation

S Corporation

Partnership

Trust/estate

Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=Partnership) **P**

Note: Check the appropriate box in the line above for the tax classification of the single-member owner. Do not check LLC if the LLC is classified as a single-member LLC that is disregarded from the owner unless the owner of the LLC is another LLC that is not disregarded from the owner for U.S. federal tax purposes. Otherwise, a single-member LLC that is disregarded from the owner should check the appropriate box for the tax classification of its owner.

Other (see instructions) **P**

4 Exemptions (codes apply only to certain entities, not individuals; see instructions on page 3):

Exempt payee code (if any) _____

Exemption from FATCA reporting code (if any) _____

(Applies to accounts maintained outside the U.S.)

5 Address (number, street, and apt. or suite no.) See instructions.
13387 BRYAN RD

6 City, state, and ZIP code
LOXAHATCHEE FL 33470

7 List account number(s) here (optional)

Requester's name and address (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on line 1 to avoid backup withholding. For individuals, this is generally your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the instructions for Part I, later. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN*, later.

Note: If the account is in more than one name, see the instructions for line 1. Also see *What Name and Number To Give the Requester* for guidelines on whose number to enter.

Social security number

--	--	--	--	--	--	--	--	--	--

or

Employer identification number

2	0	-	1	3	3	1	0	7	0
---	---	---	---	---	---	---	---	---	---

Part II Certification

Under penalties of perjury, I certify that:

- The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me); and
- I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding; and
- I am a U.S. citizen or other U.S. person (defined below); and
- The FATCA code(s) entered on this form (if any) indicating that I am exempt from FATCA reporting is correct.

Certification instructions: You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions for Part II, later.

Sign Here Signature of U.S. person **[Signature]**

Date **01/01/2023**

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Future developments. For the latest information about developments related to Form W-9 and its instructions, such as legislation enacted after they were published, go to www.irs.gov/FormW9.

Purpose of Form

An individual or entity (Form W-9 requester) who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) which may be your social security number (SSN), individual taxpayer identification number (ITIN), adoption taxpayer identification number (ATIN), or employer identification number (EIN), to report on an information return the amount paid to you, or other amount reportable on an information return. Examples of information returns include, but are not limited to, the following:

- Form 1099-INT (interest earned or paid)

- Form 1099-DIV (dividends, including those from stocks or mutual funds)
 - Form 1099-MISC (various types of income, prizes, awards, or gross proceeds)
 - Form 1099-B (stock or mutual fund sales and certain other transactions by brokers)
 - Form 1099-S (proceeds from real estate transactions)
 - Form 1099-K (merchant card and third party network transactions)
 - Form 1098 (home mortgage interest), 1098-E (student loan interest), 1098-T (tuition)
 - Form 1099-C (canceled debt)
 - Form 1099-A (acquisition or abandonment of secured property)
 - Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN.
- If you do not return Form W-9 to the requester with a TIN, you might be subject to backup withholding. See What is backup withholding, later.

Exhibit 5

Vivien McWilliams

From: Cindy Galt <cgalt@dbehdd.co>
Sent: Monday, July 31, 2023 1:34 PM
To: Vivien McWilliams
Cc: James Galley
Subject: RE: DBE MANAGEMENT LLC - DUE INVOICE...
Attachments: EFT form Rev 1 (1).pdf; DBE_Void_Cheque.pdf

Importance: High

Good day, Vivian and James,

Find attached form and voided check, for payment processing.
Kindly update our remittance information and let me know once updated.
Awaiting your prompt response.

Cindy Galt
DBE Management, LLC.
Dba DBE Utility Services
13387 Bryan Rd
Loxahatchee, FL 33470.

On 07/31/2023 10:21 AM EDT James Galley <jgalley@sjcfl.us> wrote:

Cindy,

Here is the EFT for the County. Please send back to Vivien McWilliams who is copied on this e-mail.

Thank you,

Exhibit 6

EFT Setup Checklist

Vendor Name & Number	<u>DBE MANAGEMENT, LLC (VENDOR# 122511)</u>
Date EFT form received	<u>7/31/2023</u>
How was form rec'd (fax, mail, interoffice)	<u>Email</u>
How contact info found, website?	<u>James Galley/Utility Staff sent initial request for their vendor to be paid via EFT</u>
Contact @ company who confirmed info.	<u>Cindy Galt, Accounting Representative</u>
Need for Additional information	<u>None</u>
Date Turned in for Review:	<u>7/31/2023 <u>Yes</u> 8/2/23</u>
REVIEWED/APPROVED BY AND DATE:	<u>JK 8/2/23</u>
Date Entered New/Change Info:	<u><u>Yes</u> 8/2/23</u>
Date Prenoted:	<u>8/1/23 Dec AIP Voucher <u>Yes</u></u>
Date Complete:	<u>8/1/23 <u>Yes</u></u>


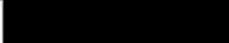
Exhibit 7

JULY, 5, 2023

To: Whom it may concern

Re: Void Cheque

Please accept this copy of void cheque as confirmation of " DBE Management " bank account information for the purposes of pre-authorized debit or credit.

DBE Management, LLC. 13387 Bryan Rd Loxahatchee, FL 33470		<u>07</u> <u>5</u> <u>2023</u>
PAY TO THE ORDER OF	VOID	\$ _____ / DOLLARS
BMO 		
Harris Bank		
MEMO	071025661 Routine	 Account Number