INTERNAL AUDIT REPORT

Operational Audit
ACH Payment Fraud

January 2021 – December 2021

Issue Date: March 30, 2022
Report No. 2022-01

Port of Seattle | INTERNAL AUDIT

TABLE OF CONTENTS

Executive Summary

Internal Audit (IA) completed a targeted audit of the processes that contributed to eight payments totaling $572,682.79, being wired into fraudulent bank accounts. The payments were for the Port of Seattle's (Port's) Opportunity Youth Initiative and were intended for the Seattle Parks Foundation (Seattle Parks) and the Urban League of Metropolitan Seattle (Urban League). The purpose of the audit was to identify the control breakdowns that allowed the fraud to occur and to recommend ways to reduce the likelihood of future misappropriations. Using a targeted approach, we evaluated both preventive and detective internal controls, segregation of duties, and change management processes for the period January through December 2021. The criminal aspect of this case was handed off to the Port Police for their continuing investigation.

Through a control design failure, over the course of four months, the Port made eight Automated Clearing House (ACH) payments to fraudulent parties. For Seattle Parks, two payments were processed for $135,678.02 and were unrecoverable by the Port's bank, Wells Fargo. A third payment for $48,084.93 was returned by Wells Fargo, as the fraudulent bank account had been closed. For Urban League, five payments were processed for $388,007.38. As of the time of this report, an unknown amount of funds in a fraudulent account, were frozen by Citibank, upon being contacted by Port Police. The funds were targeted for Urban League.

Both cases appear to be the result of Business Email Compromise[1]. A genuine email account, of a staff level employee, at both Seattle Parks and Urban League was compromised. The fraudster, using the compromised email account and copying fraudulent domain names, that appeared to be other Seattle Parks and Urban League employees, requested a change to banking information. For example, a fraudulent email was received on October 4th, 2021. The email appeared to be from a Seattle Parks Foundation employee's email account. The parties involved in the fraud also set up a fraudulent email account for the director at the Seattle Parks Foundation using Michelle@Seattle**Praks**Foundation.org. Seven Port employees failed to identify the fraudulent domain name, that the tone and font in the emails had changed, that the emails used improper grammar, and that the emails were now requesting changes to banking information. Additionally, the first fraudulent payment of $91,593.09, to a PNC Bank account, was returned to the Port with a reason code of: "ACCOUNT FROZEN/RETURNED PER OFAC REQUEST". The Office of Foreign Assets Control ("OFAC") of the US Department of the Treasury administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States. This was a red flag that was not appropriately acted on by Port employees.

The fraudster then emailed the Port and said, "the ACH you sent last week have returned due to the account Audit…Kindly confirm respond and we will send you ACH details to resend the payment." Standard Port Controls were not followed, and employees unknowingly worked with the fraudster, responding several times to Michelle@SeattlePraksFoundation.org. Accounting and Financial Reporting (AFR) then proceeded to transfer funds to the fraudster's accounts. This front-end failure underscores the need for certain employees to attend basic cybersecurity training. According to Human Resources' training records, five out of seven Port employees who directly or indirectly received the fraudulent emails, had not attended the Port's required cybersecurity training in 2021.

However, the key control failure that allowed this fraud to occur, was a process that put the burden of verifying and approving supplier banking changes, on an Administrative Professional within AFR's Core Services Team, who worked remotely during this time, with inadequate oversight. The Notes section in PeopleSoft Financials system on how the verification was performed, was not completed as intended. Our testing found that 58 employees at the Port had the ability to add or change supplier information, and

[1] https://www.interpol.int/en/Crimes/Financial-crime/Business-Email-Compromise-Fraud

supplier contact information was poorly maintained; contact name, phone number, and email address were often missing. Procedurally, all changes had to be verified and approved by the AFR Core Services Team, before becoming live in the PeopleSoft system.

Numerous red flags were missed, however, the fundamental flaw that allowed this fraud to occur was the key control failure described above. A more detailed timeline is provided in the Background section of this report.

We have categorized our findings into the five issues listed below. Additionally, we have provided recommendations on how to potentially correct these control deficiencies within the body of this report.

1. **(High)** – Internal Controls to validate changes to supplier information, including banking information, were not functioning as intended. Supervisory oversight needed improvement for this critical role.
2. **(High)** – Procedures to confirm the authenticity of supplier requested bank account changes were not placed at the appropriate level.
3. **(High)** – Fifty-eight Port of Seattle employees had the ability to add and modify supplier information, including sensitive banking information, although these changes do not go live in PeopleSoft until the AFR Core Services Team approves them. Adequate controls did not exist to assure that supplier information, including banking and contact information, was entered accurately, consistently, and correctly. Additionally, with the high number of users, the risk of internal fraud increases, because an employee could change bank account data, putting the onus on one individual to approve these changes.
4. **(High)** – Detective controls to identify fraudulent activity and payments did not exist. Instead, the Port was only notified of the fraud by the client, approximately two months after the fact.
5. **(Medium)** – The methodology to assure that vulnerable employees received required training was not functioning effectively. Our review of training records indicated that, of the seven Port employees who either directly or indirectly received the fraudulent emails, only two had completed the Port's mandatory Information Security Awareness training in 2021. Additionally, Port-wide, only 51 percent or 1,036 of the 2,041 employees had completed the annual training.

These issues are discussed in more detail beginning on page eight of this report.

Glenn Fernandes, CPA
Director, Internal Audit

Responsible Management Team
Rudy Caluza, Director, Accounting and Financial Reporting
Dan Thomas, Chief Financial Officer
Ron Jimerson, Chief Information Security Officer
Pete Ramels, General Counsel / Chief Compliance Officer
Katie Gerard, Senior Director, Human Resources
Dave Soike, Chief Operating Officer
Nora Huey, Director, Central Procurement Office
Bookda Gheisar, Senior Director, Equity, Diversity & Inclusion

Background

Business Email Compromise (BEC) fraud, is a type of social engineering scam where criminals deceive company employees into transferring money to them. In this particular case, criminals gained access to a staff user account at Seattle Parks and at Urban League through malware or other security vulnerabilities. They then used these exploits to convince Port employees to electronically transfer funds to them.

An effective fraud prevention strategy includes a multi-layered approach, where all employees participate. Training programs should be designed to increase employee fraud awareness. Internal reporting structures should be established and understood so that appropriate mitigation steps are taken. However, most importantly, an internal control structure must be in place to reduce the liklihood of fraud, including a detection strategy to quickly identify the fraud if it occurs.

The following is a timeline of the Seattle Parks Foundation fraud:

Date	Event
October 4, 2021	A phishing email from a compromised email address at Seattle Parks and a fraudulent domain name using SeattlePraksFoundation, are sent to an employee in the Port's Equity, Diversity & Inclusion Office, offering a five percent (5%) discount if payment is made through ACH that week. The fraudster also requests changes to bank name, and account/routing number.
October 5, 2021	The fraudster provides updated bank information via email. (PNC Bank Account ending in 2567).
October 7, 2021	After receiving email instructions to change the bank, routing, and account number, the first (ACH) payment is made for $91,593.09. It is returned on October 13, 2021, by PNC bank with the reason code of "ACCOUNT FROZEN/RETURNED PER OFAC REQUEST."
October 13, 2021	The fraudster emails the Port and communicates that the ACH payment was "returned due to the account Audit" and requests payment to be sent again to a new account. AFR (Disbursements) communicates that payment will be re-sent the next day. Fraudster provides a different bank name, account number, and routing number (Dollar Bank ending in 0014).
October 14, 2021	The first fraudulent ACH payment is re-issued to Dollar Bank for $91,593.09.
November 2, 2021	The second fraudulent ACH payment is sent to Dollar Bank for $44,084.93.
December 9, 2021	Wells Fargo notifies the Port's Treasury Department that the ACH payment for $48,997.39 was declined because the account had been closed.
December 9, 2021	In less than an hour of being notified that the ACH payment had been returned, Port Employees submit a request to change the bank account, back to the original fraudulent PNC Bank Account.
December 9, 2021	Michelle Benetua, the Director of Strategic Partnerships and Programs, Seattle Park Foundation, states via email "We've had some fraud issues lately, so just want to clarify where you're sending it."
December 10, 2021	Michelle Benetua, via email states "Please wait until Monday before doing anything. PNC is not our bank!!"
December 14, 2021	Fraud is reported to Wells Fargo, Port Police, and the Federal Bureau of Investigation, through the Internet Crime Complaint Center. The fraud is also reported to the State Auditor's Office as required by RCW 43.09.185.

ACH Payment Fraud

The following is a timeline of the Urban League of Metropolitan Seattle fraud:

Date	Event
December 6, 2021	A phishing email from a compromised email address at Urban League and fraudulent domain name using Urban**l**eague (L changed to I), is sent to an employee in the Port's Equity, Diversity & Equity Office notifying them that the Key Bank Account was closed and unable to receive payments. The fraudulent domain name was very hard to spot without changing the font. The Port employee unknowingly forwards the phishing email to two other Port employees. The fraudster then expresses a sense of urgency and sends a falsified bank letter (Appendix B) that requests the change in banking information to Citibank. (Citibank Account # ending in 1236) The letter has several indicators of fraud including the wrong spelling of Citibank and grammatical issues. The change is entered into PeopleSoft by Port employees and approved without following Port procedures.
December 7, 2021	A Port employee confirms back to the compromised email address, copying the fraudulent domain names, that the banking information has been changed and approved.
December 9, 2021	The first payment of $66,234.70 is sent to the fraudulent Citibank account.
December 13, 2021	A Port employee sends an email to the compromised email address, copying the fraudulent domain names, and notifies the fraudster that payment has been made. The fraudster asks if payment was made to their Chase Account (The fraudster is referencing the wrong bank; Chase instead of Citibank). The fraudster then thanks the Port employee for updating the banking information and asks her to confirm payment date for the attached invoice. That attached invoice shows Chase Bank, Routing # 271070801, and Account # ending 1236, which are the routing and account numbers for the fraudulent Citibank account.
December 14, 2021	A second payment of $14,250 is sent to the fraudulent Citibank account.
January 4, 2022	A third payment of $9,850 is sent to the fraudulent Citibank account.
January 18, 2022	A fourth payment for three separate invoices for a total of $243,126.16 is sent to the fraudulent Citibank account.
January 25, 2022	A fifth payment for four separate invoices for a total of $54,546.52 is sent to the fraudulent Citibank account.
January 28, 2022	Mansour Camara, Chief Financial Officer at Urban League emails the Port, inquiring about payments.
January 31, 2022	The Port contacts Mansour Camara, who indicates that the Citibank account is fraudulent.

Audit Scope and Methodology

We conducted the engagement in accordance with Generally Accepted Government Auditing Standards and the International Standards for the Professional Practice of Internal Auditing. Those standards require that we plan and conduct an engagement to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our engagement objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our engagement objectives.

In some cases, we used a judgmental method to determine the samples selected for our audit test work, in those cases, the results of the work cannot be projected to the population as whole, as we did not select a statistical sample. The period audited was January 2021 through December 2021 and included the following procedures:

Evaluation of bank account change management processes and internal controls

- Reviewed policy and procedural documentation (AC-18 Supplier Management Policy and Procedures as of 2/28/2020) and assessed whether they were clear and generally easy to understand.
- Interviewed both management and staff to determine whether they were familiar with and understood roles and responsibilities.
- Inquired with staff and management to obtain their assessment of the breakdowns and their assessment of what could have been done to prevent the fraud.
- Obtained information security awareness training records for the 12-month period ending December 31, 2021. Separated the records between those individuals who completed and those who did not complete “general phishing” training.
- Analyzed email data between the fraudsters and Port employees to identify the timing of the fraudulent requests and time frame that Port Policies were not followed.

Assessment of segregation of duties

- Obtained a list of Port employees with the ability to edit/modify supplier data and a list of employees with the ability to approve supplier updates.
- Interviewed AFR management to obtain an understanding of roles and responsibilities and internal controls.
- Reviewed CPO documentation regarding supplier set-up procedures.
- Evaluated department roles, including the appropriateness of approval functions.
- Validated that quarterly user access controls were performed.

Evaluation of fraud preventive and detective controls

Fraud Preventive Controls: Evaluated in the above two procedures.

Fraud Detective Controls:

- Researched the best practices of detective controls for electronic supplier payments.
- Inquired with management and staff, and reviewed relevant documents to determine whether there were a process and controls established for monitoring, reconciling, and detecting unusual/irregular ACH payment activities and/or banking/ACH information changes.
- Conducted process walkthroughs to identify controls/gaps in the process and evaluate the effectiveness of key controls, if any established.
- Obtained and analyzed the data of suppliers' banking/ACH information changes requested/made to the PeopleSoft Financials system for the recent 12 months.
- Reviewed the procedures currently being taken by the AFR/AP managers to re-validate banking information changes made for the recent 16 months with supplier representatives.

Schedule of Findings and Recommendations

1) Rating: High

Internal Controls to validate changes to supplier information, including banking information, were not functioning as intended. Supervisory oversight needed improvement for this critical role.

Numerous people can make changes to supplier data, including banking information, however, those changes do not go live in the PeopleSoft Financials system until approved by the AFR Core Services Team (aka Vendor Management Team). The Administrative Professional tasked with approving these changes was not performing the appropriate verification of changes as required.

When documented processes are not followed or enforced, internal controls typically do not operate as intended and the likelihood of fraud and errors increase. Listed below are essential control requirements that were noted in the AC-18 Supplier Management Policy and Procedures, but were not followed:

> *Requirement(s):* "*All requested changes will be reviewed and approved by the AFR Vendor Management Team…If you received the request by mail, fax or text message or email, verify it with a phone call."*
>
> *"To ensure appropriate internal controls, Supplier approvers independently verify adds or updates to specific changes to Supplier data."*
>
> *Status:* This was the primary control that failed. If a call had been correctly placed as required, the supplier would have indicated that their bank had not changed.
>
> *Requirement(s):* *"Before entering any changes into PeopleSoft Financial system, AP staff must validate any change to payment instructions, banking information, address changes or contact information by contacting the department or buyer that is managing the vendor/invoice or by contacting the vendor directly."*
>
> *Status:* Management indicated that this practice was not followed.

The policy also includes the following language: *"Failure to follow this Policy and Protocols: A staff member who fails to follow the policy and protocols can be held accountable and subject to disciplinary action."* While true, management should not abdicate responsibility for this control failure.

We would like to emphasize that segregation of duties between those inputting the data and those approving the data is still important and should be maintained.

Recommendations:

We recommend AFR management develop an oversight function to identify, when critical requirements, such as confirming bank account changes, have not been performed. We also suggest that management update any policies that are no longer followed.

To aid in authenticating bank information, AFR management should consider investing in a software service that assists in bank verification by providing account holder name, bank name, account holder tax ID number, etc. This vital information will provide the verifier at the Port, the appropriate tools to authenticate changes and additions to bank account information.

Management Response/Action Plan:

Recommendations: We agree.

Management oversight has been strengthened to ensure that compliance with existing protocols is well documented for all critical validations such as bank account changes. The documentation is stored centrally and reviewed regularly. Extract reports from the Supplier data files are also generated weekly for manager review, including the comments section that documents the validation steps taken for completeness.

DUE DATE: Completed

Policy updates will be made including for any new protocols implemented.

DUE DATE: In-progress, 5/31/2022

A bank account verification service solution is being reviewed with demos already provided by two potential providers. Such a service would augment, not replace, current validation control protocols in place.

DUE DATE: 4/30/2022 (Vendor selection)

Audit Observations: We provide the following for accuracy in understanding.

The finding states that numerous people can make changes to supplier data, including banking information. To ensure clarity, it is important to note that the referenced fifty-eight employees are not broadly dispersed across the Port. Rather, they are primarily in the central procurement office administering the procurements and having the most reliable direct communication lines with the Supplier for key supplier information. This is explained with completeness in management's response to Finding 3 below.

It is correctly indicated that the Accounts Payable staff no longer perform the validation tasks as noted in the finding above. To strengthen internal controls through operational segregation of duties, the validation tasks were reassigned to a separate operation within the Accounting & Financial Reporting (AFR) Department. The change was instituted to separate the operations that administer payments to Suppliers, from the operations that administer the Supplier payment/ACH information. This separate validation function has been performed for the past several years independently in this manner and in accordance with a detailed procedural checklist. The policy will be updated to reflect this change, while also to reflect recent enhancements that have been implemented.

2) Rating: High

Procedures to confirm the authenticity of supplier requested bank account changes were not placed at the appropriate level.

A well-designed process places the approval function at a level commensurate with the individual(s) responsibility. The more critical the approval, the more reliance and responsibility the organization gives that individual(s).

This is similar in concept to the Port's Delegation of Authority, where Port Commission delegates to the Executive Director, who then redelegates this responsibility to specific positions/employees with the authority to enter contractual obligations within predefined limits. The delegation schedules give increased authority to positions/individuals higher in the company because the company relies on their expertise, background, and decision making to a greater extent.

According to the AC-18 Supplier Management Policy and Procedures, "Under no circumstances will AFR staff initiate a vendor/employee payment, refund to a customer, or change to an employee's or vendor's banking or tax withholding information based upon instructions received via an email (internal or external) by phone call, by fax, or by text messages without independently validating the requested change."

However, a contributing factor to the fraud was excessive reliance placed on less experienced staff, which allowed them to perform a critical review. The skills required to perform this essential review did not align with the individual's position within the organization. An Administrative Professional had the responsibility to validate and approve supplier requests for all bank accounts changes. This individual approved approximately 82% of changes in the previous year; a Records Management Specialist approved the remaining 18%. Additionally, according to Human Resource records, the Administrative Professional had not attended the Port's required Information Security Awareness training, in both calendar years 2020 and 2021.

Recommendations:

We recommend assigning the approver validation function to an individual with the appropriate skillset, background, and knowledge. This individual should also receive the appropriate training on a regular basis as a requirement of their job.

Management Response/Action Plan:

Recommendations: We agree in part.

We agree that key to any team or individuals performing work effectively is adherence to clearly established policy and procedures, which does exist at the Port, and having the necessary skill sets along with ongoing training. Administrative Professionals at the Port prove themselves to be a very capable and valuable resource. The refinements pursued should not preclude opportunities for and the ability to leverage the talents of Administrative Professionals, by reference to their position or capabilities in the Port organization. Ongoing training and enhanced oversight, as recommended, would support success in this arena.

DUE DATE: Completed

Audit Observations: We provide the following for accuracy in understanding.

In addition to the Administrative Professional, a Records Management Specialist, both in a separate AFR Core Services operation, perform the Supplier validation and approval responsibilities.

3) Rating: High

Fifty-eight Port of Seattle employees had the ability to add and modify supplier information, including sensitive banking information, although these changes do not go live in PeopleSoft until the AFR Core Services Team approves them. Adequate controls did not exist to assure that supplier information, including banking and contact information, was entered accurately, consistently, and correctly. Additionally, with the high number of users, the risk of internal fraud increases, because an employee could change bank account data, putting the onus on one individual to approve these changes.

A shared module between Purchasing and Accounts Payable in the PeopleSoft Financials system was used to capture supplier information. The people, companies, and even internal employees from whom a company buys, or contracts goods and services are called "Suppliers." When suppliers are added, basic information is updated into the module including physical address, payment options that establish defaults for payment processing, and remit to and pricing locations.

The Port has established segregation of duties, which are an important control. However, both the individual inputting the data and the individual approving the data, need to do their respective jobs correctly.

A critical piece of information is contact phone number, which is essential, so sensitive information, such as a change to banking account data, can be verified; however, this was not a required field in PeopleSoft. Per the AC-18 Supplier Management Policy and Procedures, if a supplier requests a change using email, staff validates the authenticity of the request via a phone call, using the contact information in the supplier module. Conversely, if the request is made via phone call, it is validated through email.

We obtained contact data for suppliers who had changes to banking data, for the period January 1, 2021, through January 24, 2022, and noted that a Port Administrative Professional had approved 216 and a Record Management Specialist had approved 47 of the 263 total changes. However, most of these changes did not have phone numbers entered and only a few had email addresses entered. A lack of information makes validating the authenticity of the request more difficult. A supervisory review, to validate that the information was complete and accurate, did not appear to be occurring.

Recommendations:

We recommend reducing the number of individuals, who have system access to request additions or modifications to supplier information. We also recommend structuring the supplier module of the PeopleSoft system, so that certain fields are required to be entered (supplier phone number/ email address), either via system controls, if possible, or else via policy.

Management Response/Action Plan:

Recommendations: We agree.

A controls centric LEAN process improvement project was immediately initiated. This involved the Central Procurement Office and Accounting & Financial Reporting Department, facilitated by the Office of Strategic Initiatives (OSI) certified LEAN specialists. The team identified and is continuing to implement several enhancements, two of which parallel the recommendations.

Changes have been instituted to the ACH bank account request initiation and verification process. It refines this function to a small, centralized team of about 4 or 5 charged with this responsibility. The team includes the manager and lead of the AFR accounts payable operations who make direct contact with the Supplier and then enter and initiate the requests. The requests continue to be administered by the manager and team of the AFR core services operations to independently validate and approve or deny requested additions and changes. The work is performed in conformance with established protocol, is monitored, and will be augmented with ongoing training.

DUE DATE: Completed

Changes have been implemented to make the collection of key Supplier information a requirement and at an early point during the procurement process. The objective is that any requests to setup or change Supplier information cannot be initiated unless the required information is obtained and entered to initiate the request process. The substance of this control was implemented earlier on first through procedural controls where requests not containing the required data is denied and returned to the requester. A PeopleSoft Financials system modification that automates the inability to submit and initiate requests if the required Supplier information is not entered in the data fields online, has since been programmed. Testing was completed and this system-driven control has been timely implemented. This action strengthens controls to assure completeness in the Supplier data files for key information.

DUE DATE: Completed

Audit Observations: We provide the following for accuracy in understanding.

It is important to note that the referenced fifty-eight employees are not broadly dispersed across the Port. Moreover, they do not have the ability to add or modify any Supplier data in the system, but to only enter information to initiate requests to do so, which are then independently vetted for propriety and approved or denied accordingly. These employees are predominantly in the Central Procurement Office (CPO) and, hence, are knowledgeable and in the best position to leverage the Port's established communication lines directly with Suppliers to obtain key information through their procurement and contracting relationships. The other few are in the Accounting & Financial Reporting (AFR) Department necessary to administer the data.

Nevertheless, as detailed above in alignment with the recommendations, changes have been instituted to the ACH bank account request initiation and verification process by refining this function to a small, centralized team charged with this responsibility. ACH banking information is also no longer viewable by anyone other than a member of this limited team.

The Port of Seattle has internal controls in place that are generally strong and have proven to be effective over the past many years. System controls in place include: (1) Suppliers can be paid only if approved to be setup and active in the system through a formal validation process; (2) A Supplier is automatically rendered unapproved and cannot be transacted against when Supplier information is entered and requested to be changed until approved through formal validation; (3) Separate system access privileges exist between the ability to "request" versus the responsibility to "approve or deny" requests, and no one individual can be assigned both roles for internal controls purposes; and (4) On a monthly basis, Suppliers with no payment activity in the previous 12 months are set to "Inactive" status, which disables the ability to make payments to them until approved again through a direct phone contact with the Supplier for revalidation of ACH information.

As for process controls: (1) A formal policy is in place delineating clear expectations and control protocols to be followed; (2) Detailed guidance is in place that provides a step-by-step checklist to guide compliance with policy including directly calling Suppliers to verify ACH banking additions and changes; (3) Clear segregation of duties is in place where requesters have no edit privileges to unilaterally add or change bank account data; (4) Standard PeopleSoft system protocol is followed to enter to initiate requests for Supplier information changes, similar to other system facilitated requests such as purchase requisitions which are approved by a central procurement team; (5) Change requests are vetted independently for propriety and only if approved, they become effective; (6) The team vetting requests has no ability to enter, update or change Supplier data information, only to approve or deny.

Additionally, immediate and strengthened engagement with the Information Security Department has been

implemented. This includes a protocol that in the event of any suspicion on the credibility of email communication involving a financial transaction, the Information Security Department is immediately alerted to further investigate the situation. This will assure the ability to quickly identify and stop suspicious communications to mitigate exposing funds to any risk. Information Security will also assist the Information Communications & Technology Department (ICT) integrate an advanced technology to incorporate a more secure and confidential messaging protocol once this decision is finalized.

Moreover, internal controls can be expected to provide reasonable, and not absolute, assurance to mitigate risk exposures. The human element is a factor and can become a point of failure in any well-designed internal control environment. When the procedural compliance failure was identified involving the payment fraud, immediate stop-gap exposure mitigation measures were instituted. All ACH payments were immediately halted, and revalidations of banking information were instituted. All ACH payments are required to be compared to a complete listing of all Suppliers that had banking information additions or changes between September 2020 to-date January 2022. For any pending ACH payments that match, the Suppliers are directly called by phone to again affirm the validity of the banking information change. Also, all banking information additions and changes require two separate calls by different operations. This provides assurance that the human element does not present a single point of failure. Through this immediate risk mitigation protocol, no further exposures have been identified to-date.

It is also important to note that the Port is proactive and has in place an insurance policy that will cover such losses involving criminal activity after a $25k deductible for each of the two situations. A claim has been filed.

4) Rating: High

Detective controls to identify fraudulent activity and payments did not exist. Instead, the Port was only notified of the fraud by the client, approximately two months after the fact.

Ideally, processes are well established to prevent fraud from occurring, however, such preventative controls may not completely reduce the risk of misappropriation or errors. Therefore, detective countermeasures can also help identify when fraud has occurred, disrupt additional fraud, and reduce the consequences. Detective countermeasures are not as cost effective as prevention countermeasures. However, if detected early, the impact of fraud can be significantly reduced.

We identified some existing detective controls within the ACH payment process, including the Senior Disbursements Manager's daily review of the Accounts Payable journal against payments, the monthly bank reconciliation that agrees payment details, and the review of the Wells Fargo report that identifies remittance irregularities, such as the supplier's bank account cancellation. However, these controls do not necessarily detect fraud.

If fraud detection controls had existed, management could have identified the breakdown earlier. Instead, both fraud instances were only identified when the suppliers alerted the Port, about 60 days after the initial ACH payments to the fraudsters. See below:

Seattle Parks Foundation

October 7, 2021: The first fraudulent ACH payment is sent to the fraudulent PNC bank account.

December 10, 2021: Seattle Parks Foundation sends the following email, "Please wait until Monday before doing anything. PNC is not our bank!!" ~ Michelle Benetua, Director of Strategic Partnerships and Programs, Seattle Parks Foundation.

Urban League

December 9, 2021: The first fraudulent ACH payment is sent to the fraudulent Citibank account.

January 31, 2022: Urban League notifies the Port that Citibank was not their bank and that Urban League had recently had a similar issue (someone impersonating an Urban League employee via email).

If this communication had not occurred, the fraud would likely have continued.

Recommendations:

We recommend implementing general detective controls based on best practices, to detect abnormalities with banking/ACH information changes. These might include:

1. Sending a confirmation notification of any changes to the supplier. This would include banking changes and address changes; if an address changes, it should go to both the old and new addresses.
2. Implementing a management review/sign-off of paperwork/validations for all banking/ACH information changes, utilizing a system generated exception report, to determine if they have met expectations.
3. Monitoring daily ACH payment activity details for abnormalities and timely corrective action, using a fraud focus.

Management Response/Action Plan:

Recommendations: We agree, with clarification as provided below.

Although a primary focus continues to be enhancements to strengthen preventative controls, we acknowledge benefits to implementing effective detective controls as well. We look forward to working with Internal Audit to explore any such measures that would offer a reliable protocol to detect fraud. We explored sending a system generated notification triggered by any changes made to the Supplier company. While this is possible to do, this potential detective control relies on Suppliers to be diligent to read their email and, most importantly, reply back to the Port. Bank account pre-noting which auto-generates and sends an email notification to Suppliers is also dependent on replies back to serve as effective detective controls.

DUE DATE: Under review, 4/30/2022 (Decision)

An exception report has been implemented to enhance visibility and management oversight. A central SharePoint library is used to store the documented efforts involving the administration and independent validation of requested additions or changes to Supplier banking information.

DUE DATE: Completed

Daily review of bank statement activity, investigating and resolving ACH returns, and pre-review of ACH payments pending release will continue, to assure timely attention for corrective action along with an enhanced fraud focus.

DUE DATE: Completed

5) Rating: Medium

The methodology to assure that vulnerable employees received required training was not functioning effectively. Our review of training records indicated that, of the seven Port employees who either directly or indirectly received the fraudulent emails, only two had completed the Port's mandatory Information Security Awareness training in 2021. Additionally, Port-wide, only 51 percent or 1,036 of the 2,041 employees had completed the annual training.

Training is one element an organization can implement to raise awareness of fraud and the various ways fraud schemes occur. In 2021, the Port required all employees to complete security awareness training. Every employee initially received the training upon hire, thereafter employees were required to complete an annual refresher training. We requested a report from Human Resources (HR) of the Port employees who completed the security awareness training (*ICT Information Security Awareness Learning Needs*) in 2021 and determined that 1,036 employees completed the training. Another HR report listed 2,041 active employees as of 12/31/2021. Therefore, slightly more than half the Port employees received the training in 2021. Below are the descriptions of some of the topics covered:

General Phishing: Explains the differences between spam, phishing, and spear phishing; what you can do to minimize the risk of a phishing attack; and how to identify indicators of a phishing email.

Spear Phishing: Covers why spear phishing poses a threat to the Port, the three types of spear phishing emails, and the indicators of a spear phishing email.

Business Email Compromise (BEC) Scams: BEC Scams covers topics on identifying BEC scams, differentiating between the three main types of BEC scams, and reporting a suspected attack.

Insider Threats: Covers topics on the danger insider threats pose, the three types of insider threats, and what to do if you observe suspicious activity.

The first set of emails received from the fraudster contained poor grammar, possessed a sense of urgency (offered a five percent discount if paid that week), included two unexpected requests to change bank account detail, was received from a slightly modified email than usual (font changed) and copied a co-worker where the email address was misspelled (Michelle@Seattle**Praks**Foundation.org – this was actually a domain created by the fraudster to imitate the real email address). These are all elements of a phishing email and may have been identified by Port staff if training had been completed. The second set of emails exhibited similar characteristics as the first but were harder to spot because of the upper case "I" used in "UrbanIeague.com", but also included a poorly written bank letter (See Appendix B), a sense of urgency, and grammar errors.

Recommendations:

We recommend that all Port employees (and contractors) that are involved in the process of creating, modifying, or requesting changes to supplier banking information, receive additional focused training on cybersecurity and the risks related to Business Email Compromise scams twice per year. If training is not taken, we recommend that user access be disabled until completed.

We also recommend that all employees (and contractors) that use a Port computer or have a Port email account, be required to complete the existing Security Awareness Training and we recommend developing a system to assure individuals complete such training by the due date.

Management Response/Action Plan:

Recommendations: We agree.

After technical issues with the updated Learning Management System (LMS) tool at the Port of Seattle are resolved through the Human Resources (HR) Department, we expect to see a more accurate listing of individuals who have received annual awareness refresher training. In addition, the Port has recently

invested in a more robust cyber awareness training solution through the Information Security Department aimed at user behavior patterns which concentrates training in the areas most needed. The Information Security Department is also currently developing an internal process to monitor and track awareness training based on data from the new training platform.

DUE DATE: In-progress, 6/30/2022

Since this incident, Information Security has conducted advanced training for all teams in the Accounting & Financial Reporting (AFR) Department at their request, which was focused on Business Email Compromises. Similar training is scheduled for all teams in the Central Procurement Office (CPO) including CPO-Purchasing, CPO-Construction, and CPO-Service Agreements.

DUE DATE: Completed & Ongoing training throughout the year

Information Security will continue to offer its monthly cyber awareness seminars, routine messaging, and special learning events to ensure a Port-wide content awareness campaign. This is in addition to the department's Port intra-net site hosted resources aimed at broadly educating Port staff. Information Security will continue to conduct Phishing exercises, including one recently conducted among 2,244 Port email recipients which has broadened awareness throughout the organization.

DUE DATE: Completed & Ongoing training throughout the year

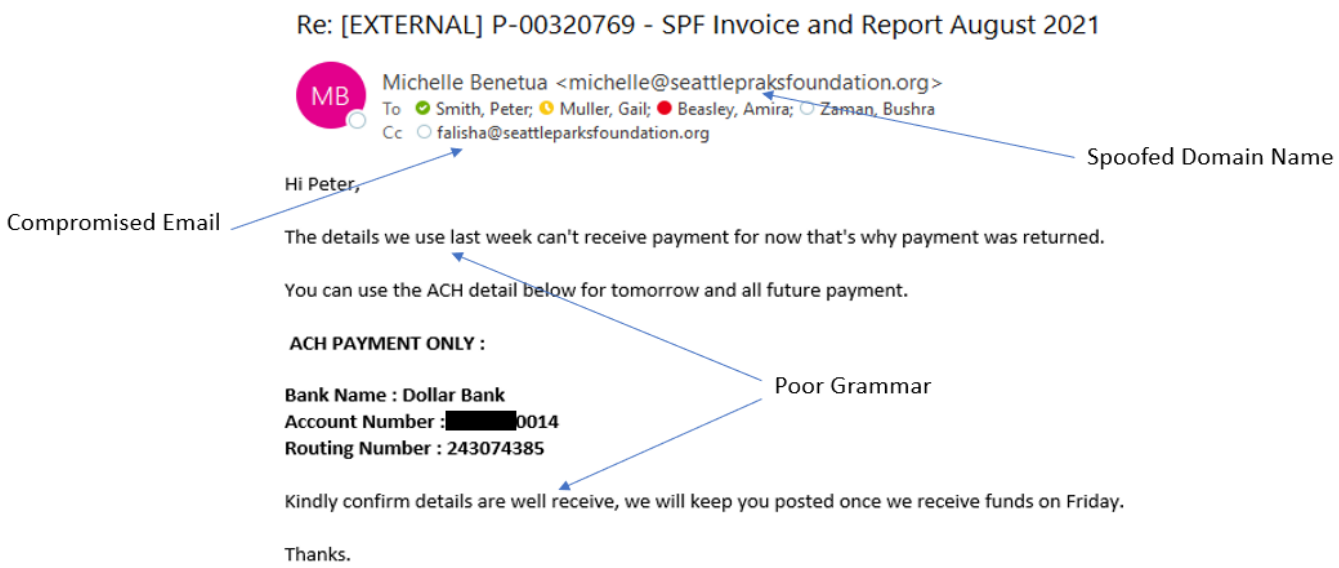
Appendix A: Risk Ratings

Findings identified during the audit are assigned a risk rating, as outlined in the table below. Only one of the criteria needs to be met for a finding to be rated High, Medium, or Low. Findings rated Low will be evaluated and may or may not be reflected in the final report.

Rating	Financial Stewardship	Internal Controls	Compliance	Public	Commission/ Management
High	Significant	Missing or not followed	Non-compliance with Laws, Port Policies, Contracts	High probability for external audit issues and / or negative public perception	Requires immediate attention
Medium	Moderate	Partial controls Not functioning effectively	Partial compliance with Laws, Port Policies Contracts	Potential for external audit issues and / or negative public perception	Requires attention
Low	Minimal	Functioning as intended but could be enhanced to improve efficiency	Mostly complies with Laws, Port Policies, Contracts	Low probability for external audit issues and/or negative public perception	Does not require immediate attention

Appendix B: Fraud Examples

Email using "Michelle@Seattle**Praks**Foundation.org"



Fraudulent bank letter: