The Fresno County Civil Grand Jury

2023 - 2024

GONE PHISHING:

HOW THE CITY OF FRESNO FELL VICTIM

TO A $613,737 SCAM

Phishing: Malicious emails cyber criminals send hoping to gain access to money or to important data and systems.

source: www.fresno.gov/informationservices/cybersecurity-tips/

Summary

This report investigated and assessed the internal controls and management practices of the City of Fresno (City) Finance Department and made recommendations for improvement. This investigation was prompted by a “phishing scam” that occurred in 2020 and resulted in a loss of over $600,000 to the City. Over the past four years, little information has been released to the public. An independent CPA firm, Price Paige & Company, was contracted to evaluate the City’s Finance Department effectiveness of internal controls. Their “Report on Internal Control - Accounts Payable and Disbursements” was issued on November 16, 2023. However, it did not directly address many of the concerns raised in this report.

To determine if recommendations are needed, it was necessary to 1) examine the Finance Department’s internal controls and practices in place at the time of the “phishing scam”, 2) determine how existing internal controls at the time failed to prevent the loss, 3) review how internal controls and policies have been changed/improved since that time, and 4) assess the probability of similar losses in the future.

Methodology

The relevant and material facts cited in this report were collected during Grand Jury interviews of both current and former City employees. These interviews, along with the Jury’s examination of City records and documents, agreed with the facts being reported. The jury also interviewed a representative of the CPA firm contracted by the City to

evaluate the Finance Department's internal controls. This evaluation included assessing the reliability of financial reporting, the safeguarding of City assets, and compliance with current laws and regulations.

The "Phishing" Scam

In 2020, the City was the victim of a brazen fraud that resulted in a loss of $613,737. If established city policy had been followed, this loss would not have occurred. Instead, policies designed specifically to guard against this kind of fraud were not followed which made it possible for two large payments, made over the course of several months, to be sent to a false bank account.

In December 2018, the Fresno City Council approved a contract for the construction of a new police substation in southeast Fresno (note: the total cost of the project and the name of the contractor doing the work is a public record). Construction began in April 2019. The contractor had requested that installment payments be made by physical checks. On January 6, 2020, the City Finance Department received an email from a perpetrator who identified as an "accounting specialist" for the construction company. The perpetrator requested a change to the installment payments method. Instead of physical checks, the construction company was now asking to receive payments via an Automated Clearing House (ACH) fund transfer (note: according to city staff**,** a vendor requesting a change of payment method from check to ACH is not common). The Finance Department, assuming the perpetrator was an actual construction company employee, emailed an ACH form to the perpetrator who promptly completed and returned the form by email. The fraudulent emails appeared to come from the legitimate contractor, but they did not.

Investigative Notes: the jury observed the domain extension of the fraudulent email addresses ended in ".us." However, the legitimate contractor's email address ended in ".com." Even though an early response by the City to one of these fraudulent email addresses was returned as "undeliverable", the fraud was not detected. The jury also observed that, during the multiple attempts to deceive City staff, the perpetrators gave multiple bank account numbers located in different states. This, too, did not alert city staff to the fraud.

On January 30, 2020, the Finance Department authorized an electronic fund transfer (EFT) of $324,473 to be sent to the new account they believed belonged to the legitimate contractor. Five weeks later, on March 5, the Finance Department authorized an additional $289,264 EFT payment bringing the total of fraudulent payments to $613,737.

Upon learning of the fraud, City officials made unsuccessful attempts to recover the fraudulent payments. The City conducted an internal investigation and determined that there was no evidence of criminal actions committed by City employees. During this time, COVID 19 policies were in effect and management of this incident was difficult. When City Finance Department staff alerted the Fresno Police Department of the fraud, a criminal investigation was promptly initiated. The FBI became involved when it was suspected that the perpetrators may be from out-of-state. It was later learned that the perpetrators belonged to an international organized crime ring. Other municipal governments throughout the nation were also defrauded in a similar manner.

At no time did the perpetrators submit fraudulent invoices. Based on a review of documents and interviews, it appears they simply scoured the internet for large construction contracts being awarded by local governments. Using real data gleaned from the City Council agendas and minutes, they were able to identify this particular contract, used what information was publicly available, and initiated a successful phishing scheme on unsuspecting city employees.

Glossary

ACH	Automated Clearing House. Allows electronic money transfers between banks. A type of EFT (electronic funds transfer). An ACH requires additional steps in the verification process and transfers funds more securely.
A/P	Accounts Payable. Refers to the business department or division that is responsible for making payments owed by the agency to suppliers and other creditors
CPA	Certified Public Accountant. A licensed accounting professional.
EFT	Electronic Funds Transfer. A way to move money across an online network, between banks and people. EFT payments are frequently used in place of paper-based payment methods, like checks and cash.
Prenote (Prenotification)	A zero-dollar test to verify the accuracy of bank account information (routing number, account number, and account type).

Investigation

Internal Control Policies In Place at the Time of the Scam.

At the time of the incident, the City's Finance Department had relevant internal control policies/practices in place. Some policies were not formally written and were communicated to staff through an informal and undocumented training process. Ultimately, the policies (both written and unwritten), if followed, would have prevented this loss from occurring. For example:

A Any time an established city vendor requested the City start making payment via electronic funds transfer (EFT) or a new bank account number is used, the Finance Department will first authenticate that the Automated Clearing House (ACH) form submitted by the vendor is actually from the vendor of record. Next, a zero-dollar pre-notification is sent by the Finance Department to the recipient bank to verify the bank information matches the information inputted into the City's financial system. A successful "prenote" would confirm that the new bank routing and account numbers match.

B At the close of the business day, procedure requires a different staff member to review all "large disbursements" to confirm/verify payment details. When a vendor was being paid via a new method or account number, the successful processing of a "prenote" would also be confirmed.

Failure of the Existing Internal Controls

The Finance Department's two relevant "policies" described above failed for the most basic of reasons: the authentication of the ACH form did not happen, and the end of day large disbursements confirmation procedure was not performed.

The ACH Authentication Did Not Happen

An initial prenote was attempted but failed (indicating that the account number being used did not belong to the legitimate vendor). In light of the initial pre-note failure, Department policy required a second pre-note attempt. However, contrary to policy, no second attempt was made, and the bank account information was not verified. Notably, in an attempt to process a successful pre-note, the perpetrators had utilized multiple bank account numbers located in different states. Unfortunately, these multiple accounts did not create a sense of suspicion on the part of city staff.

The Final Safeguard: The End of Day Check Register Review Was Not Implemented.

The routine “end of day” check register review procedure, intended as a safeguard inspection of larger payments, would have revealed that the required prenote process had not been executed successfully. This discovery would have stopped this payment and any future payments from being sent. The procedure was not implemented.

Review of Finance Department Policy Regarding Electronic Payment Procedures

The Finance Department Electronic Funds Transfers procedure was largely unwritten at the time of the incident. The primary goal of the policy is to ensure EFTs are initiated, executed, and approved securely based on a legitimate ACH form. The jury noted the City’s preferred method of payment to vendors is EFT. When new vendors are entered into the City’s financial system, and no EFT is requested, they are set up to receive a paper check by default. In this case, the legitimate contractor had specifically requested payment via paper check.

Training for the handling of these important money transfers was conducted verbally, and it appears that not all Finance Department employees were properly trained.

The Finance Department placed no dollar limits or enhanced accounting controls when ACH changes were recently made. The unwritten procedures (in effect at the time of the scam) specified the authority needed to approve payment change requests, required the use of a prenote to verify new account information, required that two staff members were needed to make payment method changes, and that staff contact the vendor by telephone to confirm that their payment method change request is legitimate.

The Grand Jury noted from multiple interviews that It is not common for vendors to request payment changes from physical check to EFT. As noted previously, suspicions should have been raised when the perpetrators asked for multiple ACH forms for different bank accounts located in different states.

The City's Response to the Incident

According to witness interviews, the incident resulted in serious reflection and introspection within the Finance Department. Awareness of the potential for future fraud has been significantly heightened.

In response to the phishing scam, the Finance Department adopted another critical step in its authentication policy. City staff will continue to contact vendors by phone to verify all ACH change requests, but now they must only use the telephone number already on file in

the City's data system (entered at the time of the Vendor contracting). Employees are now expressly forbidden to rely on the phone number provided on the ACH request form.

An independent CPA firm was contracted to evaluate the City's Finance Department effectiveness of internal controls, the reliability of financial data, safeguarding of assets, and compliance with laws and regulations. At the time of this report, the CPA's recommendations for improvements were being considered by the city. The Grand Jury concurs that the Finance Departments internally updated procedures appear appropriate for preventing this type of fraud from occurring again if they are competently implemented by city staff.

The Probability of Similar Losses in the Future

The addition of the new internal control procedure (contacting vendors by telephone using only the phone number already on file) is an improvement. However, this additional safeguard can/will fail for the same reasons as in 2020: internal control policies must be followed by department staff. Without strict observation and enforcement of new and existing internal controls, there is a high probability of similar losses in the future.

Despite multiple ACH/EFT forms, multiple bank account numbers in different states, and different email address domain endings, conspicuous red flags within the Finance Department were apparently not noticed. Ultimately, an increase in vigilance and a recognition that the City of Fresno is engaged in an ongoing cybersecurity arms race with sophisticated criminals will be key to their success. Future attacks will most likely involve the use of AI (Artificial Intelligence) and voice recognition software.

More importantly, the Grand Jury believes most errors and mistakes happen because the employees work in complex systems with a myriad of rules and procedures. Human error is the starting point of an investigation but rarely its conclusion. Therefore, the Jury encourages the City to develop human error prevention and reduction strategies to protect themselves from falling victim to fraudulent activities (see Recommendations).

The Grand Jury is satisfied the current Finance Department staff is dedicated to fulfilling its mission "*to ensure the city's financial integrity . . . and to guide fiscal policy and advocate for sound business processes"* (www.fresno.gov/finance).

Findings

California Penal Code §933(a) mandates that a grand jury report issue findings and recommendations.

F1 The Finance Department did not identify, or appropriately act upon, indications of fraud in this specific phishing attack.

F2 The Finance Department policies, if correctly followed, would have prevented this fraud from occurring.

F3 Upon learning of the fraud, City officials immediately began to ascertain the magnitude of the loss, the reasons why the loss occurred, and the steps to ensure a fraud of this nature would not occur again.

F4 Today, the Finance Department staff appears to be following policy and exhibiting sound business practices.

Recommendations

R1 By December 31, 2024, the Fresno City Council should adopt a written city-wide policy specific to indicators of fraud similar to the *Department of Defense, Inspector General's* website (Fraud Detection Resources (dodig.mil)).

R2 By December 31, 2024, the Fresno City Council should ensure only the vendor provided data contained in approved contract documents is utilized when engaging in any financial transaction.

R3 By December 31, 2024, the Fresno City Council should ensure changes to a vendor's bank account are verified and reviewed by multiple staff members.

R4 By December 31,2024, the Fresno City Council should adopt a city-wide written procedure for changing ACH payments including dollar limits and appropriate accounting controls.

R5 By December 31, 2024, the Fresno City Council should ensure that changes to an existing vendor payment method (i.e., physical check to electronic fund transfers) is approved by the Director of Finance.

R6 By December 31, 2024, the Fresno City Council should ensure that only the Director of Finance is authorized to bypass the prenote process.

R7 By March 1, 2025, the Fresno City Council should develop a single, current, authoritative source of Finance Department written policies (including those listed in R1 - R6) for which its employees are held responsible.

R8 By March 1, 2025, the Fresno City Council should enjoin the Finance Department, to the extent possible, to avoid relying on "understood" or verbal policies.

R9 By March 1, 2025, the Fresno City Council should contract with an outside firm to conduct penetration “phishing” tests that identify vulnerabilities in the system.

R10 By March 1, 2025, the Fresno City Council should direct the city manager to provide a written report to the council addressing all the recommendations made in the independent CPA’s “Report on Internal Control - Accounts Payable and Disbursements” (issued on 11/16/2023).

R11 By June 30, 2025, the Fresno City Council should ensure all city-wide finance/fiscal affair managers and supervisors attend annual human error prevention and reduction strategy training.

Required Responses

The following responses are required pursuant to Penal Code Sections 933 and 933.05 from the following governing body within 90 days:

- The Fresno City Council (F1-F4, R1-R11)

Invited Responses

The following responses are invited pursuant to Penal Code Sections 933(a) and 933.05 from the following elected official within 60 days:

- The Mayor of Fresno (F1-F4, R1-R11)

Disclaimer

Reports issued by the Civil Grand Jury do not identify individuals interviewed. Penal Code Section 929 requires that reports of the Grand Jury not contain the name of any person or facts leading to the identity of any person who provides information to the Civil Grand Jury.