Collier County Clerk of Courts
Office of Inspector General

Investigative Report 2021.06
Fraud Scheme Using Clerk's Bank Information

Inspector General Insights

Background: The Collier County Clerk's Administration Office requested assistance from the Office of the Inspector General (OIG) to conduct a preliminary review and additional examination concerning a phone call that the Clerk's Customer Service Desk received. The complainant claimed she was a victim of a fraud scheme after she applied for a home-based data entry position with a company named Blu Logistics Warehouse.

The complainant alleged an unknown suspect, claiming to be a representative from the Blue Logistics Warehouse, sent her a copy of a check via email with instructions to deposit the check so she could use the funds to purchase a work computer. She stated the check displayed information indicating it was issued by "*Dwight E. Brock, CLERK OF THE CIRCUIT COURT COLLIER COUNTY Brock, FLORIDA*," in the amount of $1,500.00. She further stated the fraudulent check was issued to her name at her home address in Texas, and it included a bank routing number, account number and corresponding check number.

The complainant stated that the unknown suspect asked for her credit card username and password, stating it was required before the unknown suspect could disburse the funds. After the unknown suspect insisted on obtaining her credit card information, the complainant became suspicious and refused to release her personal information, nor did she deposit the check. The complainant then contacted the Clerk's Office and reported the incident.

Objective: Our review was to determine the facts of the case, and to ascertain whether the Clerk's bank account had been compromised. We suspected this could be a fraud scheme, which may require referral to Law Enforcement.

Observations: An OIG initial inquiry and review of the bank routing number, account number and related check number revealed these numbers matched exactly the numbers of a legitimate check the Clerk's Office issued to a Naples resident in 2018.

The OIG conducted a phone interview with the complainant who confirmed on January 9, 2021, she submitted a job application for a data entry position with Blu Logistics Warehouse. The complainant explained that she found the job announcement posted on the Facebook Jobs board. She stated on the same date (January 9th) the unknown suspect sent her a message via the Facebook "Messenger" application, stating he was going to refer her application to the company's Human Resource office.

The complainant explained that on Saturday, March 20, 2021, approximately 71 days after she submitted the application, she received a Facebook message from the unknown suspect with additional information about the position. On the Facebook messages, the unknown suspect told her he was going to direct her to the online job interview, and he asked her to get the Google "Hangouts" application, a cross-platform messaging app developed by Google that allows conversations between two or more users. The complainant indicated she then completed an online interview via Google Hangouts on the same date (March 20th) with a second suspect who identified herself "Juliet Lawrence" (Suspect #2).

The complainant added that after she completed the online interview, Suspect #2 told her she was hired and asked her to provide her credit card limit, account name, username, and password in order to proceed with ordering her work computer and equipment. The complainant explained that when she refused to provide her credit card information, Suspect #2 told her the company was going to work on another method of payment for the purchase of her work computer.

The complainant then stated on Monday March 22, 2021, she received an email from manoisjessy@gmail.com titled FRONT AND BACK CHECK (all capital letters), which included a set of instructions on how to deposit the check, and a copy of the back side of an electronic check. The email also included an attachment that included the front side of the electronic check as a pdf format entitled "opemy.gee check.pdf." The complainant explained the check was issued in her name and home address in the amount of $1,500.00. She believed the information written on the check looked suspicious, and the check looked fake.

The complainant explained Suspect # 2 contacted her via the Google "Hangouts" application, and instructed her to print the check, to cut and trim it to its exact size, and to endorse and deposit it by using her personal bank account mobile application. Suspect # 2 also requested that the complainant send a screen shot of her bank deposit confirmation.

The complainant stated she felt uncomfortable following Suspect #2's instructions because she believed the check was fake. The complainant stated she did not deposit the check. Thereafter, Suspect #2 sent her multiple messages via Google "Hangouts", asking for the check deposit confirmation.

The complainant added that Suspect #1 also contacted her via the Facebook messaging board, asking for the check deposit information. The complainant stated that Suspect #1 also made threats of legal action against her for failure to provide the deposit information.

When questioned if the complainant incurred a financial loss during the attempted fraud scheme, the complainant confirmed she did not incur a financial loss. She also stated that she believed her personal information was not compromised. She explained that after she researched the Clerk's Office contact information and realized it did not match the Clerks' information on the check, she contacted the Clerk's Customer Service Desk and reported the incident.

Conclusion: Based on the review of the documentation and information from the complainant's phone interview, the OIG made the determination to refer the case to law enforcement on March 25, 2021 for possible criminal/prosecutorial consideration or any other action they deemed appropriate. The Federal Bureau of Investigations was contacted, yet they did not open an investigation as there was no loss to the complainant.

The OIG subsequently prepared a confidential report for the Clerk's Finance department, to potentially reduce exposure of the Clerk's banking information to outside parties.

Total # Transactions	Amounts Audited or Reviewed	Questioned Costs	Taxpayer Savings	Description
1	$1,500.00	$1,500.00	N/A	Fraudulent check issued with the Clerk's bank information