EyeWatch NEWS

March 2022

Eyewatch News provides a snapshot of suspicious activity that has occurred at the Bank within the last month. All potential suspicious activity is investigated to determine what type of action may need to take place on an account or with a customer.

Category	Activity
Check Fraud	A customer presented a large dollar check for deposit that was received in the mail. The check was missing the MICR line and provided no information on who the check was drawn off of. The customer was unsure why the check was received in the mail.
Check Fraud	A new account was established for a new customer to the Bank. A few days after the account was opened, a check was deposited to the account. The check provided red flags, including a memo line of “payment approved”. The check was returned by the paying bank and deemed fraudulent. In discussion with the customer, he answered a job add related to his farm operations. Not all details were provided on how the customer made contact with the individual.
Vishing	A customer contacted the Bank after receiving a phone call from the Amazon customer service number. The number ended up being a vishing attempt. The caller had the customer log into Internet Banking and also send himself funds via the Cash App. The customer was also asked to apply for a Cash App credit card and provide the credit card number to the individual. The credit card number was not provided. The customer was able to retract the funds sent via Cash App as well.
Elder Financial Exploitation	During the account opening process, a customer mentioned red flags associated with past account abuse by a family member utilizing funds without permission.

Category	Activity
Check Fraud	A check was submitted for deposit via mobile deposit. The check image was a picture of a check on a computer screen. In discussion with the customer, it appeared to be part of a Facebook scam. The customer was to use a portion of the funds to send to a non-profit organization. The fraudster initially wanted the customer's Internet Banking login credentials, but since the customer would not provide them, the fraudster emailed the customer the check to deposit.
Online Loan Scam	A customer with previous fraudulent activity inquired on getting Internet Banking access for a "loan company" to view a list of account transactions before approving a loan. The "loan company" was going to send the customer a link for them to upload their login credentials. The request was denied for Internet Banking access.
Tech Support Scam	A customer visited the Bank after falling for a scam. The customer's computer had froze, so the customer reached out to a repair company for assistance. The "repair company" began asking the customer uncomfortable questions but promised they could fix the computer. The "repair company" had the customer log into Internet Banking and provide her debit card number. Five attempts to purchase Target gift cards were noted on the customer's debit card. No attempts were successful.
Check Kiting	It was noted on an existing customer's account, funds were being deposited into the account as other checks from another financial institution were debiting the account. In review of the account, red flags were presented for check kiting. With further discussion with the customer, it was determined the customer was trying to float funds to pay bills debiting the other account.
Check Fraud	A check was submitted for deposit via mobile deposit. The customer does not typically use the product to deposit checks. In discussion with the customer, a potential business customer had sent the check for prepayment of services. The potential business customer asked for the customer to send a portion of the funds back for overpayment. The check was not negotiated.

Category	Activity
Check Fraud	A new account was opened for a new customer to the Bank. At account opening, the customer mentioned their daughter would be depositing funds into the account. After the customer left the branch, the customer called in to receive wire instructions as a relative was going to be sending funds to help with bills. No wire was received on the account, however, two weeks after account opening, the customer deposited a check for $9500 from an individual in Arkansas. Once the funds were made available, the customer purchased a cashier's check to an individual. The customer claimed to be paying for work the individual had done for her. Due to suspicion, a follow-up call was made to the customer for further questions. The customer then stated the funds were being sent to her stepson because his father passed away. With the multiple changes in stories and red flags, the account was closed to mitigate future risk.
Identity Theft	A new account was opened via NuFund, the Bank's online deposit account opening program. Red flags were presented regarding the name format in the application, communication methods by the applicant, and verification of information. Shortly after the account was opened, the FAD report demonstrated various IP addresses accessing the Internet Banking profile. In the process of closing the account, the opening ACH deposit was also returned by the paying bank as not authorized. The account opening was deemed to be a fraudulent account.
Check Fraud	A check was submitted via mobile deposit on behalf of a customer. The customer had received a pre-approval email from an online loan company. The customer then clicked on the link and entered his personal information to apply for the loan. The link took the customer to a lender's website that appeared legitimate at the time. The customer provided the lender with his Internet Banking login credentials for the check to be deposited. The check was not negotiated.

Category	Activity
Marijuana-Limited	Six new relationships were established for marijuana-related businesses. No suspicious activity has been identified.