SECURITY OFFICER'S ANNUAL REPORT

Report date: January 20, 2021
Presented by: Susan R Shaffer, QCBT VP BSA & Security Officer

To identify transaction fraud, the Bank uses a combination of customer behavior monitoring (as observed during the course of normal business) and an automated system called Verafin to assist us in identifying transactions which would be unusual or outside of expected activity as compared to a customer's previous habits. Our Security Officer also participates in community banker forums where information can be shared by and with other banks about various types of fraud trends experienced by others in market.

Through these efforts, we have been informed of, experienced, or prevented fraudulent activity such as what is described below in 2020:

- **Malware and Botnets,** a form of Social Engineering, grows as fraudsters impersonate security specialists, customer support workers, and others. Attackers using social engineering have found the phone and email channels to be the weakest link for corporations and consumers. This trend will continue in 2020 as fraud schemes become more and more creative. Hackers impersonating customer support people, IRS agents, and even security specialists claiming to have detected fraud will continue to be a source of stealing personal financial data.

- **Debit card fraud/Credit card fraud** is a wide-ranging term for theft and fraud committed using a credit/debit card or any similar payment mechanism as a fraudulent source of funds in a transaction. The purpose may be to obtain goods without paying, or to obtain unauthorized funds from an account.

    - **Data Breach** - In the credit/debit card industry, data breaches occur when hackers snatch credit/debit card information that could be used to commit fraud or identity theft. Increasingly, data breaches occur at computing choke points through which many thousands of pieces of financial data must pass.

    - **In–Person Fraud** – Credit/Debit card fraud can be committed in-person by a thief who steals your card and uses it to make purchases at various merchants.

    - **ATM Fraud** - If a thief has managed to get your PIN, he can use your credit/debit card at any automatic teller machine (ATM) to withdraw money from your bank account. He will also be able to access any line of credit that might be attached to the account.

    - **Online Fraud** - A thief can commit credit/debit card fraud online without even having your card in their possession. According to the Corporate Travel Safety website, all they need is the card number and expiration date, and they can use it to make purchases until they drain your account and tap out any attached credit line or overdraft protection. They can enter your address for the purchase and supply a different "ship to" address. They may also sell the credit/debit card to other criminals who will use it until they have tapped it out or until you report it stolen and your account is frozen.

    - **Identity Fraud** - A thief may use your credit/debit card to steal your identity. If he or she has other information about you, or has stolen your purse or wallet and have other forms of identification such as your driver's license or Social Security card, they may combine those with the credit/debit card to "prove" that he or she is you.

SECURITY OFFICER'S ANNUAL REPORT

QUAD CITY BANK & TRUST

- **ATM skimming.** The perpetrator puts a device over the card slot of an ATM (automated teller machine), which reads the magnetic strip as the user unknowingly passes their card through it. These devices are often used in conjunction with a pinhole camera to read the user's PIN at the same time. These have recently been discovered on ATMs in the Quad Cities and continues to happen around the Chicago/Des Moines areas.

- **ACH fraud** – Infecting computers used to perform transfers with spyware often installed via social engineering techniques or by exploiting vulnerabilities in out-of-date software. The money goes to so-called 'mules" or people who have agreed to receive the funds and then further transfer it to the fraudsters.

- **Fraudulent cashier's checks** – Come in a variety of different scams. The most common are for Nigerian/similar check scams, foreign lotteries, fraudulent scams regarding alleged inherited money, or through payment for items sold on auction sites such as Craigslist. Generally, these scams entail a large check with instructions to keep a portion of the funds and wire the remainder, or send cash back. With Craigslist, people will send a cashier's check for more than what the purchase is and then request a wire for the difference.

- **Check fraud and forgery** – This may involve stolen checks, forged signatures or check alterations.

- **Identity theft** – Lost or stolen wallets, checkbooks or credit cards continue to be the primary source of personal information theft.

- **Elderly Financial Exploitation** – Occurs when a person misuses or takes the assets of a vulnerable adult for his/her own personal benefit. This frequently occurs without the explicit knowledge or consent of a senior or disabled adult, depriving him/her of vital financial resources for his/her personal needs.

- **The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) Fraud -**
    - Small Business Administration (SBA) Programs Fraud – Identity theft and falsifying documents.
        - **Grants** - Grant fraud typically occurs when award recipients attempt to deceive the government about their spending of award money.
        - **Loans** – Loan fraud occurs when a person or business knowingly makes a false, material statement to a financial institution or federal agency in order to mislead the lender into making a loan.
        - **Stimulus Payments** – sent to taxpaying consumers by a government. Stimulus checks are given to boost the economy by providing consumers with funds to spend.
        - **Unemployment State fraud** – knowingly collect benefits based on false or inaccurate information that you intentionally provided when you filed your claim. Identity theft, people claiming unemployment under your name.