As your financial partner, we want to make you aware of some recent fraud trends we have experienced in our local market. To have fraud occur on your business account, or any account, can be both alarming and aggravating. The purpose of this letter is to provide information that can help you protect your account(s).

Current Fraud Trends

Mailbox Thefts

What happens?
You send a payment to your vendor via mail, but a few weeks pass, and the vendor calls you to say the check hasn't shown up. Although this seems strange, you simply re-issue the check to the vendor and move on. You may or may not have placed a stop payment on the original check. A few weeks pass and, during reconciliation, you notice that a few checks have cleared your account that you don't recognize.

What is the result?
You contact FSB with your concerns and learn that your account has been compromised and counterfeit checks have been produced and cashed. At the point of notification, FSB places your account on hold, meaning all transactions are manually reviewed and have to be approved by you. While this review is happening, a decision must be made: do you close the account you have had for so long and start a new one, or add fraud mitigation services to your arsenal?

How can you help to prevent this?
Take all of your mail either to a secure outgoing mailbox, or drop it at the post office. While you can control your outgoing mail, you cannot control your vendor's mail receipt process. The persons committing this type of fraud typically come to the area a couple times each month and pull checks from mailboxes. We have seen this occur more frequently when our customer has mailed a check to the vendor, and the vendor's mailbox becomes compromised. Fraudsters can then either produce counterfeit checks right away, or defraud the accounts they picked up on a prior run through town.

To reduce the number of checks you write – and thus your exposure to this type of fraud – you can explore alternate payment methods with vendors, such as credit card or electronic payment with FSB's Treasury Management Officer, Shelley Schroeder. It's important that you practice diligence surrounding your outgoing mail and the receipt of your mail to help prevent check fraud from happening to your account.

Current Fraud Trends
Page Two

Ransom Ware

What happens?
You get to the office and turn on your computer but instead of the happy pictures that typically greet you on your desktop, you receive a cryptic message that says your files have been encrypted and you must pay $1,000 to retrieve the files.

What is the result?
Your company now has a decision to make. You can either pay the ransom for your files, or you can restore the files from your last backup, in hopes the backup was recent. Unfortunately, there is nothing FSB or the authorities can do to assist you with restoring your files.

How can you help to prevent this?
Ensure you have current anti-virus and anti-malware software on your computers. Additionally, don't allow your systems to become outdated and susceptible. You should have a plan in place in the event your systems become compromised so you and your employees know exactly what to do in such a circumstance. Unfortunately, once the attack has occurred, it's too late to make a plan.

Wire Fraud

Scenario #1: What happens?
A trusted employee receives an e-mail from what appears to be the CEO of your company. The message states that a wire needs to be sent out urgently to pay for goods or services and *"code to admin expenses"* is an instruction often used. The fraudsters that have infiltrated the company's systems wait for a day that is very busy with meetings or travel. The trusted employee, who was instructed in the email to "*process the wire right away*" dutifully forwards the e-mail to the bank to process the wire.

What is the result?
Whenever wire requests are submitted, FSB has procedures in place to call an account signer or an employee authorized for wires to verify the request. While our policy has prevented fraudulent wires from being sent, it cannot always stop it from happening. For example, in the above scenario, if the employee is authorized to submit wires, then it most likely would have been sent. Once a wire is sent from FSB it is nearly impossible to recover, which is why those committing fraud like to use wire transfers as a way to defraud accounts.

How can you help to prevent this?
Establish internal procedures for wire verification, or enact dual control for wire requests. Dual control functions where one person requests the wire, but another person must approve the wire upon the callback. Implementing dual control internally will generally enforce cross checking within your organization's walls.

Additionally, if you forward the received e-mail back to the supposed wire requester (CEO) and type in their e-mail address (instead of just hitting reply), you may catch an issue. While this is not fail-proof, it is a better option than clicking reply, since that action simply returns the email to the fraudster.

Scenario #2: What happens?
We have also begun to see fraudulent vendor payment requests via e-mail with wire instructions. This occurs where your system or, more commonly, your e-mail, has been hacked and fraudsters watch your activity. The fraudster figures out you purchased goods from a certain vendor. Then, the fraudster sends you an invoice with wiring instructions, and it appears to be from the vendor to whom you owe funds from previous legitimate purchases. You make the payment assuming the invoice is directly from the vendor.

What is the result?
30 days after the wire has been sent, you receive a call from your vendor's Accounts Payable department asking when they can expect to receive your payment. You then learn that the money you wired was sent to the fraudster and the funds are not recoverable. FSB's callback procedures would not have intercepted this type of fraud.

How can you help to prevent this?
Establish an internal procedure to have a verbal conversation confirming wiring instructions with any vendor who sends instructions via e-mail or an e-mail attachment. If you do receive an invoice with wire instructions via e-mail, call your vendor directly using the phone number you have on file – *not from the invoice* – to verify wire instructions and the attached invoice.

Debit Card or Credit Card Point-Of-Sale (POS) System Compromised

What happens?
You start hearing complaints from your regular customers that their debit or credit card has been compromised and they think it's because they used their card to pay for something from your store. You don't think too much about it until the comments continue from other customers. Then, a few days later you get a visit from the local authorities asking you questions regarding your Point-of-Sale system. After some research, you realize that malware has been unknowingly placed on your computer system. Every card swiped on your machine(s) over the past month has been captured and sent to a criminal in Russia. You also learn that the technician who provides your POS system support was hacked and his remote login credentials to your system were used to place the malware on your system.

What is the result?
The local news reports that your store has a security breach on your Point-Of-Sale system and anyone who used their card at your store in the past several weeks has been compromised. You now have upset customers and lose business from people not wanting to risk having their cards compromised.

How can you help to prevent this?
Make sure your POS software provider is on the certified QIR List. If they are not on the list, they probably don't understand the risks involved with your payment system. Never allow unlimited access to your computer system with the use of a remote access program like LogMeIn, RemotePC, pcAnywhere, and GoToMyPC. Forensic investigators have discovered that remote access is a top avenue fraudsters use to gain access into merchant systems in order to install custom-tailored POS malware. Ask your system technician about two-factor authentication for remote access to your system. Or, better yet, manually turn on the remote access when your technician requests it and turn it off when the work has been done.

Unfortunately, these are real cases that have occurred in our local area. I hope you have found this information to be useful in knowing how to protect your organization. If you have any questions, or would like more information, please reach out to FSB's Treasury Management Officer, Shelley Schroeder at 730-6866.

Warmest Regards,

Gene Neighbor
CEO and President