What you need to know to protect your Business Account

By Joan Woldt, EVP-Regional President, Bank First National

How many of you have dealt with the wasted time and energy of having to change your bank account due to a fraud issue? If you haven't yet, the chances are high that you will.

According to the American Bankers Association, Fraud against bank deposit accounts cost the industry an estimated $1.744 billion in losses in 2012. The amount has grown considerably since 2012. Debit card fraud accounted for more than half of 2012 losses (54 percent), followed by check fraud (37 percent). Online banking and electronic transactions such as wire and ACH accounted for the remaining 9 percent of losses.

- Survey respondents reported seeing an increase in social engineering and information gathering attempts by fraudsters using the phone channel.
- The leading check fraud categories were return deposited items, forgeries, and counterfeit checks.
- Banks' prevention measures stopped approximately $13 billion in fraudulent transactions in 2012.

Many small business owners mistakenly think that federal fraud regulations cover their business accounts in the same way that regulations protect personal accounts. However, federal regulations that protect financial accounts from fraud cover only personal accounts, leaving business accounts out in the cold when there's a cybersecurity breach. Ask your bank what their policy is for reimbursing business accounts when a fraudulent transactions occurs.

How the criminals do it:

Hackers will use social engineering and often target email accounts to get their victims' bank credentials. Small businesses often fall victim and are targets for these fraud schemes because larger corporations have tighter security in place to prevent these attacks. Criminals will often obtain an employee email address and create a new email account address slightly different than the actual employee's address. They will use that fake email address acting like the employee to obtain information and access to the system including asking employees to click on a link.

Criminals will often steal mail from one of your vendors. If you mailed them a check, they have all the numbers from your Bank and Bank account needed to create a new check and/or an ACH (automated clearing house) to generate a payment to take funds from your account. Many will test a smaller dollar amount to see if you have fraud protection, such as, Positive Pay or ACH blocks and filters. Ask your bank what fields on the check are actually reviewed by these services. Sometimes the criminals know that your Bank's service only covers check amount and check number. They can copy the amount and use that check number and change the payee, and these systems will not prevent it.

Many business owners rely on outdated security tools and strategies that are ineffective against cyberattacks in the first place. Staying on top of current events and being aware of threats in an ever-changing security landscape are the first steps to preventing bank fraud. You can protect your business from outside threats with the following methods:

Employee training. Hackers gain entry to your accounts using a variety of methods, including links in what appear to be routine emails from financial institutions or other companies with whom you routinely do business. Train your employees to report any email that looks suspicious.

Other training should include running scans on portable storage devices, like flash drives, before opening files, and limiting personal use of company business computers and devices.

Passwords. Treat passwords like underwear.
Change yours often/ don't share with friends or anyone/the longer the better/be mysterious, not obvious/don't leave yours lying around.

System integrity. Equip your computers and other system components with the most up-to-date firewalls and antivirus software. This means protecting smartphones, tablets and other mobile devices. Add to the protection level by executing daily backups of critical business data on every computer or server.

Two-step logins. To manage your bank account online, you generally need only your username and password. If those are compromised, anyone can get in. Set up two-step, out-of-band authentication, whereby a single-use code is sent to your phone or email for you to enter after you input your login credentials. Even if a cybercriminal intercepts that code, it will expire shortly after it's sent, and your account will remain protected.

Fraud Insurance. Check with your property and casualty company if they offer fraud protection insurance. Many will have an affordable deductible to protect you from the higher risk and losses that occur from bank account fraud.

Educate yourself on how your bank handles fraud situations so you are well informed and prepared if this happens to you. Understanding the policies, procedures and the approach that your bank has to business account fraud can make a very big difference in getting your business account back up and running smoothly and knowing if you have any liability or not.

Staying on top of the latest issues with bank fraud will help you ask better questions of your banker and be able to implement new protections to your accounts as the industry and world rapidly changes. Ask your banker, "What should I know that I haven't asked?"

Fraud insurance is an excellent way to limit your liability and reduce the impact to your bank. We have experienced firsthand the reduced impact to customers and the bank. Check with your insurance provider for the coverages and costs.

Be prepared, work hard, and hope for a little luck. (Quote from Ed Bradley).