FIRSTCORPORATE NEWSLETTER

First State Bank of Bloomington
www.fsbblm.com
serving the residents of McLean County since 1906

Issue 1

Business Identity Theft and Corporate Account Takeover

As a community bank, we are committed to our customers and the communities we serve because we understand the value and importance of local businesses. This is our first Corporate Newsletter created to help keep our business owners updated on relevant topics that may affect their business. We plan to publish several times throughout the year and we welcome your feedback on topics you would like to see in the newsletter. We truly appreciate your business and look forward to your feedback!

What is Corporate Account Takeover?

Corporate account takeover is the business equivalent of personal identity theft. Professional criminal organizations and hackers are targeting small and medium sized businesses to obtain access to their Internet Banking credentials. These hackers will then deplete deposit balances and lines of credit of the compromised bank accounts by redirecting the money overseas. A computer can be compromised easily by visiting an infected website or by simply opening an email. There is a huge increase in Identity Theft and the criminals are now targeting businesses instead of consumers due to the potential for larger bank balances. When it comes to protecting your financial information from hackers, knowledge is the best practice. As a business or business owner, you need a level of understanding about how to secure your computer to minimize threats. Below are some steps to assist you in protecting your information:

Steps to Take for Enhanced Security

- Review your banking transactions daily.
- Review your credit report regularly.
- Use a dedicated computer for all of your financial transactional activity. Do not use this computer for Internet web browsing and email.
- Have firewall software installed on your computer.
- Apply operating system updates regularly.
- Ensure your anti-virus software is updated with the current version.
- Use the latest version of Internet browsers, such as Internet Explorer, Google Chrome, Firefox and keep patches up to date on your computer.
- Activate a "pop-up" blocker on Internet browsers to prevent intrusions.
- Turn off your computer when not in use.

What are My Risks as a Business?

While consumer banking accounts are covered under Federal Reserve Regulation E, which requires banks to provide reimbursement for certain fraud losses, Regulation E does not apply to business accounts. Instead, business and commercial bank accounts are covered by the Uniform Commercial Code (UCC). Under the UCC, business account holders have significantly higher liability for fraud than consumer banking customers. This means much of the responsibility for protection of your business bank account from cyber-crime and other fraud rests squarely on you and your business. This responsibility, and liability, particularly extends to safeguarding against ACH and wire transfer fraud, check fraud, account takeover, and protecting your business' banking credentials.

cont. to page 2

What is First State Bank of Bloomington doing to help protect my information?

First State Bank of Bloomington is committed to providing you with a secure online experience that protects your confidential information. Our employees are trained on our security policies and procedures and work diligently to protect the integrity of your information.

We use industry-accepted security practices, including firewalls and encryption, to safeguard the security of your personal financial information. These controls allow us to properly authenticate your identity when you access our online services and help to protect your information as it travels over the Internet between your computer and the bank. We also constantly monitor and assess the security of our systems.

Secure Login

First State Bank of Bloomington employs a layered security approach to help protect your accounts and your identity. When you set up your account, you will be asked to provide personal security questions and answers to help authenticate your user ID and password. In addition, our security system will recognize your user patterns (when and how you access the online banking site) and use this information to verify your identity. Also, if you sign on to First State Bank of Bloomington Online Banking from a device that we do not recognize we will ask you to answer a Security Question for which only you know the answer.

The bank requires a difficult to guess password using a combination of upper and lower case letters, numbers, and special characters.

All Cash Management functions require an extra layer of security called Out of Band Authentication. Out of Band Authentication is the use of two separate networks working simultaneously to authenticate a user. This requires the person accessing the Cash Management module to receive a one-time unique pass code to the telephone number established within the module before access is granted to the Cash Management system.

continued to page 2

Automated Time Out

To provide additional protection, a time out feature is used on selected portions of our website. This feature will automatically log you off of your current online session after a period of inactivity. Re-establishing and authenticating your credentials for your online session helps to reduce unauthorized access to your accounts.

Use of Firewalls

To protect data stored on our systems and to prevent unauthorized access, we employ firewalls where appropriate. Firewalls are software and hardware products that are intended to define, control and limit the access to a website, network or computer system.

Third Party Verification

First State Bank of Bloomington works with independent third-party security firms to perform security reviews of our online services and systems. Systems are monitored and updated as needed to protect against known security risks. In addition to the third-party testing, our internal security personnel use several risk assessment and security tools to monitor and maintain the security of our online systems.

Encryption

Most web browsers have the ability to communicate securely with a website by encrypting the information as it passes across the Internet. This method of communication is called Secure Socket Layer (SSL). First State Bank of Bloomington requires the use of a browser which supports 128-bit SSL encryption to log in to the online banking website. If you see a website address that begins with "https" (as opposed to "http"), you are using an SSL connection to transfer your confidental information.

We take the safeguarding of your information seriously. In fact, we believe keeping your information safe and secure is every employee's responsibility. However, even the best security measures can only prevent fraud if you are also vigilant about employing the necessary safeguards to protect your information.

Our concern for the safety of your financial information goes beyond our banking relationship with you.

We're here to give you the latest tools and information that can help you safeguard your information!

Give us a call at 309-662-0411

What is Business Identity Theft?

Business identity theft is a broad term that encompasses a wide variety of crimes involving the unauthorized use of a business' identity.
Business identity theft is not an information security breach, or an incident involving the loss or theft of confidential consumer information that a business may possess.
Rather, **business identity theft involves the actual impersonation of the business itself.** It can occur through the theft or misuse of key business identifiers and credentials, manipulation or falsification of business filings and records, and other related criminal activities.

How to Protect Your Business from Identity Theft

Treat and protect your business EIN as you would your own Social Security number. There are many circumstances under which the business EIN must be provided, such as business bank accounts, tax and wage reporting, W-9 forms, etc. However, be aware that thieves can commit numerous business identity theft fraud schemes, tax fraud schemes and fraudulently access or open many types of business accounts with only your business name, address, and EIN. Just as you would protect your Social Security number, attempt to limit EIN disclosure to those circumstances under which disclosure is required. Be suspicious of unsolicited business credit applications, and verify the authenticity and return mailing address before you complete and return the form.

✓ *Keep all documents containing business information or business identifiers* in a safe, secure location not accessible by unauthorized persons

Be certain to protect and secure hardcopy documents that contain business identifiers, account numbers, and other sensitive information at all times. This includes employee workspaces, public access areas, waste and shred receptacles, filing cabinets, and any other locations where these documents may be found. Be cognizant of all persons that may be able to view or have access to these documents (authorized or not), including clients and customers, visitors, contractors, cleaning crew personnel, etc.

✓ Securely shred old or unnecessary documents that contain your *business information or business identifiers*

Shred any old or unnecessary documents containing business license numbers, business registrations, EIN / TIN, account numbers, etc. using a cross-cut, confetti cut, or diamond cut shredder, or utilize the services of a secure document destruction company. Any documents waiting to be shredded should be placed in a secure, locking receptacle or locked storage room not accessible to unauthorized persons.

✓ Regularly review your business registration information online (for all active and closed businesses)

You can go to the Secretary of State website and use the public "Business Entity Search" to enter your business name and review the information on file for your business. You should also periodically check any past businesses that you may have closed, to ensure that they have not been fraudulently reinstated.

✓ Be certain *to file your annual reports and renewals on time*

In addition to the risk of administrative dissolution of your company for failure to file, business identity thieves will often target companies that are classified as inactive, suspended, in default, etc. The thieves quite logically assume that, if a business doesn't keep up with its basic quarterly or annual business filings, the owners probably won't realize the information has been changed until it is far too late. Likewise, the apparent lack of attention to detail may mean that other forms of fraud may go unnoticed as well.