



AUBURN BANK

Member FDIC
www.auburnbank.com

CORPORATE ACCOUNT TAKEOVER & PAYMENTS FRAUD

WHAT IS HAPPENING NOW?

APRIL 2018

VERSION 4

SECURITY NOTICE 04/2018

- Please be aware that some malware (computer viruses) may attempt to capture your token number (this is the number that changes every 30 seconds). If you enter your token and receive a message that bank systems are down, please call Electronic Services at 334-821-9200 immediately to confirm if there is an issue.
- Other malware may ask you to input various information to allow the bank to update your records. Information may include your date of birth, SSN/EIN, etc. The system may then tell you to expect a phone call from the bank. The caller will ask for your token number. If you see a screen or receive a call requesting this information, do not provide it. Call Electronic Services at 334-821-9200 immediately.
- AuburnBank offers several security measures to help protect your funds. You can review this PDF that is linked on both the Wire and ACH screens within the AuburnBank Cash Management system. Antifraud layers that are successful are IP restrictions and dual control access for creating and initiating or transmitting ACH files and Wire Transfers. The IP restriction limits access to your accounts to certain locations. There is no additional charge from AuburnBank for these added security features. Please contact us if you would like more information.
- When you originate ACH you may receive a fax concerning suspicious transactions. Please provide a prompt response to these so we can help protect your accounts. To further assist in protecting our wire customers, we will call to confirm all Internet wires. If you send an Internet wire, and know you will be out of the office, please call the Wire Department at 334-821-9200 to confirm that you did initiate a wire. If we are unable to verify the wire, your funds transfer could be delayed. We apologize for the inconvenience, but we want to protect your funds.
- If you need to reach the bank concerning suspicious activity, please call us instead of using email. If your computer system has been compromised, the hacker could have access to your email and delete messages before we can receive them or send fake messages authorizing various activity.
- As always, if you are concerned about any electronic banking security issue, please do not hesitate to call us. If your call is urgent, please select 0 out of voice mail and ask the operator to find someone to address your issue.
 - > Leigh Ann Thompson: 334-887-4639

AS A BEST PRACTICE, REVIEW THE INFORMATION LOCATED IN THE
LINK ON THE WIRE OR ACH SCREEN



AUBURN BANK

NetTeller

Bill Pay

Cash Manager

eStatements

ACH
a

Wires

ARP

Users-

Reporting

File Status

Batch List

Upload

Tax Payment

Activity

Search

Please review important information about [Business Internet Bankina Security](#)

ACH Category List

WHAT'S CORPORATE ACCOUNT TAKEOVER?

- Corporate Account Takeover is a type of business identity theft in which a criminal entity steals a business's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business can fall victim to these crimes.
- Attacks today are typically perpetrated quietly by the introduction of malware through a simple email or infected website. For a business that has low resistance to such methods of attack, the malware introduced onto its system may remain undetected for weeks or even months.

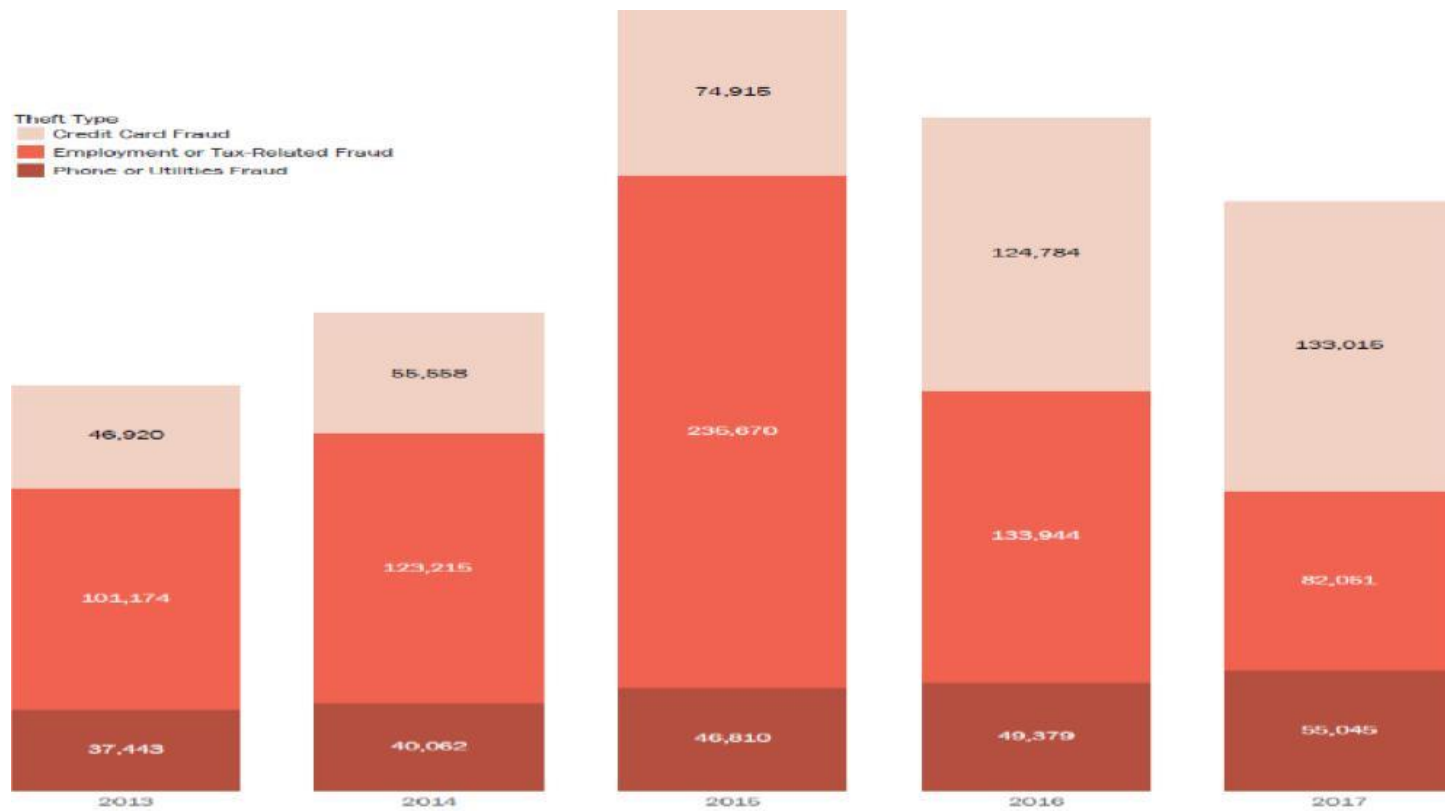
AM I PROTECTED?

- Consumers enjoy a certain level of protection that business bank accounts, DBA's, and Estates do not, and it's called "Regulation E".
- **Losses from Corporate Account Takeover are not covered under Regulation E. This means the financial institution is not obligated to replace funds that are stolen.**
- We encourage you to perform risk assessments and evaluate controls periodically.

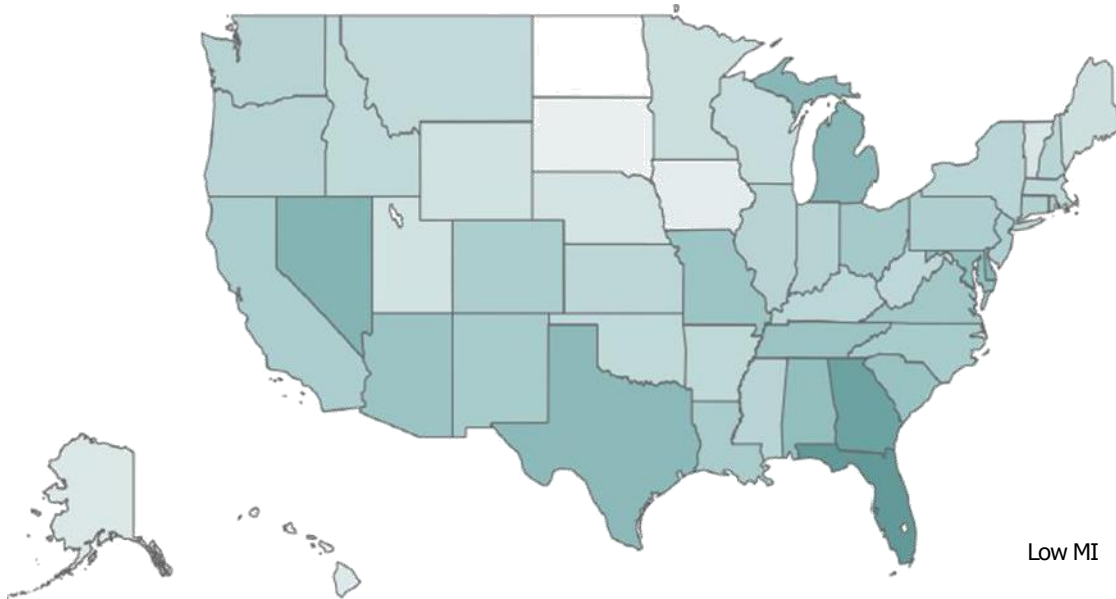
MALWARE-SHORT FOR MALICIOUS CODE DESIGNED TO DISRUPT AND/OR DENY OPERATION, GATHER INFORMATION, AND GAIN UNAUTHORIZED ACCESS

- Ransom Ware - a form of malware in which rogue software code effectively holds a user's computer hostage until a "ransom" fee is paid. Ransomware often infiltrates a PC as a computer worm or Trojan horse that takes advantage of open security vulnerabilities.
- Malware – short for 'Malicious Code Software' that is designed to gain unauthorized access, disrupt or deny operations, and gather private information.
- Virus – a computer program that can replicate itself and spread from one computer to another.
- Worm – a standalone malware computer program that replicates itself in order to spread to other computers.
- Trojan Horse (or Trojan) – a program with a benign capability that conceals another malicious program.
- Spyware – a type of malware installed on computers that collects information about users without their knowledge.
- Rootkit – a stealthy type of malware designed to hide the existence of certain processes or programs from normal methods of detection and to enable continued privileged access to a computer.

TOP THREE IDENTITY THEFT REPORTS BY YEAR



2017 STATE RANKINGS: FRAUD AND OTHER REPORTS



| RANK | STATE | REPORTS PER 100K | # OF REPORTS |
|------|----------------|------------------|--------------|
| 1 | Florida | 993 | 208,443 |
| 2 | Georgia | 924 | 96,316 |
| 3 | Nevada | 770 | 23,071 |
| 4 | Delaware | 758 | 7,290 |
| 5 | Michigan | 750 | 74,689 |
| 6 | Texas | 729 | 206,305 |
| 7 | Maryland | 694 | 42,032 |
| 8 | Alabama | 687 | 33,467 |
| 9 | South Carolina | 660 | 33,137 |
| 10 | Tennessee | 649 | 43,579 |

Low MI Reports per 100K Population High

STATES ARE RANKED BASED ON THE NUMBER OF REPORTS PER 100,000 POPULATIONS. POPULATION ESTIMATES ARE BASED ON 2017 U.S. CENSUS POPULATION ESTIMATES

HOW BREACHES MIGHT OCCUR

- Hacking – finding weaknesses in a computer or computer network and exploiting them. The term can also refer to someone with an advanced understanding of computers and computer networks.
- Malware – a malicious software designed to disrupt computer operation, gather sensitive information, or gain unauthorized access to computer systems.
- Physical attacks – occur when attackers are able to physically access a system.
- Social tactics – Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or internet to trick a person into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes.
- Privilege misuse – fraud by gaining access rights and is committed by trusted users.

FORGET NORMAL BUSINESS HOURS!

Cyber crime is not a 9 to 5 job and it is not only local. It is a global issue and cyber criminals are working 24 hours a day to access information illegally.

Criminals might begin the day with a nice compiled list of computer addresses for vulnerable devices along with exact user names and passwords needed to access them. After that, they may put in a few hours cramming malware onto selected systems and then revisit last week's victims to collect any captured data.

They then sell it to make their money. This is their livelihood.

AUBURNBANK SECURITY

AuburnBank maintains layered security methods in addition to your user name and password including:

- U RSA secure tokens
- U Fraud detection monitoring systems
- U Challenge questions
- U Exposure limits
- U Bank approval of new users and changes in user settings.

Additional methods available to you at no additional cost

- U Token authentication
- U IP restrictions-only allow certain IP addresses
- U Time restrict-Administrator can establish days or times users can access NetTeller
- U Dual control on ACH & Wire transfers
- U Secure Token Code to Create, Modify, or Initiate an ACH batch or transmit Wire Transfer

WHAT CAN I DO?

While AuburnBank takes multiple security measures to help protect your personal information, unfortunately fraud is constantly changing. Here are some tips on how to protect your sensitive information:

- We encourage you **not** to communicate sensitive information through an unsecure method.
- Create a secure financial environment by dedicating one computer exclusively for online banking and cash management activity. This computer should not be connected to the business network, have email capability, or connect to the Internet for any purpose other than online banking.
- Reconcile accounts online daily; at a minimum, review pending or recently sent ACH files and wire transfers.

WHAT CAN I DO (CONTINUED)?

- Be very skeptical of random pop-up windows, error messages and attachments.
- Use appropriate tools to prevent and deter unauthorized access to your network and periodically review such tools to ensure they are up to date. These tools include:
 - > Firewall and virus protection programs
 - > Security suites
 - > Anti-botnet, anti-malware, and anti-spyware programs
 - > Encryption of laptops, hard drives, VPNs or other communication channels
 - > Education of all computer users

CONTACT INFORMATION

Please make sure that we have valid information to contact you in the event we suspect unusual activity. Such as:

>email address

>phone numbers

>fax number




RESOURCES

Additional information can be found at

<http://www.fbi.gov/about-us/investigate/cyber/cyber>

<http://onguardonline.gov/>



Please contact AuburnBank if you have any questions or would like additional information on corporate account takeover, payments fraud, or treasury management services.

AuburnBank Contacts:

Leigh Ann Thompson – lthompson@auburnbank.com

334-821-9200

External Website Disclaimer - At certain places on our Website, there are links to other Websites. AuburnBank does not endorse, approve, certify, or control those external sites and does not guarantee the accuracy, completeness, efficiency, timeliness, or accurate sequencing of the information contained in them.