Garland W. Binns, Jr.
Dover Dixon Horne PLLC
Attorneys at Law
425 West Capitol, 37th Floor
Little Rock, Arkansas 72201
Telephone: (501) 978-9923
Facsimile: (501) 375-6484
Email: gbinns@ddh-ar.com
Web Site: www.GWBinns.com

DECEMBER 2014

U P D A T E

News of Developments in the Financial Sector and Related Areas

* *IN THIS ISSUE* *

Cybersecurity

Computer security is generally referred to as Cybersecurity. The technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access is known as Cybersecurity. In a computing context, the term *security* implies Cybersecurity.

JP Morgan Chase, K-Mart, Target, Home Depot and Dairy Queen stores have been the targets of recent cyber-attacks with the hackers obtaining access to such things as customer names and credit and debit card numbers. The cost of a cyber-attack is significant. Publish reports indicate that Home Depot expects to pay $62 million this year to recover from the recent data breach.

Probably one of the most important things that a bank can do in protecting from a security breach involving customers of the bank is to select the right vendor. A bank should engage in comprehensive due diligence of a vendor and should compare the services provided by different providers. It is important for the bank to review the experience and reputation of a vendor in connection with security data issues. If the vendor is to subcontract a portion of the services to the bank, the bank will want to conduct similar due diligence of the subcontractor. This also may include the bank upgrading its security systems and requiring customers to adopt additional security measures in addition to the ones currently in place.

In small business customers, a tool in a cyber-attack is keylogging malware. A keylogger is a software program that records the keystrokes entered on the PC on which it is installed and transmits a record of those keystrokes to the person controlling the malware over the Internet. Keyloggers can be surreptitiously installed on a PC by simply visiting an infected website or by clicking on an infected website banner advertisement or email attachment. Keylogging can also be accomplished via a hardware device plugged into the PC which stores the captured data for later use. They often go undetected by most antivirus programs. Keyloggers are used to steal the logon ID, password, and challenge question answers of financial institution customers. This information may enable the hacker to log into the customer's account and transfer funds to accounts controlled by the hacker.

Other types used in small business customers of more sophisticated malware allow the hacker to perpetrate man-in-the middle (MIM) or man-in-the browser (MIB) attacks on the victim. In a MIM/MIB attack, the hacker inserts himself between the customer and the financial institution and hijacks the online session. In one scenario the hacker is able to intercept the authentication credentials submitted by the customer or modifies the transaction or

inserts additional transactions and transfers funds to accounts controlled by the hacker. The hacker conceals his actions by directing the customer to a fraudulent website that is a mirror image of the institution's website. The hacker may have the capacity to delete any trace of the attack from the log files.

Attempts on financial institutions may include disrupting online services with excessive traffic from multiple sources, or hackers impersonating customers and sending unauthorized transactions.

The Texas Bankers Electronic Crimes Task Force was formed by the Texas Banking Commissioner in cooperation with the United States Secret Service to develop processes and controls for reducing the risks from cyber-attacks by hackers. The processes and controls of the Task Force center on three core elements which are *Protect; Detect; and Respond.*

Protect – A risk assessment should include the risks to online payment services with an identification of the bank's existing controls that need to be implemented. All customers using online banking services should be evaluated for risk. Reviews of risk rating should be conducted annually by the bank. The Board of Directors of the bank should be informed of the risks and controls and provided with examples of crimes perpetrated by hackers, how they occur and the losses experienced. The bank should periodically communicate to customers security practices to reduce the risk of theft. The bank needs to have controls that include account monitoring and fraud detection systems that flag unusual transactions for further review. The bank should have written agreements with corporate customers using online banking services. A bank must work with its vendor to conduct annual risk assessments.

Detect – The Federal Financial Institutions Examination Council's *Supplement to Authentication in an Internet Banking Environment* conveys the minimum expectations that banks should implement to detect anomalies related to initial login to online banking and transactions relating to the transfer of funds to other parties. Monitoring for large transactions is one of the most effective techniques for detecting fraudulent transactions. Educating bank employees is fundamental in detecting fraudulent account activity. Educating account holders on how to detect anomalies or potential fraud is important in preventing cyber-attacks.

Respond – An incident response plan should include actions for stopping fraudulent account activity. The plan should be reviewed annually. The plan must include bank employees knowing how to contact account holders immediately. The customer's primary and secondary contact information including after-hours phone numbers are critical. The plan should include the ability of the bank to cover funds quickly. The plan must include notifying other banks that have received stolen money and requesting a hold on those funds. The bank needs to act quickly to close off the method being used to commit the crime. Law enforcement and regulatory agencies should be contacted and notified by the bank. Procedures need to be in place in connection with contacting customers and documenting all discussions. The plan should include the names of firms to use for forensic analysis.

Because of the security demands and reputation risk of the bank, it is important to engage in comprehensive due diligence in selecting the vendor to provide the security systems, services, and measures needed by the bank.