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

MARCH 2015

U P D A T E

News of Developments in the Financial Sector and Related Areas

* *IN THIS ISSUE* *

Cybersecurity Insurance Coverage

Cybersecurity insurance is designed to mitigate losses from a variety of cyber incidents, including data breaches, business interruption and network damage. JP Morgan Chase, K-Mart, Target, Home Depot and Dairy Queen have been the targets of recent cyber-attacks with hackers obtaining access to such things as customer names and credit and debit card numbers. The cost of a cyber-attack is significant. The risk of cyber-attacks creates a continuing and complex challenge for banks.

It is the bank's obligation to protect the data and financial information of its customers. Cybersecurity insurance coverage is insurance coverage for liability that arises out of unauthorized use of, or unauthorized access to, electronic data or software within a bank's network. Cyberinsurance liability policies provide coverage for liability claims for spreading a virus or malicious code, computer theft, extortion, or any unintentional act, mistake, error, or omission made by employees of the bank while performing their duties. The typical insurance policy only covers what is referred to as tangible assets and electronic data is not considered tangible under the typical policy definition. Cyperinsurance coverage fills this gap.

In order to purchase cyberinsurance coverage, insurers will want to conduct a due diligence audit of the bank's data protection plan or review the bank's disaster plan. The insurer is going to want to know what technical protections exist in the bank's system and what employee training and security steps that have been taken to secure the bank's network and data.

Besides the purchase of the cyberinsurance policy, it is important to have the right vendor in place in protecting customer information from a security breach. The bank should engage in comprehensive due diligence of a vendor and compare the services provided by different vendors. It is important for the bank to review the experience and reputation of a vendor in connection with security data issues. If a vendor is to subcontract of portion of the services to be provided to the bank, the bank will want to conduct similar due diligence of the subcontractor. In protecting customer information, the bank may need to upgrade its security systems and require customers to adopt additional security measures in additional to the ones currently in place. Because of the security demands and reputation risk of a 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. It is a good idea to conduct a thorough review of the bank's security measures and have them in place such as antivirus software and firewalls before the insurer conducts its due diligence

audit which may lead to lower premiums on the cyberinsurance policy. Because cyber threats are constantly evolving, a bank must be vigilant in safeguarding customer data.

A bank has various options in selecting the cyberinsurance coverage offered by an insurer. *Third party coverage*, which involves a lawsuit against a bank by a customer or third party, covers defense costs and the ultimate settlement or damages relating to:

● Network security which covers customers bringing suit arising from a breach in network security.

● Privacy liability which covers claims from clients that typically arise from a release of their personal information through a non-cyber breach such as a dumpster dive, lost laptop and exposed customer list.

● Media liability which covers a party bringing suit alleging online copyright infringement.

● Regulatory which covers governmental or regulatory claims arising from a data breach.

First party coverage, which involves reimbursement to a bank relating to:

● Crisis management which covers public relations services needed in response to a breach.

● Breach remediation which covers costs for credit monitoring, forensics and restoration of data.

● Notification costs which covers costs to notify customers of a cyber-breach.

● Cyber extortion which covers investigation of a threat of a cyber-attack or the actual extortion of a breach.

● E-business interruption which covers the loss of income and extra expense resulting from a cyber-attack.

Cyberinsurance cannot protect a bank from a cyber-incident any more than flood insurance can save a person's house from a storm surge or directors and officers insurance from a lawsuit. However, cyberinsurance does provide a measure of financial support in the event of a data breach or a cyber-attack. Qualifying for cyberinsurance may provide useful information for assessing the bank's risk level and identifying cyber-tools and practices that may be lacking.

SIG TARP Quarterly Report

The Office of the Special Inspector General for the Troubled Asset Relief Program ("SIGTARP") was established by the Emergency Economic Stabilization Act of 2008. Under the Act, the Special Inspector General has the responsibility to conduct, supervise and coordinate audits and investigations of the purchase, management and sale of assets under the Troubled Asset Relief Program ("TARP"). Early this year, SIGTARP issued its quarterly report to Congress.

As of December 31, 2014, 134 institutions remained in TARP as follows: 34 banks remaining in the Capital Purchase Program ("CPP") with principal investments owned by the Treasury; 34 CPP banks for which Treasury now holds only warrants to purchase stock; 66 banks and credit unions in the Community Development Capital Initiative ("CDCI"). The Treasury does not consider the 34 CPP participants in which it holds only warrants to be in the TARP program, however, the Treasury applies all proceeds from the sale of warrants in these banks to recover amounts in TARP's CPP program. The Treasury is continuing to exit the TARP program through the auction of TARP securities.