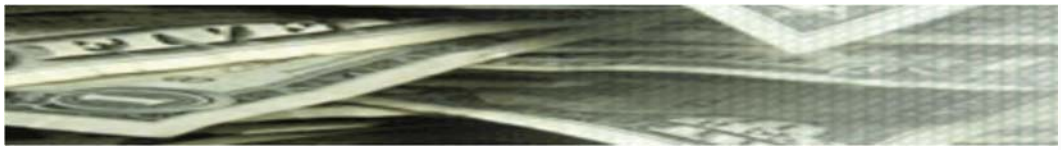
January 2017 Volume 6, Issue 1



State of North Dakota DEPARTMENT of FINANCIAL INSTITUTIONS

A MESSAGE FROM COMMISSIONER ENTRINGER

First, let me wish you all a Happy and Prosperous New Year! 2016 was certainly an interesting year especially for me; some of you were aware of my plans to retire at yearend 2016. Obviously, I did not retire! After visiting with a number of people and of course some personal reflection, I decided to seek reappointment by Governor Doug Burgum. On December 12th the Governor announced his cabinet and I was pleased to be reappointed! I would like to thank all of you who supported my decision to seek reappointment; your confidence in me is certainly humbling.

Now for the New Year; the legislature is in full swing. On the second day of the session, the only bill introduced by the department was scheduled for a hearing. As luck would have it, our appropriation bill was scheduled for a hearing on day three. I would like to thank Rick Clayburgh and Barry Haugen for their support of the department's appropriation request; at this time it is much too early to tell what action the legislature will take regarding our appropriation request.

As you all know, Initiated Statutory Measure No. 5 related to medical marijuana passed rather handily and I am sure many of you are wondering what to do should a medical marijuana business approach your institution to open an account. Our staff has been diligently working to find answers to the questions we anticipate receiving. We are looking to plan a Day with the Commissioner at which we hope to be able to provide some useful guidance to you and your staff.

You may recall last year the department hosted an Executive Leadership of Cybersecurity Seminar. The speaker from the US Secret Service made a comment that bankers are considered experts in the area of cybersecurity. Upon hearing this comment, one banker started working to provide a cybersecurity seminar for their institution's business customers. In September, this institution hosted a workshop entitled "Cybersecurity for Business Made Simple." The reason I mention this workshop is to seek your input. An individual from the National Cybersecurity Alliance who helped put together the above referenced workshop has reached out to our department to see if we would be interested in hosting a similar workshop which would essentially be a "train-the-trainer" so your staff would be able to sponsor such an event for your business customers. You can read more about NCSA on page two but my thought is that this would be part of a Day with the Commissioner, such as an afternoon workshop for your staff members to be trained to host such an event. If you think this is something you would be interested in please contact either myself (REntring@nd.gov) or Chief Examiner Lise Kruse (LKruse@nd.gov).

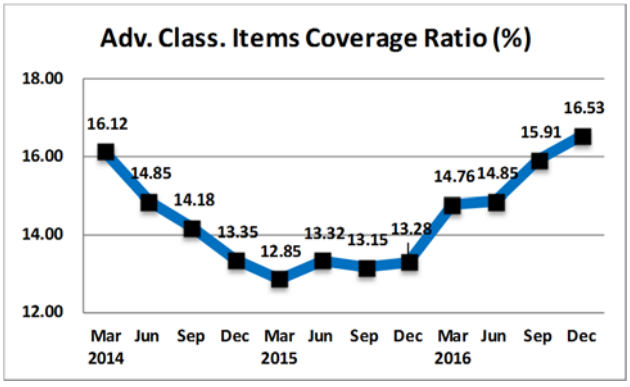
Once again Happy New Year and I look forward to meeting with you in the coming months at a Day with the Commissioner. If you have other topic suggestions for the Day with the Commissioner please feel free to let Lise or myself know.

FACTS & FIGURES

As of December 31, 2016:

- Average Adversely Classified Items Coverage Ratio: 16.53%
- Average Adversely Classified Assets/Total Assets: 1.70%
- Average Adversely Classified Loans/Total Loans: 2.20%
- Average Past Due & Nonaccrual Loans/Total Loans: 1.64%

Averages are of the 69 North Dakota state-chartered banks.



Cybersecurity and Small Businesses

Cybersecurity is a challenge in today's society. Banks are facing attacks and so are bank customers. Corporate account takeover and business email compromise is becoming more and more frequent. In the last few months, several institutions have reported ransomware attacks (backups that work are extremely important) that came from customers' compromised email accounts. Luckily these institutions had quick-thinking employees that knew to disconnect from the network and the institutions were able to utilize their backup, preventing any financial loss. The best way to prevent these attacks is education. Educating employees and customers to not open suspicious attachments or clicking links can prevent a majority of these compromises.

Community banks have important relationships with small and medium-sized businesses (SMBs). SMBs are the backbone of the American economy. According to the U.S. Small Business Administration, the 28 million small businesses in America account for 54 percent of all U.S. sales. Additionally, firms with fewer than 100 employees make up the largest share of small business employment. When these businesses fail or suffer, the economy reacts in the same way. Small businesses provide the fabric that builds communities and holds them together. These businesses generally don't think they are targets for cyber attacks; they may think they are too small or have nothing of value for cybercriminals to steal. Many SMBs do not hire IT or technical security people because of cost or a lack of awareness about the cybersecurity vulnerabilities they face.

The reality is that companies of all sizes are at risk, and small and medium-sized businesses are growing targets for cyber thieves. According to Symantec, there has been a steady increase in the prevalence of phishing attacks targeting businesses with fewer than 250 employees, with 43 percent of all attacks in 2015 targeted at small businesses. SMBs are often targeted because they do business with larger companies, some which may be operators of critical infrastructure.

NATIONAL CYBERSECURITY ALLIANCE

The National Cyber Security Alliance (NCSA) is creating a comprehensive program to engage this audience and provide much-needed information to SMBs to help them become more cyber-secure. As the cornerstone of the program, NCSA has translated the NIST Cybersecurity Framework into simpler language and incorporated it into an introductory-level, in-person, highly-interactive workshop. The NCSA has created and field-tested a workshop designed to help SMBs learn to integrate cybersecurity practices, utilizing a simplified version of the NIST Cybersecurity Framework and incorporating content from federal and industry partners, including recent threat data. Through these workshops, NCSA teaches smaller organizations how to think about cybersecurity, leading them through various scenarios and steps they can take to better secure their data.

Recognizing the opportunity to assist its customers in protecting themselves from Cybersecurity attacks, Starion Bank held a Cybersecurity seminar for its small business customers in partnership with NCSA in September. The seminar was well received and provided the bank with positive media coverage (here). The Department has been in touch with NCSA and would like your feedback to gauge your interest in a "train-the-trainer" session conducted by NCSA in order for your bank to host a seminar to educate and help protect your customers from Cybersecurity fraud. Please contact Lise Kruse (328-9938) or Bob Entringer to let us know if this is something your bank would be interested in attending.

Bank Secrecy Act and medical marijuana

Measure number 5, also known as the Compassionate Care Act, for medical use of marijuana passed in North Dakota on November 8, 2016. The Department of Health is tasked with regulating and enforcing the new act, which is expected to take up to a year to be put in place. Each bank's Board of Directors and management should assess the risk and decide how to handle marijuana-related customers. These businesses should be included in the bank's BSA risk assessment, policies, and procedures. Enhanced customer due diligence and reporting requirements are necessary if the financial institution decides to serve these type of customers. Click here for guidance issued by the Financial Crimes Enforcement Network (FinCEN) on February 14, 2014, regarding marijuana businesses, and click here for corresponding guidance issued by the Department of Justice entitled Guidance Regarding Marijuana Related Financial Crimes.

BSA Reminder: Financial institutions must comply with the Final Rule on Customer Due Diligence (CDD) requirements by May 2018. Frequently Asked Questions regarding CDD requirements were issued by FinCEN on July 19, 2016, and can be found here.

Regulation O

Several recent examinations have included an apparent violation related to Regulation O. The more common violations typically relate to (a) the failure to obtain prior approval from the Board of Directors for a loan to a director, executive officer, or principal shareholder, and (b) loans which exceed the lending limit restrictions for executive officers. Often, this latter issue occurs because management does not fully understand which loans are subject to the lending limit restrictions, including loans to partnerships in which the executive officer has a majority interest. The regulation states that a bank may extend credit in any amount to finance (1) the education of the executive officer's children or (2) to finance the purchase…of a residence of the executive officer provided (i) the extension is secured by a first lien and (ii) is owned by the officer. Additionally, a bank may extend credit in any amount if the extension is (A) properly secured by bonds, notes, certificates, or Treasury bills, (B) subject to an unconditional takeout commitment or guarantee of a U.S. establishment, or (C) fully secured by segregated deposits in the bank. If the extension of credit is for any other purpose, the aggregate amount of extensions of credit to that executive officer is limited to the higher of 2.5 percent of unimpaired capital and surplus or $25,000, but in no event more than $100,000. The executive officer lending limit also applies to partnerships in which one or more of the bank's executive officers hold a majority interest. The amount of credit extended to the partnership is considered to be extended to each executive officer of the bank who is a member of the partnership.

Ransomware- are you prepared?

Headlines and stories abound regarding businesses being compromised by ransomware. These stories are concerning and we are not immune. The DFI is aware of banks in North Dakota that have experienced ransomware attacks. As a refresher, ransomware is a type of malicious software that targets your network systems for the purpose of extortion. Your network may become infected with ransomware if a user opens an attachment from an unsolicited email or clicks on a link. The ransomware locks down the system and demands payment for the "key" to unlock the network. Often times, the "key" provided does not work and the network remains locked down. Institutions that are victims of ransomware may experience permanent loss of information, disruptions, financial losses, and/or potential harm to their reputation. So, what is a business to do? How do you protect yourself? How do you respond if you are the victim of such an attack? While there is no magic answer, this document prepared by the Treasury Department together with a group of U.S. intelligence and regulatory agencies, provides some effective prevention and response actions that help to mitigate the risk posed by a ransomware attack. Under certain circumstances, it may be necessary to file a Suspicious Activity Report. The following advisory was recently issued by FinCEN and addresses cyber events and cyber related crime, along with a FAQ.

Department of Financial Institutions
2000 Schafer Street, Suite G
Bismarck, ND 58501-1204
Phone: 701-328-9933
Fax: 701-328-0290
E-mail: dfi@nd.gov
Website: http://www.nd.gov/dfi/