Nebraska Banker
JANUARY/FEBRUARY 2021
NBA Nebraska Bankers Association

Financial Education is Key

Page 8

OFFICIAL PUBLICATION OF THE NEBRASKA BANKERS ASSOCIATION

SBS CyberSecurity

NBA Nebraska Bankers Association

Understand your cybersecurity risk.

Gain a trusted cybersecurity advisor and ensure your ISP is well-managed with **CONSULTING** services.

Receive personalized **NETWORK SECURITY** testing tailored to your size and complexity.

Go beyond a checklist with a risk-based **IT AUDIT**, reviewing for compliance and adequacy.

Participate in uniquely designed, role-based, industry-specific cybersecurity **EDUCATION**.

Contact David Edwards

913-225-6382 | david.edwards@sbscyber.com

www.sbscyber.com

PMA™
FUNDING
Relax.
We do the work.
For over 35 years, PMA Funding™ (PMA) has been a leading provider of stable deposit and cost-effective funding solutions. The result: financial institutions have been able to diversify and manage their liquidity needs with greater flexibility.
The PMA companies provide financial services to more than 3,200 public entities and administer client assets over $30 billion, which offers our banking partners a dependable source of funding. Through unique funding capabilities, we develop custom deposit programs to meet your funding needs using a variety of deposit vehicles. PMA's client deposits provide the size and savings of the secondary CD market with the flexibility and stability of core deposits, without disrupting your local markets.
Put the days of worry—and cannibalizing your funding sources—behind you, and relax. We do the work. Call us at 800.783.4273 or visit us at www.pmafunding.com
*Total assets under administration as of 10.31.20 include money market pool assets for which the PMA companies serve as fund administrator/accountant, marketer/distributer, fixed income program provider (brokerage services), and/or investment advisory, or separate institutional accounts. PMA Funding is a service of PMA Financial Network, LLC and PMA Securities, LLC (member FINRA, SIPC) (collectively "PMA"). PMA Securities, LLC is a broker-dealer and municipal advisor registered with the SEC and MSRB. ©2020 PMA Financial Network, LLC. All rights reserved.
P 800.783.4273
W pmafunding.com

CONTENTS

Nebraska Banker
JANUARY/FEBRUARY 2021

EDITORIAL: Nebraska Banker seeks to provide news and information relevant to Nebraska and other news and information of direct interest to members of the Nebraska Bankers Association. Statement of fact and opinion are made on the responsibility of the authors alone and do not represent the opinion or endorsement of the NBA. Articles may be reproduced with written permission only.

ADVERTISEMENTS: The publication of advertisements does not necessarily represent endorsement of those products or services by the NBA. The editor reserves the right to refuse any advertisement.

SUBSCRIPTION: Subscription to the magazine, which began bi-monthly publication in May 2006, is included in membership fees to the NBA.

NBA BOARD OF DIRECTORS

CHRIS HOVE
NBA Chairman
(402) 423-2111
Nebraska Bank of Commerce
Lincoln

KIRK RILEY
NBA Chairman-Elect
(308) 784-2515
Waypoint Bank
Cozad

KATHRYN M. BARKER
(402) 894-7001
Core Bank
Omaha

NICHOLAS W. BAXTER
(402) 602-1839
First National Bank of Omaha
Omaha

CORY A. BERGT
(402) 434-4122
Wells Fargo Bank, N.A.
Lincoln

JOHN BOTHOF
(402) 334-0300
Northwest Bank
Omaha

JOHN T. DAUBERT
(402) 323-8008
Security First Bank
Lincoln

JUSTIN H. DOUGLAS
(402) 864-4191
Mainstreet Bank
Cook

DANIEL A. FULLNER
(402) 454-1000
Madison County Bank
Madison

KARL W. GRAMANN
(402) 988-2255
Adams State Bank
Adams

REX R. HASKELL
(402) 687-2640
First Northeast Bank of Nebraska
Lyons

KRISTA K. HEISS
(308) 534-2877
NebraskaLand National Bank
North Platte

DONALD A. JIVIDEN
(402) 759-8113
Heartland Bank
Geneva

ZAC KARPF
(308) 632-7004
Platte Valley Bank
Scottsbluff

JOHN F. KOTOUC
(402) 399-5088
American National Bank
Omaha

STEVE D. KUNZMAN
(308) 382-4000
Home Federal Bank
Grand Island

BRANDON MASON
(402) 918-5434
Bank of the West
Omaha

RAYMOND M. MCKENNA
(402) 363-7411
Cornerstone Bank
York

KAYE L. MONIE
(308) 368-5555
Hershey State Bank
Hershey

STEPHEN E. STULL
(308) 262-1500
Farmers State Bank
Bridgeport

JOSEPH T. SULLIVAN III
(402) 348-6000
U.S. Bank, N.A.
Omaha

CHRIS WIEDENFELD
(402) 952-6015
Great Western Bank
Omaha

CHRISTINE WILCOX
(402) 323-1067
Union Bank & Trust Co.
Lincoln

LYDELL L. WOODBURY
(402) 563-3659
First Nebraska Bank
Columbus

SCOTT A. ZIMBELMAN
(308) 784-2000
Homestead Bank
Cozad

ALAN D. EMSHOFF
NBA Past Chairman
(402) 266-5931
Generations Bank
Exeter

NBA EDITORIAL STAFF

RICHARD J. BAIER
NBA President and CEO
richard.baier@nebankers.org

KARA HEIDEMAN
Director of Communications
and Marketing
kara.heideman@nebankers.org

NBA Nebraska Bankers Association
233 South 13th Street, Suite 700
Lincoln, NE 68508
Phone: (402) 474-1555 • Fax: (402) 474-2946

The Baker Group Is Here to Help

FREE TRIAL

As American financial institutions—along with the rest of the world—face unprecedented times, The Baker Group is ready with tools and services to help ***maximize the performance*** of your institution.

That's why we're offering new clients our Software Solutions* ***service package for a six-month free trial***. Not only will you have access to our latest market research and insight from our Financial Strategies Group, you'll be included in all of our webinars. There you'll hear the latest on how COVID-19 could impact your institution and its investment portfolio.

Baker's Software Solutions Service Package Includes:

Asset/Liability Analysis – Interest Rate Risk Monitor (IRRM®)

Your management team will find that The Baker Group's quarterly review of the loan and deposit information outlined in the Interest Rate Risk Monitor and Asset Liability Analysis is an effective tool in managing your risk and performance.

Baker Bond Accounting® (BBA)

The Baker Group will provide you with accurate, easy-to-read reports delivered electronically to you each month.

Investment Analysis – Advanced Portfolio Monitor (APM®)

The Advanced Portfolio Monitor is a key monthly report that we utilize to help you measure, monitor, and manage the overall risk and performance of your investments.

To obtain the resources you need to maximize the performance of your bank, contact Ryan Hayhurst with our Financial Strategies Group at **800.937.2257**, or via email at Ryan@GoBaker.com.

Member: FINRA and SIPC

Oklahoma City, OK | Atlanta, GA
Austin, TX | Indianapolis, IN | Long Island, NY
Salt Lake City, UT | Springfield, IL

Ryan@GoBaker.com

www.GoBaker.com

800.937.2257

*The Baker Group LP is the sole authorized distributor for the products and services developed and provided by The Baker Group Software Solutions, Inc.

Financial Education is Key

Richard J. Baier, President and CEO, Nebraska Bankers Association

NEBRASKA BANKING FRIENDS:

Nebraska bankers all too often have a front-row seat when it comes to witnessing the financial understanding, or lack thereof, of their fellow Nebraskans and customers. We know that poor financial decision making can lead to extreme personal and professional hardships. Acquiring a solid understanding of financial concepts is an important skill set that is learned starting at an early age, both at home and through our education systems. While Nebraska has made strides in recent years to improve the financial education efforts within our school systems, more needs to be done!

In 2018, your NBA team, along with key bankers from across the state, worked with the Nebraska Department of Education and other interested stakeholders to modernize and enhance the state's K-12 business curriculum standards. These standards outline the goals and expectations for business classes taught by all Nebraska schools, including important classes such as economics and personal finance. Unfortunately, these business standards only apply to business classes, which are optional for our Nebraska students. In addition, these classes are typically limited to high school students.

More recently, the NBA and banking leaders again worked proactively with the education community to enhance the state's social studies educational standards. These social studies standards incorporate the foundations of economics and finance for kindergarten through 12th grade. Concepts contained in these standards represent only a portion of the overall content, which also incorporates history, government, geography and politics. Likewise, the Nebraska social studies standards do not require a specific full credit class focused on economics or personal finance. Unlike Nebraska, five states plus the District of Columbia currently do not have any type of economics and finance requirements within their educational standards.

Every two years, the National Council on Economic Education conducts the Survey of the States, which evaluates the Economic and Personal Finance Education in our Nation's Schools. Nebraska scores in the middle of the pack in these national comparisons. Twenty-one states, for example, require high school students to take a personal finance class. Similarly, 25 states now require students to take an economics class to graduate. Enrollment in a specific personal finance and/or economics course is not required by Nebraska educational standards. (https://www.councilforeconed.org/survey-of-the-states-2020/)

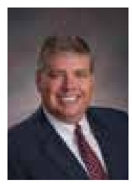
To supplement and encourage enhanced financial education, NBA member banks of all sizes offer a wealth of resources, programs, online platforms and classroom presentations. A number of Nebraska banks, for example, partner with NBA preferred vendor EverFi to offer the firm's online platform. Other NBA members have created and offer their own financial education platforms. Similarly, bankers from across the state annually make hundreds of classroom presentations with a focus on practical advice and real-world experience. The

NBA Personal Education Program (PEP – Soon to be Leaders in Financial Education) recognizes and rewards those NBA members who take their mission of supporting financial literacy in our schools extremely seriously. It can be argued that these tools are integral to education efforts in Nebraska.

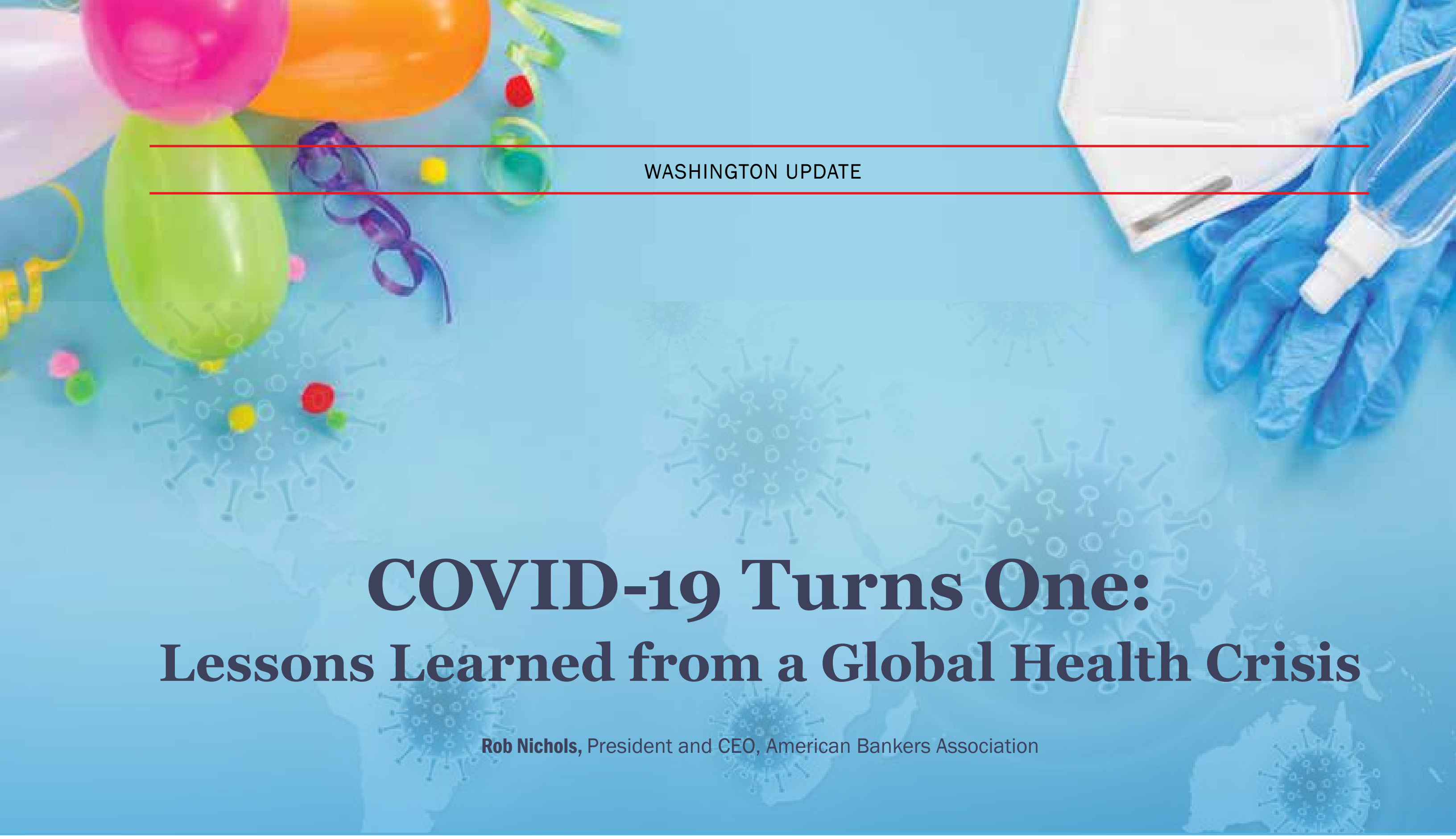
Over the past year, members of the Nebraska Legislature have taken an increasing interest in the topic of financial education. Numerous senators from both rural and urban Nebraska have dialogued with our NBA team about how to improve financial education in Nebraska. Other leaders including Nebraska State Treasurer John Murante, have also doubled down on enhanced efforts. As a result of these continued discussions, Senator McKinney of Omaha (LB 452) and Senator Slama (LB 327) have both introduced legislation with the intention of increasing financial literacy efforts in Nebraska schools. Senator McKinney's proposal deliniates several specific financial topics for incorporation into the state's education standards, while Senator Slama's legislative concept would require a semester-long personal finance class for all Nebraska high school students prior to graduation.

It is too early to predict how these proposals might be considered and evaluated by the entire Nebraska Legislature, but it is clear the state is increasingly focused on this important issue. In the meantime, the NBA and our bankers will continue to offer information, support, and direction with the goal of creating smarter and more financially savvy Nebraskans.

Numerous senators from both rural and urban Nebraska have dialogued with our NBA team about how to improve financial education in Nebraska.



Contact Richard J. Baier at (402) 474-1555 or richard.baier@nebankers.org.



COVID-19 Turns One:
Lessons Learned from a Global Health Crisis

Rob Nichols, President and CEO, American Bankers Association

AS IMPOSSIBLE AS IT IS TO BELIEVE, WE HAVE BEEN LIVING in a global pandemic for an entire year. What began as a headline from a distant corner of the world quickly became a worldwide health crisis that continues to wreak havoc on our way of life and has, unfortunately, claimed the lives of too many of our fellow citizens.

As I reflect on the last 12 months and the incredible changes that occurred virtually overnight to keep our society moving in the face of perilous uncertainty, I am filled with a deep sense of pride in how the banking industry stepped up to help make that happen. It speaks to the “can-do” spirit of America’s 2 million bank employees that as the world was shutting down, as daily routines were being upended, bankers embraced their role as economic first responders and got to work extending aid that helped keep individuals and businesses afloat.

With vaccines now being rolled out to certain groups, we are anxiously awaiting the day when we can finally return to some semblance of a normal life. But achieving herd immunity from the virus will take time, and as we prepare to mark one full year of quarantines, social distancing and face coverings, I’d like to offer a few observations.

Our financial system is resilient. After the last financial crisis, banks worked diligently to increase safety and soundness and manage risk more effectively. The post-2008 reforms were intended to help banks better absorb financial shocks — and the success of those reforms was borne out in the crisis response. It was widely acknowledged, by everyone from Financial Services Committee Chairwoman Maxine Waters (D-Calif.) to Federal Reserve Chairman Jerome Powell that banks performed well and were part of the solution to the coronavirus crisis.

Thanks to the strength of our financial system, there is reason to be hopeful for the economic recovery. In fact, the top economists at some of the nation’s largest banks who serve on ABA’s Economic Advisory Committee agree that we could see growth topping 4% in 2021. We must, of course, temper that expectation with the knowledge that the recovery will likely be uneven, and that labor markets could lag behind overall growth, given the massive job losses that occurred. That’s why, going forward, our advocacy for pro-growth policies will be more important than ever.

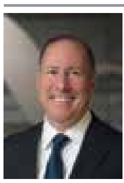
The digital revolution has been rapidly accelerated. Banks were already well on their way toward digital transformation before COVID-19. But the pandemic provided a push to bank customers who may not have fully embraced digital banking to do so in earnest. That will accelerate the digital transition even further, and will surely lead to efficiencies for banks down the road. The robust digital banking landscape also bodes well for financial inclusion—the ability to remotely access banking services will enable a broader set of customers to take advantage of the full panoply of financial tools and resources at their fingertips.

The relationships with our state associations are critical. From the earliest days of the pandemic, state associations played an instrumental role in analyzing and disseminating information that bankers needed to make PPP loans, facilitate economic impact payments and continue operating amid constantly changing health and safety guidelines.

With the help of our State Association Alliance partners, we delivered free resources to ABA members and nonmembers alike—including 33 free webinars, operational aids, crisis communications toolkits, scientific analyses and more—recognizing the importance of helping all banks weather the crisis.

Through weekly calls—and sometimes daily calls—there was a continuous flow of information and feedback between ABA in Washington and all 50 states. This collaboration was vital as policymakers worked to calibrate and re-calibrate rules and regulations implementing the first CARES Act. I have no doubt that this engagement will continue now that a second stimulus has been passed and a third package could soon follow.

These are just a few takeaways from this historic period. In the years ahead, I'm sure there will be even more robust lookbacks and more lessons that can be extrapolated from the coronavirus crisis. And the result of all of that learning, I hope, will only serve to make us stronger, safer and even more prepared for the future. ◗



Email Rob Nichols at rnichols@aba.com.

OFAC Guidance on Ransomware Payments

Bob Kardell, Attorney, Baird Holm LLP and **Halle Hayhurst,** Law Student and Summer Associate, Baird Holm LLP

On Oct. 1, 2020, the Office of Foreign Asset Control (OFAC) issued guidance on the payment of ransoms for victims of ransomware to recover from an attack. The guidance reminds everyone that payments for ransomware can go to support nation-state actors, terrorist groups and organized crime.

The Evolution of Ransomware

Ransomware has existed for many years now. One of the first instances of encryption malware can be traced to the PC Cyborg virus in 1989 . And the ransom payment for the decryption process began in 2005 and continued in several different strains. But, in 2011, cryptocurrencies began to emerge which allowed for global payments outside of the traditional banking processes. The rise of Bitcoin and other cryptocurrencies led to a rise in the ransomware attacks because the payment of the ransom could be conducted with relative ease and anonymity.

The general response to ransomware by companies has been greater IT security and multiple backups to enable recovery from ransomware in a relatively short period of time. Offline backups have become particularly important because they should be insulated from encryption malware and can help companies recover without having to pay a ransom to the attackers. The response from companies has been so good though, ransomware attackers have turned to a different method of attack – extortion.

Several groups of ransomware attackers now exfiltrate information from networks before the encryption process begins. The exfiltration of the data allowed the attackers to capture, review, and threaten exposure of potentially sensitive data even if the company were able to recover from the encryption attack by using their offline backups.

Bitcoin Used by Terrorists

Over the past year there have been many reports of government seizures of cryptocurrency which were being used by terrorist groups. In August the Department of Justice (DOJ) announced the largest seizure of terrorist organizations crypto currency assets. The seizure was part of an investigation into three different terrorists' networks: the al-Qassam Brigades, al-Qaida, and Islamic State of Iraq and the Levant (ISIS). Each of the organizations was using cryptocurrency to solicit donations from around the world and to move money and pay assets around the world.

In September, the French police arrested 29 people tied to cryptocurrency transactions designed to finance Islamist extremists.

In January 2020 the MIT Technology Review reported that criminals had laundered about $2.8 Billion through the use of Bitcoin in 2019.

And Advanced Persistent Threat actors (APT32) was recently caught deploying cyber espionage software along with cryptocurrency miner software.

The rise of cryptocurrency has allowed millions of dollars to move around the globe outside of traditional financial markets. Bitcoin accounts for only 0.04% of the world's money, but it is roughly worth $106 Billion dollars . Although the percentage of total money is small, the amount of money that can be moved outside the purview of traditional banking is quite substantive. Criminal groups, nation-state actors, and terrorists have all seen the possibilities of moving money outside of the traditional market to hide the source, nature, destination and use of the money.

While Bitcoin itself is the currency, the currency is moved and tracked using blockchain technology and cryptocurrency wallets. The blockchain uses wallet addresses to move the money to keep track of the balances of the total amount of cryptocurrency, the balances of each wallet, and the total transactions which take place. Because the blockchain and wallets use anonymous addresses, most users and people believe that the owner of the wallets are anonymous as well. But investigations into the use of the wallets and the addresses associated with the wallets often result in the attribution of the wallet to a person in many instances. Bitcoin wallets can be traced on the Dark Web and can be identified through classified sources and methods.

Because Bitcoin uses the blockchain to maintain the public ledger, once one transfer can be traced to a Bitcoin wallet and attributed to an individual, then all transfers made to the same wallet can be traced as well. All ransom payments would be able to be tracked and traced using this same method.

The OFAC Memorandum

The continued rise of seizure of cryptocurrencies from terrorists' groups and the rise of money movement outside the normal financial channels lead OFAC to issue their memorandum. The memorandum is a five-page explanatory memo interpreting the sanctions laws and regulations as they apply to ransomware payments.

The memo outlines several key points for the application of payments to ransomware:

First, ransomware threat actors, wallet addresses, and email addresses have been added to the OFAC Specified Designated National (SDN) list for the past several years. As the number of ransomware attacks have grown and payments have grown, there has been increased intelligence that money has been traced to groups engaged in the types of activities which are subject to bans. OFAC has added names and identifiers for people and addresses involved in attacks such as the Cryptolocker, SamSam, WannaCry, Evil Corp and others.

Second, ransomware itself and payments to the threat actors are a threat to national security. Research and intelligence have shown that money is being funneled to and used by terrorists groups, organized crime, and others acting against the interests of the United States. The payment of the ransom only feeds these activities and emboldens the criminals to conduct more of these attacks. The continued payment of ransoms only ensures the continued criminal activity.

Third, facilitating payments may be a violation of OFAC regulations. Facilitation can be any transaction, including transactions by non-US persons that cause a payment, either directly or indirectly, to individuals or organizations on the SDN list may be a violation. In addition, any transaction or act which causes a person to violate the regulations is also prohibited.

Fourth, organizations should adopt a risk-based approach to ransomware attacks and account for the possibility that a payment may violate OFAC regulations. This advice or guidance is for any company involved in the response to a cyber-attack including cyber insurance companies, digital forensics, and incident response organizations. Knowing the process to search the SDN list may prevent an

COUNSELOR'S CORNER — continued on page 14

COUNSELOR'S CORNER — continued from page 13

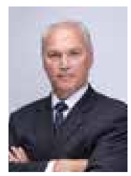
organization from unknowingly violating the sanctions. As OFAC states, a violation of the sanctions is a strict liability crime and does not require knowledge that someone is on the list; the payment to someone on the SDN list is a violation.

Finally - and this may be the most important part of the memo - OFAC highly encourages the cooperation with law enforcement and investigative officials. The cooperation with law enforcement will be considered a "significant mitigating factor." OFAC will also consider the "full and timely cooperation … a significant mitigating factor when evaluating possible enforcement outcome." During a presentation regarding this memo by members of the Department of Justice and the Department of Treasury, the presenters were quick to point out that no companies have been prosecuted for paying a ransom to a threat actor on the SDN list, but cooperation with law enforcement will ensure your organization is not the first.

Planning Ahead

According to Robert Mueller there are two kinds of companies; those that have been hacked and those that are about to be hacked. And according to the Cisco CEO John Chambers, there are two kinds of companies; those that have been hacked and those that don't know it yet. Given the recent hack of FireEye through the compromise of SolarWinds, there are most likely many companies that have yet to know that they have been compromised. As the analysis continues on the scope of the attack, there will be many more organization filing breach notifications. But there are actions an organization can take to minimize the effect and cost of a hack.

To protect themselves, OFAC encourages organizations to perform a risk-based analysis and keep regular backups to protect themselves from ransomware. Secure, offline backups are the key to recovering from ransomware attacks. Perform due diligence on the threat actors before payment. Notify and cooperate with law enforcement. This includes knowing who to contact and how to contact law enforcement. Institute and maintain a risk-based compliance program which includes a management commitment, risk assessments, internal controls, auditing and training. The key to dealing with ransomware is planning – have a plan based on a risk-based approach and practice, practice, practice that approach.



Bob Kardell, Attorney, Baird Holm LLP
Halle Hayhurst, Law Student and Summer Associate, Baird Holm LLP

In his career, Bob has also worked on cyber-crime investigations as well as public corruption, white collar, and financial criminal and civil investigations. Bob has been both a certified computer forensics examiner and an accounting forensics investigator. He has testified numerous times as a fact witness in criminal trials and before grand juries, and drafted expert reports for both accounting and computer investigations.

Bob has been a member of the Association of Certified Fraud Examiners and the Heartland ACFE for 12 years. During that time, he has served as a Director for the local board and as a member of the editorial advisory committee for the ACFE's "Fraud Magazine". He is also a Certified Public Accountant (CPA) and a member of the Nebraska Society of CPAs; Certified Information Systems Security Professional (CISSP); Certified in Financial Forensics (CFF); Certified Fraud Examiner (CFE); and AccessData Certified Examiner (ACE).

Top Six Controls to Mitigate a Ransomware Attack

Kelley Criddle, Information Security Consultant, SBS CyberSecurity, LLC

COMBATING A RANSOMWARE SCENARIO CAN BE INTENSE and stressful, so most organizations agree that it is better to stop the attack from happening in the first place. Below you will find the top six controls that can be put in place to protect your organization's network and data from a ransomware attack.

1. Backup, Backup, Backup

It's important to note that backing up your network's data will not prevent a ransomware attack in the future, but doing so will make the situation abundantly less stressful. It's been said that there are two types of people in this world: 1) those who back up their data, and 2) those who wish they would have. It is a good rule of thumb to stick with the 3-2-1 rule. Have at least THREE (3) copies of data, store your backups on TWO (2) different types of media, and keep ONE (1) backup off-site; in other words, keep one copy of the data air-gapped. Creating an "air-gapped" backup would make it very difficult for an attacker to infect this copy of your data with ransomware.

2. Endpoint Protection with Scripting Control

When it comes to today's current antivirus or endpoint protection solutions, there are two (2) types of solutions:

1. Traditional, signature-based antivirus/endpoint protection solutions that rely on a known *signature* to identify if a file is potentially *malicious*; or
2. Modern, behavior-based antivirus solutions that look at the code of a file to determine what actions the file will look to take when executed.

While there are pros and cons to each, modern behavior-based antivirus solutions will handle and identify unknown and unidentified threats, rather than relying on known-bad signatures to prevent potential cyber incidents.

It's strongly recommended that you use a modern, behavior-based solution with second-generation detection capabilities, including scripting control. Keep in mind, some providers claim their product has scripting control consistently fail to detect Powershell scripts running on your network. Applications lacking scripting detection will not be helpful in the event an attacker uses the Powershell tool to create scripts that automate attacks. Your antivirus solution should be configured to the highest level of security, alerting and protection. These controls would be able to stop any scripts that would attempt to run without the user's permission. Modern, behavior-based antivirus solutions should also alert the user if any red flags (malicious behavior) are detected on your devices.

3. Multi-Factor Authentication

Multi-Factor Authentication (MFA) is an authentication method in which a user is granted access to an application only after allowing two or more pieces of evidence to the authentication mechanism, such as an SMS code, soft token or hard token. When enabled on a system, MFA would prompt the user if a malicious adversary tried to log in to an account, since the attacker should not have access to your smartphone (SMS or soft token) or hard token (physical device).

Not only would implementing MFA help prevent a ransomware attack, but doing so would mitigate the risk to various other cyberattacks as well, such as credential stuffing, business email account takeover, and phishing attacks. However, just like with every other control, MFA has its drawbacks. You must train employees only to provide authentication factors when they know they are logging in themselves.

4. Security Awareness Training

Employees are your first line of defense and are known as the "human firewall." It is important to educate workers of potentially malicious email attachments, links, website downloads, and other methods of spreading ransomware – including how to identify phishing emails and what to do if they receive or click on something in a phishing email. Phishing emails are still the #1 delivery vehicle for malware, and training your people to handle phishing emails properly may be one of the most important things you can do to mitigate your risk. It is a great idea to not only train and educate employees, but to test them, too.

5. Email Controls

Email sandboxing along with Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC) are impactful controls that can be put in place to protect your network against a ransomware attack.

Email sandboxing, which automatically tests links and attachments in an email in a secure environment before your users receive the email, adds a layer of security and lessens the chances of an employee clicking on a malicious link. The Advanced Persistent Threat subscription to Office 365, which implements the Safe Links and Safe Attachments sandbox controls, is an excellent example of how email sandboxing can protect your organization from email threats.

SPF, DKIM, and DMARC all help authenticate senders using an organization's specific domain. SPF prevents hackers from sending emails on behalf of an organization's domain. In addition to SPF, DKIM checks if an email was truly sent by the owner of that domain. DMARC uses both SPF and DKIM to determine the authenticity of the content of an email message. SPF, DKIM, and DMARC are typically free additions to your email system that can make a significant impact on the amount of junk or phishing email your organization receives.

6. Egress Firewall Whitelisting with Geolocation IP Blocking

Egress firewall whitelisting examines all outbound traffic from your network to the internet (at the firewall level) and only allows information to leave the network if your organization's IT administrator's requirements are met. Egress firewall whitelisting works best with geolocation IP blocking, which blocks activity to IP addresses associated with geographical locations in which your organization does not do business or wants to block intentionally (like certain foreign countries known for cybercrime). Blocking traffic to certain regions and countries while examining the traffic that leaves the network in the first place is an important control that would notify the organization if a ransomware scenario is unfolding.

For more information, contact Reece Simpson at 605-270-3916 or reece.simpson@sbscyber.com.

SBS delivers unique, turnkey cybersecurity solutions tailored to each client's needs, including risk management, consulting, on-site and virtual auditing, network security and education. Learn more at www.sbscyber.com.

AML/BSA Reform Is on the Horizon

Steve Manderscheid, Compliance Alliance

WHEN CONGRESS PUSHED THROUGH THE NATIONAL DEFENSE Authorization Act for fiscal year 2021, the banking industry breathed a sigh of relief with the glimmer of hope for the potential elimination of excessive regulatory burdens under the Bank Secrecy Act.

The reason for hope is the section within the legislation dedicated solely to improvements to anti-money laundering rules, including to:

- Improve coordination and information sharing among the agencies tasked with administering anti-money laundering and countering the financing of terrorism requirements, the agencies that examine financial institutions for compliance with those requirements, Federal law enforcement agencies, national security agencies, the intelligence community and financial institutions;
- Modernize anti-money laundering and countering the financing of terrorism laws to adapt the government and private sector response to new and emerging threats;
- Encourage technological innovation and the adoption of new technology by financial institutions to more effectively counter money laundering and the financing of terrorism;
- Reinforce that the anti-money laundering and countering the financing of terrorism policies, procedures, and controls of financial institutions shall be risk-based;
- Establish uniform beneficial ownership information reporting requirements to:
    - o Improve transparency for national security, intelligence, and law enforcement agencies and financial institutions concerning corporate structures and insight into the flow of illicit funds through those structures;
    - o Discourage the use of shell corporations as a tool to disguise and move illicit funds;
    - o Assist national security, intelligence, and law enforcement agencies with the pursuit of crimes; and
    - o Protect the national security of the United States; and
- Establish a secure, nonpublic database at FinCEN for beneficial ownership information.

The main purpose of this immense undertaking will continue to focus on safeguarding the United States financial system and those financial institutions that make up that system from the abuse of money laundering, terrorist financing and other illicit financial crimes.

Today, banks must develop and implement an effective risk-based AML program consistent with rules that transcend roughly 50 years of banking. Over that period of time many things have changed, especially the recent digital innovations relating to how consumers interact and conduct their banking and transactions. Unfortunately, the same cannot be said for the regulatory burden to file reports under archaic and arbitrary thresholds.

Under the current BSA Currency Transaction Reports (CTRs) requirements (not considering exemptions as they are a burden unto themselves), financial institutions must report currency transactions over $10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to be over $10,000 in a single day.

In addition to filing CTRs, the industry must report suspicious activity under the following thresholds:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
    - o Transactions conducted or attempted by, at or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction involves money laundering or other illegal activity, evades the BSA or has no business or apparent lawful purpose.

Under the current legislation, the Treasury Department is to undergo a formal review of these current arbitrary thresholds established for filing CTRs and Suspicious Activity Reports (SARs), including:

- Review of Thresholds for Certain Currency Transaction Reports and Suspicious Activity Reports.
  - o The Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall review and determine whether the dollar thresholds, including aggregate thresholds, under sections 5313, 5318(g), and 5331 of title 31, United States Code, including regulations issued under those sections, should be adjusted.
- Considerations. In making the determinations required under subsection (a), the Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall:
  - o Rely substantially on information obtained through the BSA Data Value Analysis Project conducted by FinCEN and on information obtained through the Currency Transaction Report analyses conducted by the Comptroller General of the United States; and
  - o Consider:
    - The effects that adjusting the thresholds would have on law enforcement, intelligence, national security and homeland security agencies;
    - The costs likely to be incurred or saved by financial institutions from any adjustment to the thresholds;
    - Whether adjusting the thresholds would better conform the United States with international norms and standards to counter money laundering and the financing of terrorism;
    - Whether currency transaction report thresholds should be tied to inflation or otherwise, be adjusted based on other factors consistent with the purposes of the Bank Secrecy Act;
    - Any other matter that the Secretary determines is appropriate.
- Report and Rulemakings. Not later than one year after the date of enactment of this Act, the Secretary, in consultation with the Attorney General, the Director of National Intelligence, the Secretary of Homeland Security, the Federal functional regulators, State bank supervisors, State credit union supervisors, and other relevant stakeholders, shall:

Today, banks must develop and implement an effective risk-based AML program consistent with rules that transcend roughly 50 years of banking.

  - o Publish a report of the findings from the review required under subsection (a); and
  - o Propose rulemakings, as appropriate, to implement the findings and determinations described in paragraph (1).
- Updates. Not less frequently than once every five years during the 10-year period beginning on the date of enactment of this Act, the Secretary shall:
  - o Evaluate findings and rulemakings described in subsection (c); and
  - o Transmit a written summary of the evaluation to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate; and
  - o Propose rulemakings, as appropriate, in response to the evaluation required under paragraph (1).

How will all this play out? Well, we'll have to wait and see. Hopefully, an increase in the reporting thresholds will bring some semblance of actual tangible benefits to financial institutions being burdened under the current BSA regulatory reporting structure. ◗

Steve Manderscheid brings over 25 years of financial industry experience to the Compliance Alliance team. Previously, he focused on all aspects of regulatory compliance risk management while also serving in a Bank Secrecy Act officer capacity. In recent years, he has ventured into leadership roles in enterprise-wide risk management (ERM), complaint management, and vendor and third-party relationships.

In his role as Compliance Officer, Steve brings all of his experience to completing reviews, and working on developing tools, training materials, and training events for our members. Recently, he's started expanding his educational role and has become the main presenter of our popular C/A Minute videos.

EDUCATION CALENDAR

Due to COVID-19, event schedules are subject to change. Please visit nebankers.org/education.html or call the NBA Education Center at 402-474-1555 for the most current event schedule.

FEBRUARY 2021

Operations Conference – Technology, Marketing, Retail Banking
February 24-25
Virtual Offering

MARCH 2021

Supervisor Bootcamp Conference
March 2, 4, 16, 18
Virtual Offering

Principles of Banking Seminar
March 9-10
Virtual Offering

Tri-State Marketing & Human Resources Conference
March 18-19
Virtual Offering

APRIL 2021

Spring Agri-Business Conference
April 6-7
Virtual Offering

School of Banking Fundamentals
April 26-30
Manhattan, KS

MAY 2021

NBA Annual Convention
May 5-7
LaVista, NE

NBA Nebraska Bankers Association

For more information about these live and online education events and training tools, contact the NBA Education Center at (402) 474-1555 or nbaeducation@nebankers.org. You also may visit the NBA website at https://www.nebankers.org/education.html.

Meet the New Members of the Nebraska Legislature

THE NEBRASKA LEGISLATURE INCLUDES EIGHT NEW FACES THIS YEAR, as the first session of the 107th Legislature convened Jan. 6, 2021. On these pages, you will find photos of Nebraska's newest state senators.

The Nebraska Bankers Association urges you to advocate on behalf of the banking industry in our state by building relationships with your state senator. If you don't know your state senator, make a point to meet and become acquainted with that person, and make sure he or she has your contact information. Relationship building is the first step to a strong grassroots legislative program — and the NBA is dedicated to providing its members with the support and resources to make it happen.

Learn how you can get involved at nebankers.org/legislation. Together, we can and do make a difference!

District 9 – Omaha

John Cavanaugh

- Lawyer, Douglas County Public Defender's office

District 11 – Omaha

Terrell McKinney

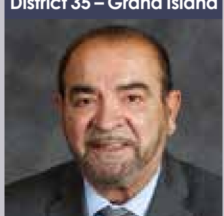
- Wrestling coach

District 29 – Lincoln

Eliot Bostar

- Board member, LES and Climate Resiliency Task Force

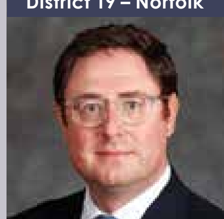
District 35 – Grand Island



Raymond Aguilar

- Retired
- Former senator (2008)

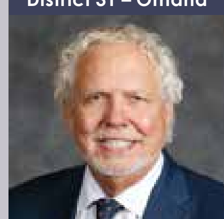
District 19 – Norfolk



Mike Flood

- Attorney and Owner of Flood Communications
- Former state senator and Speaker of the Legislature (2004)

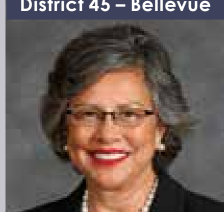
District 31 – Omaha



Rich Pahls

- Member, Omaha City Council
- Former state senator and Banking, Commerce and Committee Chairman (2013)

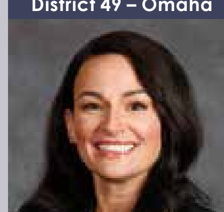
District 45 – Bellevue



Rita Sanders

- Former Bellevue Mayor

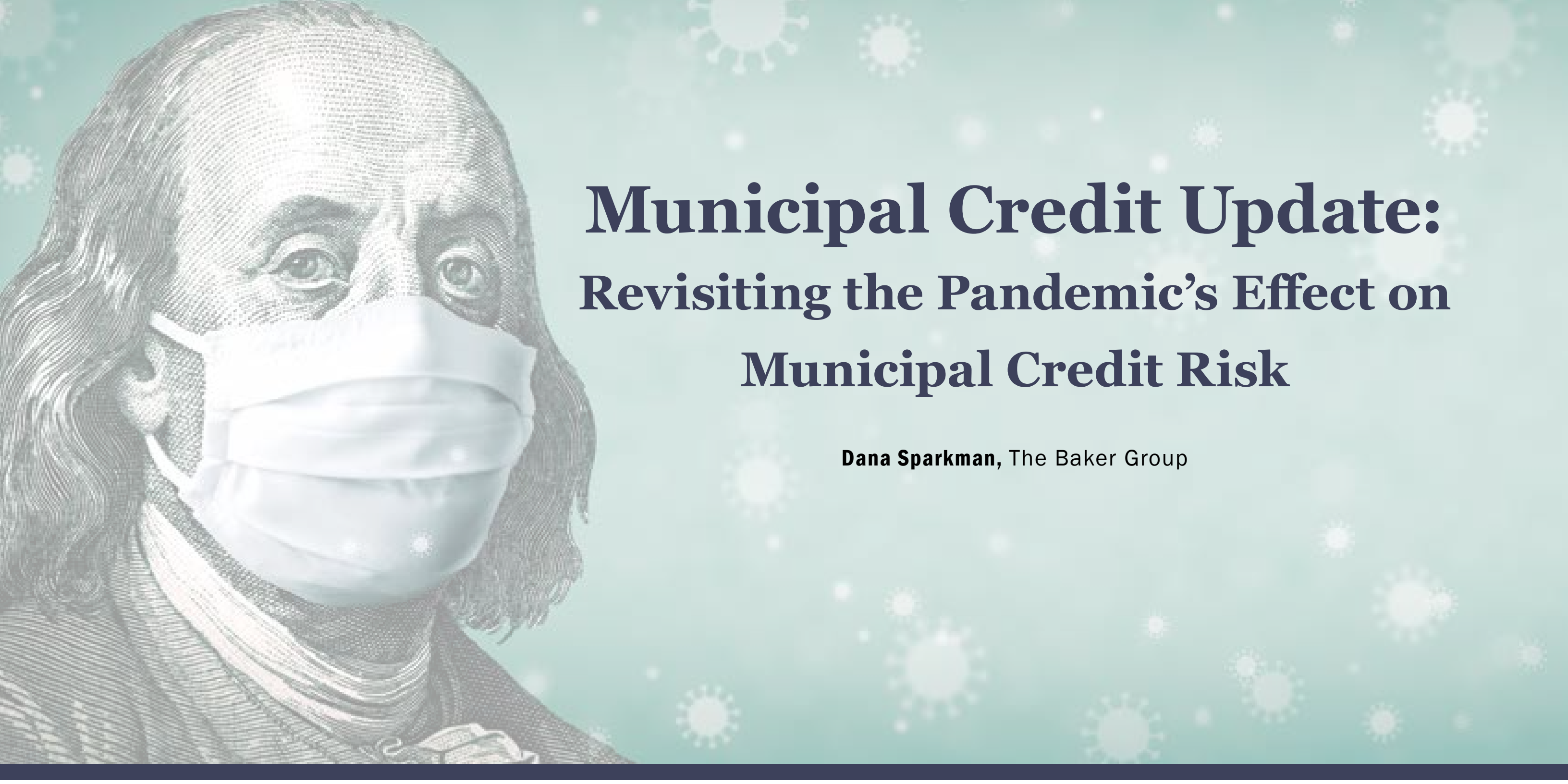
District 49 – Omaha



Jen Day

- Owner/Co-Founder, Artis Strength & Fitness/Artis Barbell

1	Sen. Julie Slama	Auburn
2	Sen. Robert Clements	Elmwood
4	Sen. Robert Hilkemann	Omaha
5	Sen. Mike McDonnell	Omaha
6	Sen. Machaela Cavanaugh	Omaha
7	Sen. Tony Vargas	Omaha
8	Sen. Megan Hunt	Omaha
9	Sen.-elect John Cavanaugh	Omaha
10	Sen. Wendy DeBoer	Bennington
11	Sen.-elect Terrell McKinney	Omaha
12	Sen. Steve Lathrop	Omaha
13	Sen. Justin Wayne	Omaha
14	Sen. John Arch	La Vista
15	Sen. Lynne Walz	Fremont
16	Sen. Ben Hansen	Blair
17	Sen. Joni Albrecht	Thurston
18	Sen. Brett Lindstrom	Lincoln
19	Sen.-elect Mike Flood	Norfolk
20	Sen. John McCollister	Omaha
21	Sen. Mike Hilgers	Lincoln
22	Sen. Mike Moser	Columbus
23	Sen. Bruce Bostelman	Brainard
24	Sen. Curt Friesen	Henderson
24	Sen. Mark Kolterman	Seward
25	Sen. Suzanne Geist	Lincoln
26	Sen. Matt Hansen	Lincoln
27	Sen. Anna Wishart	Lincoln
28	Sen. Patty Pansing Brooks	Lincoln
29	Sen.-elect Eliot Bostar	Lincoln
30	Sen. Myron Dorn	Adams
31	Sen.-elect Rich Pahls	Omaha
32	Sen. Tom Brandt	Plymouth
33	Sen. Steve Halloran	Hastings
35	Sen.-elect Raymond Aguilar	Grand Island
36	Sen. Matt Williams	Gothenburg
37	Sen. John Lowe, Sr.	Kearney
38	Sen. Dave Murman	Glenvil
39	Sen. Lou Ann Linehan	Elkhorn
40	Sen.-Elect Timothy Gragert	Creighton
41	Sen. Tom Briese	Albion
42	Sen. Michael Groene	North Platte
43	Sen. Tom Brewer	Gordon
44	Sen. Dan Hughes	Venango
45	Sen.-elect Rita Sanders	Bellevue
45	Sen. Carol Blood	Bellevue
46	Sen. Adam Morfeld	Lincoln
47	Sen. Steve Erdman	Bayard
48	Sen. John P. Stinner	Gering
49	Sen.-elect Jen Day	Omaha



Municipal Credit Update:

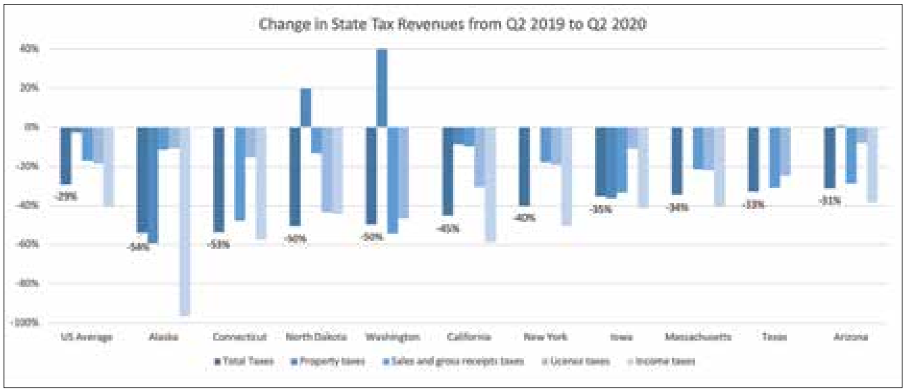
Revisiting the Pandemic's Effect on Municipal Credit Risk

Dana Sparkman, The Baker Group

"The potential impact of the COVID-19 pandemic on the City cannot be quantified at this time, but the continued outbreak of COVID-19 could have an adverse effect on the City's operations and financial condition."

THIS DISCLOSURE, OR SOMETHING like it, is now regularly included in documentation by municipal issuers. While we would love to have more details than that, the exact magnitude of the pandemic's repercussions on state and local finances still cannot be accurately determined.

However, we do have some clarity on the results of the 2020 fiscal year, given that most local government fiscal years close in June. The U.S. Census Bureau reports that total state tax revenue declined 29% in the second quarter of 2020 compared to the same quarter in 2019. The chart below exposes the states with the largest declines in total tax revenue when comparing Q2 2019 to Q2 2020. Most states did not cut funding to school districts in the 2020 fiscal year, but instead used one-time budgetary maneuvers to make ends meet. If state revenues continue to be depressed, they may be forced to make cuts across the board, including education. Vulnerability to state funding changes can be measured by analyzing the district's dependence on state funds relative to total revenues. Of course, further federal aid would mitigate this risk. Congress is working on ideas for more aid, but none have fully passed at this time. The HEROES Act, passed by the House October 1, 2020 but not yet by the Senate, contains $676 billion in funds for state and local governments with $208 billion specifically allocated for education spending. The HEROES Act comes with an important restriction: states may not cut their budgets for education spending, which will help to further protect school districts from state funding cuts if enacted.



Source: U.S. Census Bureau

Also, the National League of Cities reveals that all major local tax revenue sources slowed with severe declines in sales and income tax receipts. Sales tax revenue dropped by 11% on average in the 2020 fiscal year. Property tax revenue continued to grow, but the growth rate slowed compared to 2019 and may continue to slow and even decline in 2021 and 2022 depending on economic conditions. Property tax trends are slow to follow economic fluctuations because assessed valuations are typically set well in advance of the actual bills being due, and changes in assessed valuations are often more muted than changes in market value due to caps on assessed valuation increases and other calculation considerations. However, the longer the economy remains depressed, the more likely it is that home prices will deteriorate and cause declines in property tax revenue absent rate increases.

Certain downtown areas and other once busy areas that are now much emptier because of people working from home may be particularly susceptible to property tax revenue declines as demand for those expensive commercial spaces lessens, especially if the work-from-home trend remains after the pandemic ends. Some large cities may even experience de-urbanization if people choose to relocate to smaller cities in favor of more space and, in some cases, less taxes. According to LinkedIn, New York City and the San Francisco Bay Area both recently experienced steep declines in their inflow-to-outflow ratios with both cities losing more people than they gained while smaller cities like Jacksonville and Salt Lake City experienced net gains in new residents.

Looking forward to the 2021 fiscal year, many questions linger. Cities and states are anticipating an even larger decline in general fund revenues than they experienced during 2020, reserve levels have lessened from pre-pandemic levels, and it is not clear when or if events and gatherings may resume regular schedules. Investors must continue to diligently monitor their holdings for potential credit deterioration as outlined in our earlier Municipal Credit Update concerning the COVID-19 pandemic. ◗

(link: https://www.gobaker.com/municipal-credit-update-managing-credit-risk-amid-the-covid-19-pandemic/)

Dana Sparkman, CFA, is Senior Vice President/Municipal Analyst in The Baker Group's Financial Strategies Group. She manages a municipal credit database that covers more than 150,000 municipal bonds, providing clients with specific credit metrics essential in assessing municipal credit. Dana earned a bachelor's degree in finance from the University of Central Oklahoma as well as the Chartered Financial Analyst designation. Contact: 405-415-7223, dana@GoBaker.com.

ADVERTISER INDEX

JFC Financial Services
Comprehensive Wealth Management

EXPERTS AT **SUPPORTING** FINANCIAL INSTITUTIONS

TAKE YOUR FINANCIAL INSTITUTION TO A WHOLE NEW LEVEL OF SUCCESS

The JFC Financial Services Difference:

- ✓ Provide customers with a platform where all their financial needs are met
- ✓ Increase operating margins as well as your bottom line
- ✓ Gain more of your customers' assets by offering new products
- ✓ Acquire new customers and cross-sell traditional banking products
- ✓ Provide robust wealth management solutions
- ✓ Build high-end referral to your bank

CALL JFC FINANCIAL SERVICES

800-262-9538

LEARN HOW TO INCORPORATE A PROFITABLE INVESTMENT PROGRAM IN YOUR BANK!

9060 Andermatt Drive, Suite 10
Lincoln, NE 68526

www.joinjfc.com

@jfc-financial-services

@JFCFinancial

NBA Nebraska Bankers Association
233 South 13th Street, Suite 700
Lincoln, NE 68508

PRSRT STD
U.S. POSTAGE
PAID
SALT LAKE CITY, UT
PERMIT NO. 508

This magazine is designed and published by The newsLINK Group, LLC | 855.747.4003