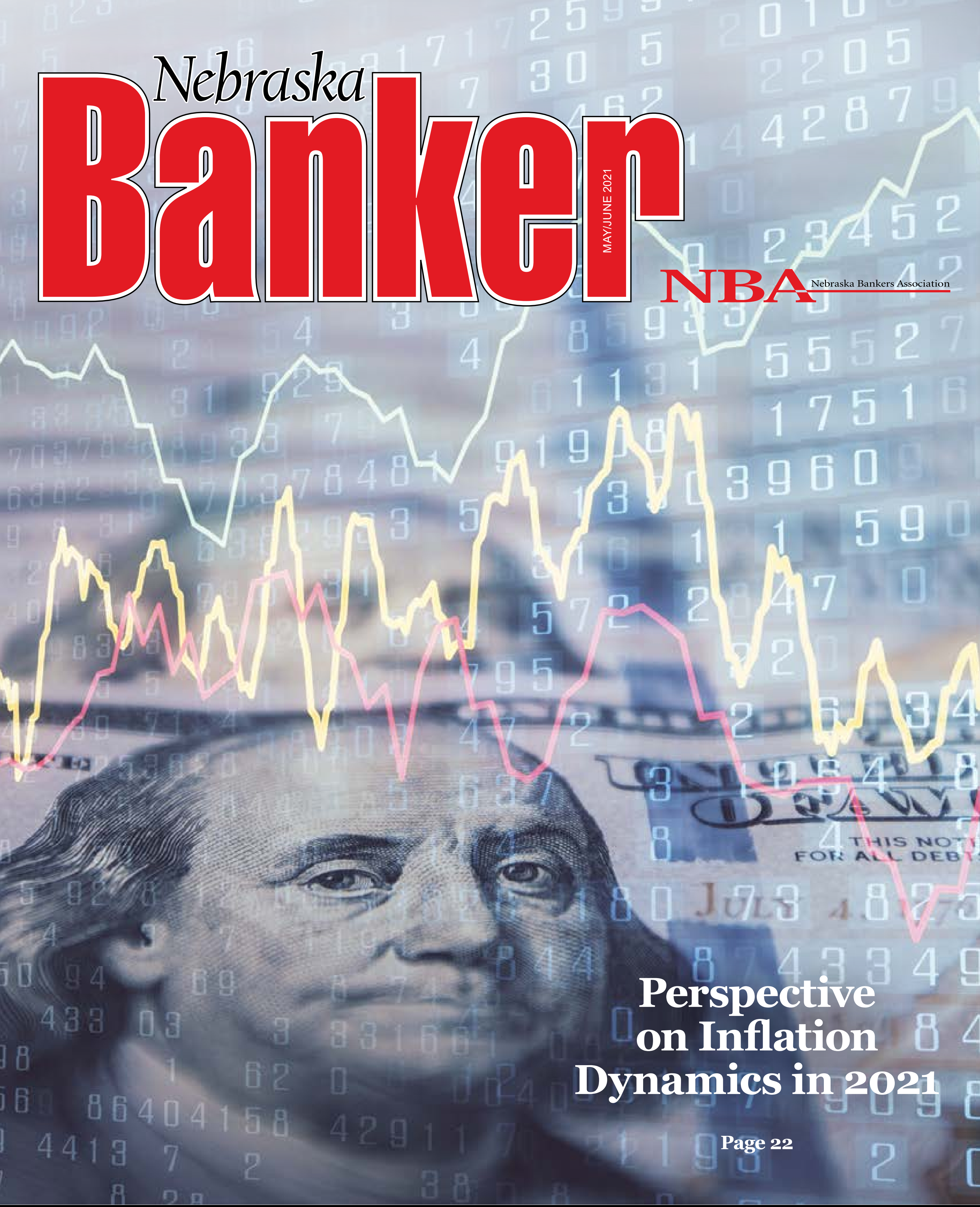


Nebraska Banker

MAY/JUNE 2021

NBA Nebraska Bankers Association

Perspective on Inflation Dynamics in 2021

Page 22

OFFICIAL PUBLICATION OF THE NEBRASKA BANKERS ASSOCIATION

CONTENTS

Nebraska Banker
MAY/JUNE 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 bimonthly publication in May 2006, is included in membership fees to the NBA.

NBA BOARD OF DIRECTORS

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

STEPHEN STULL
NBA Chairman-Elect
(402) 792-2500
Farmers State Bank
Dodge

KATHRYN BARKER
(402) 333-9100
Core Bank
Omaha

NICHOLAS BAXTER
(402) 341-0500
First National Bank of Omaha
Omaha

CORY BERGT
(402) 434-4321
Wells Fargo Bank, N.A.,
Lincoln

JOHN BOTHOF
(402) 334-0300
Northwest Bank
Omaha

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

JUSTIN DOUGLAS
(402) 864-4191
Mainstreet Bank
Cook

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

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

KIM HAMMES
(402) 918-2332
Bank of the West
Omaha

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

CURTIS HEAPY
(308) 367-4155
Western Nebraska Bank
Curtis

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

ZACHARY HOLOCH
(402) 363-7411
Cornerstone Bank
York

DONALD JIVIDEN
(402) 759-8113
Heartland Bank
Geneva

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

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

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

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

RYNE SEAMAN
(402) 643-3636
Cattle Bank & Trust
Seward

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

DAN SVEHLA
(402) 323-1828
Union Bank & Trust Co.
Lincoln

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

SCOTT ZIMBELMAN
(308) 784-2000
Homestead Bank
Cozad

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

NBA EDITORIAL STAFF

RICHARD 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


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

Richard Baier, President and CEO, Nebraska Bankers Association

NBA FRIENDS:

Each year, the month of May not only shepherds in warmer days, greener grass and thoughts about golf, baseball, boating, etc., but it also brings the start of a new NBA fiscal year. Like you, I am more than happy to turn the page on our last fiscal year, which will go down in history as the lost pandemic year. Despite the many trials and tribulations we experienced over the past 12 months, Nebraska's banking industry served as a positive light and ray of hope in what many characterize as a very dark time in our country. Your NBA also successfully navigated these challenges while serving as the primary advocate and resource for Nebraska's banking industry.

I would be remiss if I did not begin my annual reflection with a special thanks to outgoing NBA Chairman Chris Hove. When Chris agreed more than two years ago to step into the NBA leadership, none of us could have imagined the enormous personal and professional hurdles the pandemic would create. On behalf of our entire membership, I want to thank Chris for his leadership, flexibility, counsel and support.

As the pandemic kicked into high gear last spring, Nebraska banks were on the front line, working with customers and communities. Members also teamed up with various regulatory agencies and our elected officials to implement government economic programs aimed at leveling out the economic crisis that evolved on the heels of the COVID-19 health crisis. Between 2020 and 2021, Nebraska banks collectively made more than 114,800 Paycheck Protection Program (PPP) loans totaling more than $5.38 billion in assistance to Nebraska small businesses.

Your NBA team worked closely with our member banks to address program questions, seek clarification when possible, and raise issues of importance with our congressional delegation and the Small Business Administration. I recently talked with a well-known restaurant owner who advised me that he would have lost his business of more than 30 years without his PPP loan and the hard work of his Nebraska bank. The NBA marketing team worked closely with an outside marketing firm to roll out the #BanksBankNE video campaign featuring stories from five diverse PPP recipients. These videos and related media placement generated over 580,000 impressions on social media.

Your NBA education team quickly moved programs and training to virtual platforms to ensure that our members continued to be well-informed and ready to assist their customers amid ongoing economic and regulatory swings. While the pandemic drastically changed the world of professional education, the NBA continues to evaluate the best methods to deliver top-notch training at affordable prices, whether that be in-person, virtual or some combination. Based upon member input and dialogue, the NBA looks forward to in-person training programs returning in August with the Young Bankers of Nebraska Conference in La Vista.

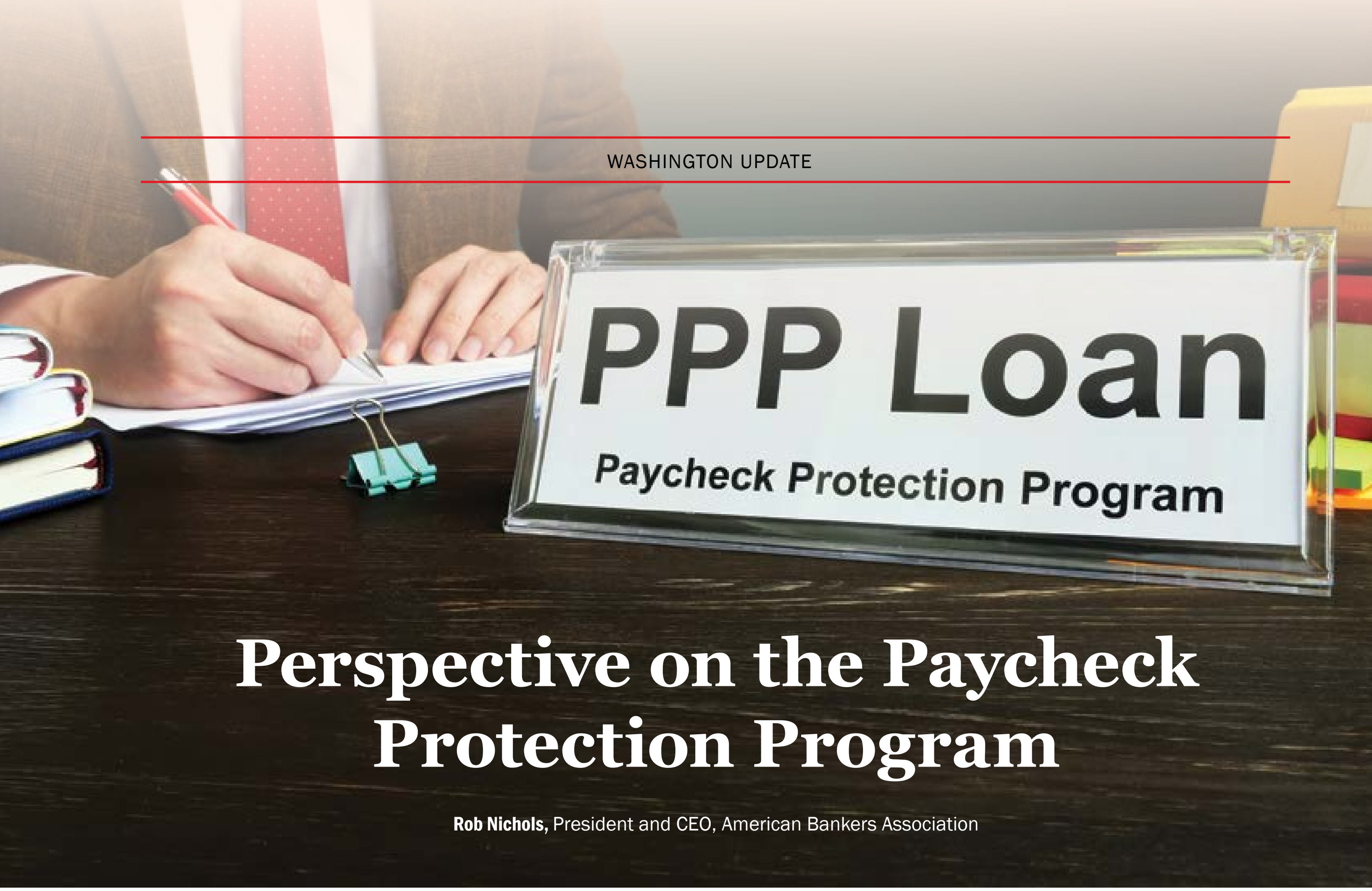
While PPP consumed a huge amount of NBA staff time, your NBA government relations team also lobbied extensively on numerous state and federal legislative issues. In Nebraska, your lobbying team actively developed several affirmative banking-related initiatives. Three of these four proposals were passed by the legislature before adjournment on May 27, 2021. The NBA also actively supported the passing of LB 452, which outlines financial literacy curriculum requirements for Nebraska's K-12 schools, including a semester-long personal finance class as a graduation requirement. Finally, your NBA team worked closely with members of the legislature to amend and refine legislation (LB 649) to create a new Digital Asset Bank Charter in Nebraska. Our team provided a yeoman's effort to slow this proposal down and offer a multitude of amendments to better protect the banking industry and our fellow Nebraskans. I will address this issue more closely in future columns.

Following is a sampling of additional activities which reflect the accomplishments of your NBA over the past year:

- All 166 member banks renewed their membership.
- 85% of all Nebraska banks participated in the NBA VEBA health insurance.
- NBA VEBA provided insurance coverage to more than 10,000 Nebraskans.
- Through NBA philanthropic efforts, we awarded more than $153,000 in higher education scholarships and support.
- NBA officers conducted more than 20 regional and national media interviews.
- NBA member banks raised nearly $150,000 in industry contributions to support the NBA State and Federal Political Action Committees.
- 15 Nebraska banks are active participants in the new Single Bank Pooled Collateral Program, covering more than $1.3 billion in public deposits.
- The Robbery Reward Fund paid out more than $40,000 through for tips leading to the arrest of bank robbers.
- The NBA rolled out, in cooperation with Compliance Alliance, new compliance audit and virtual compliance officer services.
- Completed renovations and upgrades to the NBA offices in September 2020
- Your NBA experienced an extremely strong financial year which allowed for 20% membership rebates.

While the pandemic has impacted many aspects of our lives, I am extremely proud of the role our member institutions and the NBA played in navigating these unchartered waters while planning for the future!

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



Perspective on the Paycheck Protection Program

Rob Nichols, President and CEO, American Bankers Association

AT THE END OF MAY, THE GOVERNMENT'S PAYCHECK Protection Program came to a close. If Congress does not extend the program, we can expect the "Monday morning quarterbacking" about the program's impact on the economy, its design and implementation, and its ultimate cost to begin. Those are appropriate questions to ask as we consider the lessons learned from the nation's response to the coronavirus pandemic.

Here's what I know already: The biggest small business rescue program in U.S. history would have been an unmitigated failure without the extraordinary efforts of America's banks and their dedicated employees. It would never have produced the positive results it did without the incredible collaboration between ABA and our state association alliance partners.

It's easy to forget what the world was like when PPP first launched in April 2020. The nation's economy had largely shut down, many Americans were isolated in their homes, and businesses of all sizes were dealing with the stark new reality posed by COVID-19.

Banks across the country were trying to figure out how to keep the banking system fully functioning in the middle of a global pandemic and how to help their customers survive the economic disruption while also trying to figure out how to protect the health and safety of their employees and customers from an invisible threat.

It was against that backdrop that the federal government asked banks and other financial institutions to help the Small Business Administration launch the Paycheck Protection Program. On paper, the program dwarfed any previous SBA lending program in its history, and the agency was asked to launch it within days of lawmakers passing the CARES Act.

That launch, to be generous, did not go perfectly. SBA's technical systems, built for its more traditional 7(a) lending program, could not handle the incredible load demanded by a program of this scale. The agency staff was overwhelmed and was slow in issuing the guidance banks needed to begin processing loans, and the guidance they did release was sometimes contradictory.

From the start, ABA and our state association alliance partners encouraged banks to step up and participate in PPP despite all the obstacles, and step up you have. As of April 11, banks were responsible for 80% of the nearly 9.6 million PPP loans so far and 93% of the $755 billion in PPP funding. I am particularly pleased to see how banks of all sizes supported the program. From our largest members to our smallest, the commitment to our small business customers has been truly remarkable. We have been united in this effort.

Banks were able to step up because ABA, working with our state association partners, was able to keep members informed on the program and its many iterations. In daily Zoom calls in the early months of the pandemic, state association executives served as an early warning system, keeping us updated on operational issues popping up, which we relayed back to SBA. Meanwhile, ABA provided members and state associations the latest SBA changes in real time.

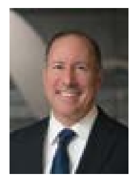
At one point, ABA hosted a PPP webinar for bankers, only to find that SBA employees in some parts of the country were trying to register. We came to learn that they were getting better information about PPP from ABA and the state associations than they were from SBA headquarters.

ABA and the state associations also partnered on targeted ad campaigns to encourage minority- and women-owned businesses to consider applying for PPP loans. This partnership was just one of many industry initiatives to ensure PPP funds reached every business that needed them.

PPP will always have its critics. Some people remain fixated on the large businesses and public companies that applied in the first wave, only to be shamed into returning PPP funds. To be fair, many of those businesses met the initial eligibility requirements set by Congress. Government watchdogs remain rightfully concerned with inexcusable examples of fraud and abuse, many spotted by banks working with law enforcement.

Others have suggested that banks earned a windfall from PPP. The reality is that for most banks, the cost of diverting staff from other lines of business to reset systems and oversee this massive new program made PPP lending a break-even business at best. And yet, all of those bankers also tell me they would participate again under similar circumstances because supporting PPP was the right thing to do for their customers, communities and the country.

I am hopeful we won't need another small business rescue program anytime soon. If we do need another PPP, please rest assured that we have learned some valuable lessons, and ABA and our state association alliance partners will once again be with you every step of the way.



Email Rob Nichols at rnichols@aba.com.

Proactive Affirmative Defense Laws Protect Companies From Litigation

Robert Kardell, Attorney, Baird Holm LLP

IN 2013 -2014, THE NATIONAL INSTITUTE OF STANDARDS AND Technology (NIST) adapted the widely used government standards of NIST 800-53 for the private sector by creating and publishing the Cyber Security Framework (CSF). The CSF provided a method for private companies to complete an assessment and adopt relevant portions of the NIST standards for their own use. Soon after, the Federal Financial Institutions Examinations Council (FFIEC) created the Cybersecurity Assessment Tool map NIST and CSF standard for banks. This framework helped banks implement cybersecurity to protect their assets and information.

Until recently, the adoption of NIST, or other recognized standards, was a good defensive legal posture. But now, the adoption of such standards can be a proactive step in establishing a legal safe harbor from lawsuits. By promoting these new laws as a legal safe harbor, the laws become incentives to adopt recognized cybersecurity standards.

Cyber attacks have become commonplace across all business lines including financial, health care, insurance, retail industry and general businesses. In 2020, the number of cyber attacks increased again due to COVID and the vulnerability of remote workers. For the banking industry, the threats and the costs of recovery are higher than all but health care. On average, banks face 85 serious attempts a year to penetrate their network, and approximately 36% of these attempts result in some data being stolen.[1] Banks also have the second-highest cost per record (second to health care) to recover from a breach.[2]

Cyber attack victims not only endured the expense of recovery from a cyber breach, but they have also endured attacks from zealous plaintiff's attorneys. As if banks are not paying enough money for cybersecurity, monitoring and recovery costs, the costs are even greater if they are forced to defend themselves in an ensuing class-action lawsuit.

But there is a new trend among legislators to protect businesses from cybersecurity lawsuits. Several newly enacted laws provide safe harbors for companies who have written cybersecurity polices and have taken the necessary steps to protect their data. Utah became the second state to provide safe harbor protections, and the federal government has provided some protection as well.

State Safe Harbor Laws

A new Utah law is entitled the Cybersecurity Affirmative Defense Act (HB80) and it amends Utah's data breach notification statute. This new law provides an affirmative defense for companies facing lawsuits which allege:

- The company failed to implement reasonable information security;
- The company failed to appropriately respond to a data breach; or,
- The company failed to appropriately notify affected individuals.

The law, however, only provides an affirmative defense if the company can prove:

- They created and maintained a written cybersecurity program;
- The program reasonably complied with a recognized cybersecurity framework;
- The framework was in place at the time of the breach;
- The cybersecurity program had protocols for responding to a breach of system security; and,
- The company followed the protocols.[3]

The law defines a cybersecurity program as one which reasonably conforms with frameworks such as:

- National Institute of Standards and Technologies (NIST) frameworks such as 800-53, 800-171:
- Federal Risk and Authorization Management Program Security Assessment Framework (FedRAMP);
- Center for Internet security (CIS) critical security controls; or the
- International Organization for Standardization (ISO) 27,000 family of controls.

In 2018, Ohio passed a similar statute.[4] The Ohio law provides for an affirmative defense for businesses that:

> Create, maintain, and comply with a written cybersecurity program that contains administrative, technical, and physical safeguards for the protection of personal information and that reasonably conforms to an industry recognized cybersecurity framework.[5]

There is some flexibility in these statutes. Companies are not forced to adopt and implement an entire framework, but rather they need only reasonably comply. Both statutes allow companies to customize their policy and tailor their approach. Utah and Ohio allow businesses to tailor their approach using criteria such as:

- The size and complexity of the entity;
- The nature and scope of the activities of the entity;
- The sensitivity of the information to be protected;
- The cost and availability of tools to improve information security and reduce vulnerabilities; and
- The resources available to the entity.[6]

The flexibility in this approach recognizes the limitations to small or medium-sized organizations' resources while still providing protections from litigation.

Connecticut is also considering a similar statue.[7] The proposed Connecticut law offers an affirmative defense if:

> [The] covered entity created, maintained and complied with a written cybersecurity program that contains administrative, technical and physical safeguards for the protection of personal or restricted information and that conforms to an industry recognized cybersecurity framework.[8]

The Connecticut law outlines a similar set of cybersecurity frameworks, such as NIST, ISO or FedRAMP, and, like Utah and Ohio, allows flexibility based on size and complexity of the organization, sensitivity of the data, cost and availability of tools and the resources of the entity.

Federal Safe Harbor Laws

Earlier this year, the federal government passed, and the president signed into law, the so-called HIPAA Safe Harbor

COUNSELOR'S CORNER — continued on page 14

COUNSELOR'S CORNER — continued from page 13

bill.[9] Under prior HIPAA/HITECH laws, an organization could face fines, audits, or the imposition of remediation remedies for cyber breaches and determined and imposed by the Secretary for the Department of Health and Human Services (HHS). Often health care organizations would argue, to no avail, that they had implemented all the cybersecurity measures they could afford to protect their information and their network, but they still suffered a cyber attack. The reality is that large organizations have very capable cybersecurity staff, but, despite their efforts and skill in defending their network, the exploitation of a single zero-day vulnerability or a single phishing email may expose a significant amount of sensitive data.

Under this new federal law, HHS may reduce fines, reduce imposed remedies or terminate an audit. The organization only need demonstrate that it had, for the prior 12 months, security practices in place that meet certain cybersecurity standards. These cybersecurity standards are defined as NIST, the Cyber Security Act of 2015, or other recognized cybersecurity programs developed by private industry.

Implications for Banking

The FFIEC established a framework for banking through the Cybersecurity Assessment Tool ("CSAT"). In the CSAT the FFIEC offers a baseline of declarative statements. These declaratives statements are then mapped to the FFIEC IT Examination Handbook and to the NIST standards. To date, none of the safe harbor laws directly recognize the CSAT as a framework, but, as an example, the Utah law allows the following:

> (ii) reasonably conforms to the current version of any of the following frameworks or publications, or any combination of the following frameworks or publications:
>
> (A) NIST special publication 800-171;
>
> (B) NIST special publications 800-53 and 800-53a;

The mapping provided by the FFIEC in Cybersecurity Assessment Tool[10] provides a direct correlation between the CSAT and the NIST standards. This correlation can provide banks with a strong basis for claiming benefits of such safe harbor provisions.

Conclusions

State and federal legislatures are recognizing the need to protect and incentivize companies for good cybersecurity. They are providing these incentives through safe-harbor laws. These laws recognize that businesses of all sizes have become victims of cyber attacks even after implementing robust cybersecurity protocols. These laws both incentivize the adoption of cyber frameworks and provide litigation safe harbors. These laws are the newest trends in cybersecurity law and banks, and companies of all sizes can take advantage of the safe harbors by adopting and implementing nationally recognized frameworks. Such measures will protect companies from overly litigious clients and customers. Banks can, and should, include direct references to recognized NIST standards in their own policies to protect their organizations as more such laws are surely on the horizon.

[1] ComputerWeekly.com, "Banks face daily cyber-attacks, many of which succeed in stealing data, research finds", https://www.computerweekly.com/news/450417135/Banks-suffer-average-of-85-attempted-serious-cyber-attacks-a-year-and-one-third-are-successful, last visited April 29, 2021.

[2] IBM and The Ponemon Institute, "2019 Cost of a Data Breach", https://www.ibm.com/security/data-breach last visited on April 29, 2021.

[3] Cybersecurity Affirmative Defense Act (HB80), Utah Code § 78B-4-702

[4] Ohio Revised Code Section 1354, "Businesses Maintaining Recognized Cybersecurity Programs".

[5] Id at (A)(1)

[6] Id at (C), and similar to Utah 78B-4-702 (4)(c)

[7] Connecticut General Assembly, H.B. No. 6607, "AN ACT INCENTIVIZING THE ADOPTION OF CYBERSECURITY STANDARDS FOR BUSINESSES"

[8] Id at (B)

[9] H.R. 7898, Public Law 116-321, to amend 41 USC Sec. 17931 et seq., officially titled "To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes."

[10] https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_App_B_Map_to_NIST_CSF_June_2015_PDF4.pdf, last visited on May 1, 2021.

Robert Kardell, Attorney, Baird Holm LLP

Should You Consider a vCISO Solution?

Shane Daniel, CPA, CISA, CIA, Information Security Consultant, SBS CyberSecurity, LLC

A Tested Solution to a Modern Problem

The strategic use of contracted resources to perform activities traditionally handled by internal staff and resources is a commonly used definition of business outsourcing. While the term vCISO (virtual chief information security officer) is a rather new designation for those in the C-suite, the solution model is rather mature.

What do vCISO arrangements look like?

vCISO outsourcing arrangements may take many varieties and are used by organizations of all sizes and sectors. The contracted service can be as limited as assisting information security staff with an assignment in which they lack expertise. Other outsourcing arrangements may call for the vCISO to perform all or several parts of the information security program. Under these arrangements, the organization should maintain an information security coordinator to supervise consulting activities adequately.

What are the benefits of hiring a professional expert?

1. **Avoiding an Extended Recruitment Process** — Even when offering competitive compensation, recruiting a CISO may take time and a significant monetary investment. Using a vCISO service provides immediate access to a team of cybersecurity experts, thus skipping a potentially lengthy, costly and risky recruitment process.
2. **Varied Professional Knowledge** — The skillset and knowledge base required for an effective information security program is constantly changing. Not only are professional consultants and advisors more apt to obtain and maintain professional certifications, but these individuals are also highly likely to be performing a similar role with other clients in your industry. That experience provides a consultant with an expansive skill set and unique perspective of best practices and trends.
3. **Establishing a Fixed Cost** — Using a contracted vCISO service solution allows the opportunity to fix the labor costs of information security over the term of the contract, locking in a predictable cost over the contract term.
4. **Providing Measurable Deliverables** — A prolonged recruitment process and training period will delay the organization's response time to address

As you scrutinize whether or not a vCISO solution is an appropriate fit for your organization, keep in mind that the security and protection of your organization's and your customer's information are ultimately up to you.

critical cybersecurity needs. An experienced vCISO service solution utilizing an established methodology can close the response gap and reduce the impact of future employee turnover and future information security gaps while improving examination and audit results.

5. **Establishing an Information Security Culture** — The vCISO can be a central part of your leadership team and provide insight to develop the organization's information security culture. Contingent on the company you choose to partner with, the consultant may be available for IT committee and board meetings.
6. **Training Staff to Safeguard the Organization's Information** — An important responsibility of a vCISO includes strengthening employee understanding of cyber risk. This can include holding workshops to establish basic cybersecurity etiquette, communicating important security tips, making sure employees are using adequate passwords, and training employees on the proper use of multifactor authentication (MFA).

What to consider before choosing a vCISO provider?

Prior to entering into an outsourcing arrangement, an organization should perform due diligence to ensure that the consulting firm has sufficient expertise and qualified staff members to perform the intended work. Since the arrangement is a professional services contract, the organization should be confident in the competence of the consulting firm and staff. The proposal of service should:

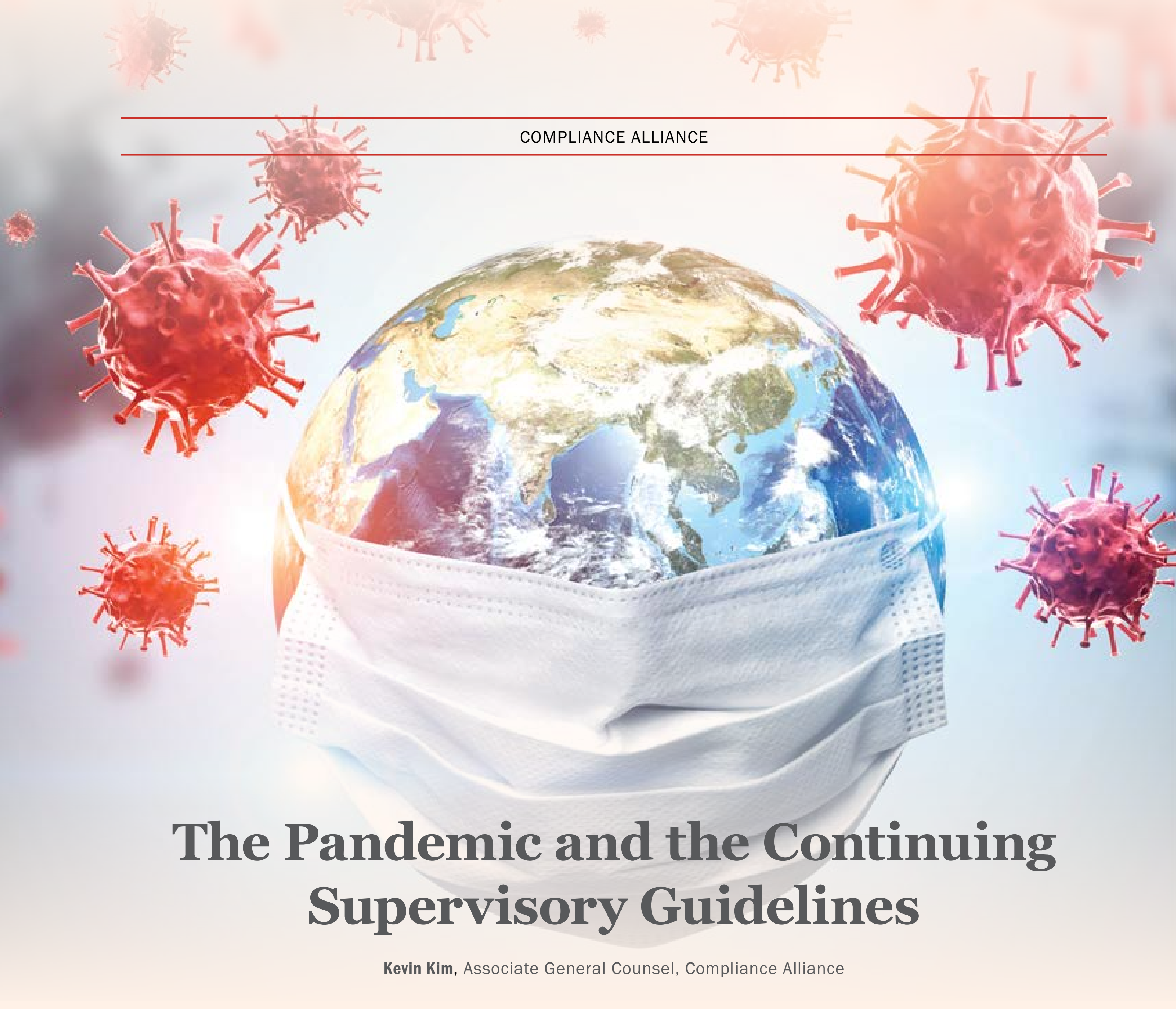
- Define the expectations and responsibilities for both parties.
- Set the scope, frequency, and cost of work to be performed by the consulting firm.
- Set responsibilities for providing and receiving information, such as the manner and frequency of reporting to senior management and the board of directors about the status of contract work.
- Establish the protocol for changing the terms of the service contract, especially for expansion of consulting work if significant issues are found.
- State that any information pertaining to the organization must be kept confidential.
- Specify the locations of deliverables.
- Specify the period that deliverables will be maintained.
- State that services provided by the consulting firm may be subject to regulatory or audit review and that examiners or auditors will be granted full and timely access to the deliverables and related work papers prepared by the consulting firm.
- Define whether the consulting firm will or will not perform management functions, make management decisions, act or appear to act in a capacity equivalent to that of an employee or a member of management of the organization, and comply with applicable professional and regulatory guidance.

A Complete Solution

Organizations cannot pursue partial solutions to solve multifaceted issues such as regulatory compliance or cybersecurity risk and expect success. A well-designed vCISO approach will permit an organization to fulfill or complement information security management without burdening current staff, enabling the organization to grow the business, stay ahead of threats, address annual compliance needs and exceed regulatory expectations.

As you scrutinize whether or not a vCISO solution is an appropriate fit for your organization, keep in mind that the security and protection of your organization's and your customer's information are ultimately up to you. However, a good vCISO can truly guide you to make better cybersecurity decisions and do what is right to protect your organization.

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, auditing, network security and education. Learn more at sbscyber.com.



The Pandemic and the Continuing Supervisory Guidelines

Kevin Kim, Associate General Counsel, Compliance Alliance

On March 9, 2020, the Federal Deposit Insurance Corporation (FDIC) issued guidance encouraging financial institutions to assist customers and communities affected by COVID-19. With the Coronavirus Aid, Relief and Economic Security (CARES) Act, many banks were faced with their own set of challenges. During this time, many banks took steps to assist consumers, including allowing loan modifications with no fees, waiving fees on accounts and offering in-home banking services. Many were also participating in providing Paycheck Protection Program (PPP) loans to small businesses. Because of these accommodations, many banks struggled with high volumes of COVID-related mortgage requests and questions from customers and PPP loans. Banks were overcoming these overwhelming volumes while also maintaining their efforts to keep the physical locations of the banks safe for both customers and the employees. Through these difficult times, financial institutions created and revised policies and procedures to adjust and provide excellent service to customers.

Throughout the pandemic, the FDIC shifted to conduct all consumer compliance examinations and industry meetings virtually. At the beginning of the pandemic, the FDIC paused examination activities to allow financial institutions to focus on meeting the needs of their customers. As the examinations resumed, the FDIC allowed flexibility in scheduling to accommodate the institution's needs. There were some hurdles in the earlier stages due to operational and staffing challenges that limited the ability of management to respond to supervisory requests because of the shift to the virtual examinations. However, the FDIC was still able to conduct all consumer compliance and Community Reinvestment Act

(CRA) examinations within the timeframes established by the FDIC policies.

The most common violations during the 2020 examinations involved: the Truth in Lending Act (TILA), Truth in Savings Act (TISA), Flood Disaster Protection Act (FDPA), Electronic Funds Transfer Act (EFTA), and the Real Estate Settlement Procedures Act (RESPA). The FDIC uses a risk-focused methodology in conducting its compliance examinations, and the most frequently cited violations typically involve regulations that represent the greatest potential harm to consumers. The FDIC initiated eight formal enforcement actions and 16 informal enforcement actions to address consumer compliance examination findings. The total voluntary payments to consumers totaled approximately $7.4 million to more than 67,000 consumers.

RESPA Section 8(a) prohibits giving or accepting a thing of value for the referral of settlement service business involving a federally related mortgage loan. The FDIC continued to find RESPA Section 8(a) violations involving illegal kickbacks disguised as above-market payments for lead generation, marketing services, and office space or desk rentals. Paying for leads is acceptable, but paying for a referral is prohibited. To distinguish between the two, examiners look to whether the person providing the lead/referral was merely giving information about a potential borrower to a settlement service provider or if was a person was “affirmatively influencing” a consumer to select a certain provider. “Affirmative influence” means recommending, directing or steering a consumer to a certain provider. Often, true leads are lists of customer contacts that are not conditioned on the number of closed transactions resulting from the leads or any other considerations, including the endorsement of a settlement service.

To mitigate the risks associated with RESPA violations, banks could provide training to executives, senior management, and staff responsible for, and involved in, mortgage lending operations. Banks can also perform due diligence when considering new third-party relationships for whom the bank, or any individuals employed at or under contract to the bank, that generate leads or identify prospective mortgage borrowers. Lastly, the bank could develop a monitoring process for identifying, assessing, documenting, and reporting executive and senior management risks.

The TILA RESPA Integrated Disclosure Rule (TRID) rule also led to many violations. The Loan Estimate helps consumers understand the key features, estimated costs, and risks of the mortgage loan for which they are applying. The Closing Disclosure helps consumers understand all of the actual costs of the transaction and provide them with the opportunity to review costs and resolve any problems before closing. Under the TRID rule, the Loan Estimate is based on the “best information reasonably available” at the time the disclosures are provided to the consumer, and the bank must exercise due diligence in obtaining this information. The Closing Disclosure is based on an accurate disclosure standard. The FDIC found multiple instances involving Veteran Administration Loans where banks failed to comply with the “best information reasonably available” and due diligence standards under TRID by issuing Loan Estimates based on unavailable interest rates and loan terms. Additionally, examiners found potentially deceptive practices when banks represented certain terms for loans that were not generally available.

Mitigating risks for TRID violations also includes providing training to executives, senior management, and

Compliance Alliance — continued on page 20

Compliance Alliance — continued from page 19

staff responsible for, or are involved in, mortgage lending operations. Additionally, the bank should establish policies and procedures to help the staff comply with regulatory requirements when preparing disclosures. Finally, the bank should also consider implementing a centralized process to complete or review disclosures to ensure accuracy.

Fair lending was also a big concern when evaluating bank compliance. During the 2020 examinations, the FDIC found a bank that would automatically deny applicants under 30 years of age. Furthermore, the source of income was provided using a drop-down menu and any applicant who did not choose employment was denied. There was another case where a credit-scoring model scored younger applicants more favorably than it scored elderly applicants. It also negatively considered applicants who were on maternity leave. Additionally, there was a bank policy that provided the loan officer should use the highest credit score of the two applicants when the applicants were married, but the primary applicant's credit score would be used when the joint applicants were unmarried.

To address the fair lending risks, banks could consider regularly reviewing credit policies to ensure the Equal Credit Opportunity Act and Regulation B permit such considerations. The FDIC finds that a strong compliance management system helps ensure that financial institutions treat consumers more fairly. Moreover, the bank should review any filers or other criteria used for online leads, website applications, and credit scoring models.

With such an unprecedented pandemic sweeping across the nation, many areas needed adjustments to adapt to the changing environment. Regardless of the impact of COVID-19, banks should continue to set up and monitor compliance programs to ensure that the banks are complying with the appropriate regulations for their business activities.

Kevin Kim, associate general counsel, joined Compliance Alliance after graduating from the Benjamin N. Cardozo School of Law in 2019. He currently serves our members as one of our hotline advisers, where he spends his days guiding our members and writing articles for our weekly and monthly publications. Before C/A, he worked at Galaxy Digital and Refinitiv (formerly Thomson Reuters Financial and Risk) as a law clerk. He also opened a cryptocurrency mining farm, and founded an after-school program business in his native New York City. His unique experience and outlook have brought an invaluable new dimension to our group.

Perspective on Inflation Dynamics in 2021

Jeffrey Caughron, Managing Director, The Baker Group

The Fear

There is growing concern that the trillions of dollars of stimulus created by governments and central banks to fight the economic fallout of the coronavirus will explode through the economy and cause a surge in inflation in the second half of 2021. Sustained upward price pressures would cause governments and central banks to curtail pandemic relief efforts, strain workers trying to keep up with household bills, and risk eroding more than $40 trillion of retirement savings. But how justified are these fears?

The History

Let's not forget that after the 2008 global financial crisis, these very same concerns were loudly pronounced as it was widely expected that massive government spending would trigger a surge in demand. But it never happened; much of the new money stayed on banks' balance sheets, and the lesson was learned that cheap money alone will not produce a stimulative effect if you are caught in a Keynesian "liquidity trap." What was needed, and did not exist at the time, was pent-up demand and the wherewithal (disposable income)

If there are additional waves of coronavirus cases, the more recent stimulus may also go into savings as consumers remain cautious about spending. But if the pandemic is truly on a fast-track to resolution, the demand side of the economy is poised to see explosive growth.

to increase consumption and investment. So, are things any different today?

Demand Side

Remember that fiscal stimulus, unlike the monetary kind, can go directly into people's hands where it is likely to get spent. Following the coronavirus outbreak, initial stimulus caused savings rates to go higher. That's partly a function of the lockdowns that left restaurants and bars shattered and air travel widely shunned. If there are additional waves of coronavirus cases, the more recent stimulus may also go into savings as consumers remain cautious about spending. But if the pandemic is truly on a fast-track to resolution, the demand side of the economy is poised to see explosive growth.

Supply Side

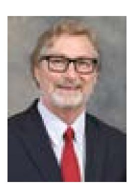
Globalization, automation, and access to low-cost labor have driven disinflationary trends in recent decades. But when COVID hit, supply chains were severely disrupted. Low-cost Asian producers were precluded from delivering low-cost products, so businesses and households turned to higher-cost alternatives. As Lacy Hunt points out, the disruption of supply chains has created "transitory monopolies and oligopolies" that charge higher prices because, well, that's what the market demands. Given time, that situation will gradually reverse, and we'll have a battle between low- and high-cost producers, which will result in competitive price wars that dampen the inflationary impulse. As supply chains are restored, inflation pressures should diminish. Also, the dollar is now strengthening after earlier weakness. That should facilitate cheaper commodities.

Money Dynamics

Another thing that hasn't changed (yet) is the "velocity" of money — the frequency with which it changes hands, as people use it to buy goods and services. Velocity fell off in the 2008 crisis and, so far, has never recovered. In 2020, it collapsed to unprecedented lows, about half the level seen in the prior decade. Money hoarding because of the pandemic and the uncertain outlook partly explains the phenomenon. But there are also legitimate concerns that the initial stimulus went to people who really didn't need it, the upper leg of the "K" in our "K-shaped" recovery. The more recent stimulus package was much larger than the initial package, and primarily designed to achieve immediate relief for middle- and lower-income groups that have a higher consumption propensity than the upper-K crowd. Those stimulus dollars are more likely to be spent rather than saved. We will soon find out if there is a pickup in velocity.

Bottom Line

Inflation will rise this calendar year. We have known this for months. But it's most likely to be a transitory event corresponding with the release of pent-up demand. We aren't convinced that current conditions will allow for a lasting inflationary impulse. The output gap is still enormous by historical standards, and even the achievement of widely expected robust GDP growth for 2021 will not be enough to push the economy into "overheating." There are too many additional dynamics working at cross purposes, including the supply-side issues mentioned above as well as demographic challenges, robotics, AI, and other disinflationary forces. Yes, there remains a trade-off between inflation and unemployment, but doubt has been cast on the strength of that link. After all, before the pandemic we had just 3.5% unemployment, yet our concern was that inflation was too low, not too high. And finally, look at the policymakers and their recent actions. There's a reason the federal reserve unveiled in August a new policy stance to allow inflation to run hotter during economic recoveries. That's because they realize the difficulty of even just getting to 2%, not to mention staying there.



Jeffrey Caughron is a managing director with The Baker Group, where he serves as president and chief executive officer. Caughron has worked in financial markets and the securities industry since 1985, always with an emphasis on banking, investments, and interest rate risk management. Contact: 800-937-2257, jcaughron@GoBaker.com.

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.

JUNE 2021

Call Report Workshop
June 15-16
Virtual Offering

School of Lending Principles
June 21-25
Manhattan, KS

Relationship & Business Development School
June 22-24
Lincoln, NE

JULY 2021

Agricultural Lending School
July 12-16
Manhattan, KS

AUGUST 2021

Young Bankers of Nebraska Conference
August 5-6
La Vista, NE

Real Estate Compliance Lending Conference
August 17-18
Lincoln, NE

School of Trust & Financial Services
August 23-27
Manhattan, KS

New Account Documentation and Compliance Workshop
August 24
Kearney, NE

Advanced Trust School
August 24-26
Manhattan, KS

New Account Documentation and Compliance Workshop
August 25
Lincoln, NE

SEPTEMBER 2021

Fall Agri-business Conference
September 2-3
Lincoln, NE

OCTOBER 2021

NBA Convention "Lite"
October 6-7
Lincoln, NE

Advanced Schools of Banking, Year 1
October 4-8
Grand Island, NE

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 nebankers.org/education.html.

ONE LAST THING ...

Did you know that you can enjoy your association news anytime, anywhere?

The new online article build-outs allow you to:

- Stay up to date with the latest association news
- Share your favorite articles to social channels
- Email articles to friends or colleagues

There is still a flipping book for those of you who prefer swiping and a downloadable PDF.

Check it out!

Scan the QR code or visit: nebraska-banker.thenewslinkgroup.org

ADVERTISER INDEX

JFC ADVISOR NETWORK

EXPERTS AT SUPPORTING FINANCIAL INSTITUTIONS

A Successful Investment Program Can:

- ✓ Provide an opportunity to acquire new customers
- ✓ Offer customers a platform where all their financial needs are addressed
- ✓ Build high-end referrals to your bank
- ✓ Present customers with robust wealth management solutions

Grow A Successful Investment Program In Your Bank

Call JFC Advisor Network at 800-262-9538 to Learn More

www.jfcadvisor.com

9060 Andermatt Drive, Suite 101
Lincoln, NE 68526

Toll-Free: 800-262-9535
Phone: 402-483-2555

Securities and advisory services are offered through LPL Financial (LPL), a registered investment advisor and broker-dealer (member FINRA/SIPC). Insurance products are offered through LPL or its licensed affiliates. The bank and JFC advisor network **are not** registered as a broker-dealer or investment advisor. Registered representatives of LPL offer products and services using JFC Advisor Network and may also be employees of the Bank. These products and services are being offered through LPL or its affiliates, which are separate entities from, and not affiliates of, The Bank and JFC Advisor Network. Securities and insurance offered through LPL or its affiliates are:

Not Insured by FDIC or Any Other Government Agency | Not Bank Guaranteed
Not Bank Deposits or Obligations | May Lose Value

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