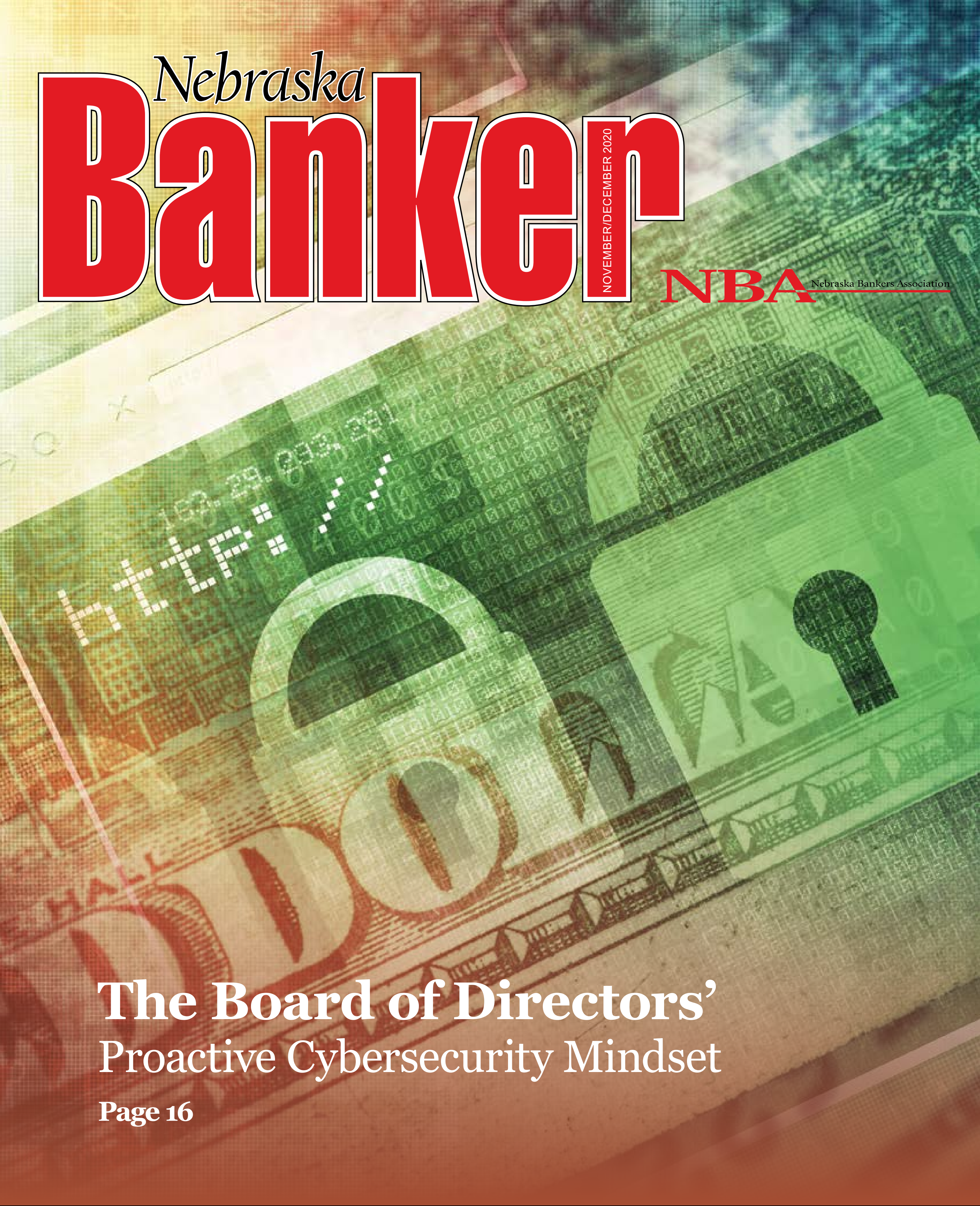
# Nebraska Banker

NOVEMBER/DECEMBER 2020

NBA Nebraska Bankers Association


## The Board of Directors' Proactive Cybersecurity Mindset

Page 16

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

# CONTENTS





Nebraska Banker

NOVEMBER/DECEMBER 2020

**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

# And the Votes Are In

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


**NEBRASKA BANKING FRIENDS:**

Another election year has come and gone. Unless you happen to live in the great state of Georgia, I suspect your televisions, social media channels and mailboxes will not be cluttered with campaign or political materials for the next two years.

The most recent election cycle was clearly unlike any I have experienced in my lifetime, with a much more polarized debate, divergent political philosophies and negative advertising taken to a whole new level. The expansion of 24-hour news outlets and aggressive social media channels will, in my opinion, reshape future political campaigns.

After careful reflection and contemplation, I think there were several valuable lessons learned through the 2020 primary and general elections. Let me begin by thanking the many candidates, regardless of their political parties or philosophies, who were willing to put their names on the ballot. These positions, especially at the local and state levels, come with little or no pay. In many ways, these local and state offices are thankless jobs. Term limits, especially at the state level, have created the need to routinely generate an increased number of candidates for office. We should celebrate our fellow Nebraskans who step forward to share their time and talents for the greater good of our communities, regions and state.

Voting is a privilege in our country that has been taken for granted by many generations. This year, Nebraska voters like their fellow voters around the country turned out in record numbers. Statistics provided by the Nebraska Secretary of State's office show voter turnout in excess of 76%, with more than 966,000 Nebraskans voting. There were many counties that had voter turnout in excess of 80%. Again, the passion and enthusiasm for this year's election is something that should be celebrated because it is the foundation of our representative democracy.

It is also important to remember these record turnouts occurred during the COVID-19 pandemic. Special thanks go out to the many poll workers, election officials and volunteers who ensured voters felt safe casting their ballots. In addition, Nebraska's election results appeared to be processed, counted and reported in a safe and efficient manner. This level of success does not occur without a great deal of planning, communication, implementation and effort by a large cast of unsung election heroes.

Again, regardless of philosophy or party, my biggest frustration from this election cycle was the tendency for voters to make their candidate selection based upon emotions, sound bites or partial information. We all read the stuffers in our mailboxes, for example, saying this candidate is bad because….! As a lifelong political junkie, I tried to engage my friends on both sides of the political spectrum in discussions about policy and priorities. I may be a bit Pollyannish, but I am sad to see the loss of civility and respectful debate that is occurring in our hyper-fractured world.

Nebraska bankers are often the leaders and visionaries in their communities and are laser-focused on problem solving. As we look to the future, I challenge our industry to channel that same leadership and focus on future election cycles:

1. Every bank and banker should strongly encourage employees, family, friends and neighbors who have a passion and aptitude for public service to run for office. Finding motivated, highly qualified candidates is key to building a stronger future.

2. If financial limitations keep an otherwise highly qualified candidate from running for public office, I would encourage the business community in your respective region to look for solutions to support the candidate and their families in other ways. Does your bank or a local business, as an example, have a part-time position

that could be filled by this potential candidate, thereby enhancing their career stability?

3. Security of the election process has received a great deal of recent public and media attention and scrutiny. Whether this issue revolved around potential outside influencers or questions about the actual election process and the counting of ballots, it is quintessential that the American election be both transparent and fair. Talk with leaders in your community about how such election requirements are implemented in your local region. Consider, for example, asking your local county clerk to make a presentation about the election process at the local Rotary or Kiwanis meeting. Similarly, maybe your bank can sponsor an election educational initiative at your local school.

4. I would be remiss if I did not also urge you to continue to give to the NBA BankPAC. This important tool allows the Nebraska banking industry to collectively support candidates who support pro-banking and pro-business enterprises.

5. And finally, I strongly encourage every Nebraska banker to foster fair, open and honest debate about important public policy issues.

Numbers provided by the Nebraska Secretary of State's office show voter turnout in excess of 76%, with more than 966,000 Nebraskans voting.

America is an amazing country with centuries of proven success and prosperity. Sure, we have had difficult times, but collectively Nebraska banks can help provide leadership focused on engaged political debate, finding common ground and recognizing the personal and professional sacrifice of every Nebraskan who is willing to put their name on the ballot for consideration!

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

# Playing the Long Game

**Rob Nichols,** President and CEO, American Bankers Association

**AFTER MONTHS OF PLANNING AND PREPARATION—AND IF** we're being honest, a little angst—Americans went to the polls in record numbers in early November to cast their votes in presidential, state and local races. The contest topping the ticket was one of the most high-profile and most contentious presidential races in recent memory, and at the time of this writing, it isn't quite in the rearview mirror: several states have yet to certify their results, some legal challenges are pending, and of course, the Electoral College has yet to meet.

But with major media outlets calling the race for former Vice President Joe Biden and Senator Kamala Harris, ABA is preparing for a Biden administration to take over in early 2021. It's also looking likely that Congress will remain divided, with Republicans in control of the Senate and Democrats maintaining control of the House—though with two critical Senate races in Georgia going to runoff elections, it will still be several weeks until we know for certain.

Regardless of how the balance of power may shift, ABA will continue to draw on its nearly 150-year history of working alongside both parties to find commonsense policy solutions that will support economic growth. It's a longstanding tradition that we're proud of, and we have made tremendous progress in recent years in advancing a pro-growth, common-sense and data-driven approach to banking policy.

In fact, many of the significant pieces of banking policy have been bipartisan in nature. Take for example S. 2155—the regulatory reform law that Congress passed in 2018. That effort was a testament to how lawmakers on both sides of the aisle were able to come together to help clear some of the roadblocks that stood in the way of banks' ability to serve their customers, clients and communities.

That same cooperative spirit is desperately needed today, when so many families and businesses are still feeling the extreme economic effects of the COVID-19 pandemic. As we look ahead to 2021, the economic recovery will be top of mind for policymakers in Washington and the financial industry will have an important role to play in the ongoing response.

Banks played a monumental role as economic first responders in the early days of the pandemic to address the economic dislocation that stemmed from the health care crisis, and we'll continue our work in the weeks and months ahead—keeping an eye on economic indicators, responding to problems early and helping to restore our nation's economy. ABA stands at the ready to work with the next administration and lawmakers from both parties to bolster the economy, increase opportunity and create a brighter future for all Americans.

At the same time, we won't lose sight of our other policy priorities. We'll continue to put our policy and advocacy expertise to work to address the important issues facing our industry, from AML/BSA reform to CECL to cannabis banking.

As one might expect from a trade association that's been around for nearly a century and a half, our eyes are on the long game. And while some of the tactics we employ may change with the times, our agenda will remain the same—and will continue to be driven, first and foremost, by the banks we serve.

*Email Rob Nichols at rnichols@aba.com.*

# Lessons from the Capital One Breach for All Banks

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

## Background

Capital One suffered a breach when credit card applications harvested from their server were posted on GitHub. Due to a misconfigured web-application, the information was accessible to individuals who had intimate knowledge of the flaw and the ability to exploit the misconfiguration. The flaw, however, was so esoteric that it could only have been known to or exploited by someone with very specialized knowledge or extensive experience in the configuration of the server.

As it turns out, the breach was perpetrated by a former Amazon Web Services (A.W.S.) employee, identified as Paige Thompson, who, in the course of her job, recognized the flaw in the configuration of the webserver software. Thompson allegedly exploited this flaw and downloaded and posted approximately 30 GB of data from the Capital One site on GitHub. The information is estimated to have affected over 100 MM individual credit card applications, which contained approximately 140,000 Social Security numbers. The F.B.I. arrested and charged Thompson with the theft of the information.

## O.C.C. Fines

The Office of the Comptroller of the Currency (O.C.C.) opened an investigation into the incident shortly after the arrest of Thompson when news of the breach leaked to the press. The investigation effectively ended when the O.C.C. announced a consent order in which Capital One agreed to the $80 MM USD fine for the breach. The O.C.C. detailed its findings in a Cease and Desist Order (Order). Specifically, the O.C.C. found that the bank failed to establish an effective risk assessment process prior to using the A.W.S. cloud environment, the bank's internal audit failed to identify numerous control weaknesses, and the weaknesses that were identified were either not reported to the Audit Committee of the Capital One Board of Directors, or they were reported and the Capital One Board of Directors failed to take effective actions. For this conduct the O.C.C. found that the Bank was in violation of 12 C.F.R. Part 30, Appendix B, "Interagency Guidelines Establishing Information Security Standards."

The breach, in this case, was a configuration error which could have only been recognized and resolved through extensive experience or knowledge. So how did the O.C.C. find liability for an exploit that is so difficult to find and repair? The O.C.C. determined that the Board never instituted a proper assessment of the controls and safeguards for the data. Capital One never conducted a cyber-risk assessment of the cloud environment which housed the data, and if they had, they might have discovered and remedied the flaw which Thompson was able to exploit.

The Order imposes an action plan on the Capital One Board of Directors to develop and supervise a risk assessment process and reassess the quality and content of reports distributed to the Board. The Order requires a plan to improve the risk assessment process for the bank, develop a cloud operations risk assessment, and enhance the audit and audit reporting processes to the Board. Finally, the Order imposes a page of prescriptive requirements on the Board that range from authorizing corrective actions, ensuring the Bank has sufficient processes in place, and ensuring the Board will hold the Bank's management accountable for executing the plan with timely and appropriate reporting.

The case, the Consent Order, and the findings by the O.C.C. incorporated in the Order summarize several issues that all banks and their boards review and incorporate into their own processes and procedures. But, the most important take-away is that any and all serious cybersecurity issues should be immediately brought to a board of director's attention. There are real consequences for a company's failure to proactively avoid cybersecurity breaches, and boards cannot avoid consequences of cybersecurity incidents by failing to address them.

### Forensics Reports and Maintaining Privilege

After the exposure of the data, Capital One hired a forensics firm, Mandiant, to conduct an investigation into the breach of their data. Mandiant was the same firm Capital One had an ongoing relationship with to perform periodic reviews and vulnerability assessments. Due to the ongoing relationship with the firm, Capital One decided that Mandiant would be better equipped to deal with the data breach than another firm that would be less familiar with the Capital One network. Based on the prior relationship, Capital One engaged with Mandiant to conduct the investigation, determine the root cause of the cyber breach, and produce a report.

Capital One initially signed a Master Services Agreement (M.S.A.) with Mandiant in 2015. Under that M.S.A., Capital One signed a series of Statements of Work (S.O.W.s). The S.O.W.s, among other services, provided for cybersecurity response services in the event a cyber-breach would occur. Mandiant thus had a preexisting relationship to provide incident response services.

In addition to the preexisting relationship, Capital One had regularly paid a retainer to Mandiant for their ongoing services. Because the retainer was already established, Mandiant initially deducted the cost of the cybersecurity investigation from the retainer. When the retainer was depleted, Capital One paid for the investigation and report from an account denominated as "business-critical" services as part of their overall cyber budget.

When Capital One suffered the breach, they retained the law firm Debevoise & Plimpton L.L.P. as their cyber breach coach. Then on "July 24, 2019, Capital One and Debevoise signed a Letter of Agreement with Mandiant under which Mandiant would provide services and advice, 'as directed by counsel,' in the areas of (1) computer security incident response; (2) digital forensics, log and malware analysis; and (3) incident remediation. These areas reflected the same scope of work Mandiant had already agreed to provide under the M.S.A. and S.O.W.s." The engagement letter provided that all work by Mandiant for this engagement would be conducted under the direction of the law firm and that deliverables would be provided directly to counsel rather than Capital One.

**COUNSELOR'S CORNER** — continued on page 14

There are a number of lessons banks and boards can learn from the Capital One case. First and foremost, boards of directors must make cybersecurity and vulnerability issues part of their regular discussions. The management of the risk assessments and vulnerability management and mitigation need to be supervised from the highest echelons of an organization.

**COUNSELOR'S CORNER** — continued from page 13

In September 2019, Mandiant issued their report. The report was initially distributed just to the law firm, but the law firm then either distributed or told Mandiant to distribute the report "to Capital One's legal department, its Board of Directors, its financial regulators, its outside auditor, and dozens of Capital One employees." It is unclear from evidence and was omitted from Capital One's opposition whether the report was distributed for business purposes or in anticipation of litigation.

Plaintiffs in the ensuing case sought to compel the production of the report. Capital One argued that the report should be afforded attorney-client privilege under the work-product doctrine. Work-product privilege applies when two requirements are met; first, the company is actually faced with suit or is preparing for impending litigation, which the court held was the case here. And second, the work-product privilege also requires that the "[r]eport would not have been prepared in substantially similar form but for the prospect of that litigation."

In the end, the district court ruled that the report was discoverable and outlined a series of missteps, which led the court to find that the second requirement of the attorney work-product doctrine test was not met. First, the court cited the fact that Mandiant had a prior engagement with Capital One for substantially similar services. Mandiant was paid out of "critical business" accounts as opposed to an account associated with their legal budget. The court also noted that the report was widely distributed without evidence of restriction. Finally, the court opined that Mandiant's engagement with the law firm referenced the preexisting M.S.A. and S.O.W. and thus, the report would not have differed substantially from a report produced pursuant to their previously signed engagements.

## Lessons Learned

There are a number of lessons banks and boards can learn from the Capital One case. First and foremost, boards of directors must make cybersecurity and vulnerability issues part of their regular discussions. The management of the risk assessments and vulnerability management and mitigation need to be supervised from the highest echelons of an organization. Regulators will begin looking at the steps boards have taken to identify, manage and reduce vulnerabilities.

Secondly, banks should limit the distribution of incident response reports to only those individuals necessary for litigation. Banks should avoid sharing the report with other organizations or individuals. The oversharing of a report may result in the inadvertent waiver of privilege. If the distribution of the report is necessary, it should include a confidentiality requirement and language limiting the use to litigation preparation. Finally, the cyber report should not be used for anything other than the preparation of anticipated litigation.

The Capital One case has provided a number of opportunities for reflection, change, and application of lessons learned in the vulnerable cybersecurity environment.

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



# The Board of Directors Proactive Cybersecurity Mindset

**Jeff Spann,** SVP Information Security Consultant/Regional Director - SBS CyberSecurity, LLC

## Board of Directors Responsibilities

Financial institutions are economic engines that drive our communities. At the head of each financial institution is a Board of Directors, who oversee and provide direction for the institution to ensure the operation and meet its customer needs. The responsibility for such oversight is massive and has evolved greatly over the last 10 years to include investments in technology and cybersecurity. The Board is held accountable to the institution's shareholders, employees, depositors, the community they serve, and the regulators for the operations of an efficient, safe and sound institution.

Each institution is examined and measured on the capital, asset quality, management, earnings, liquidity and sensitivity to market risk, which is known as the CAMELS rating. An institution's Information Security Program (ISP) is measured in the management component of the CAMELS rating and, when managed proactively, provides safe and sound risk management practices for the operations of the institution.

Managing the ISP is a team effort and includes all operational areas of the institution. To establish an organization that proactively manages the ISP, the Board annually appoints an Information Security Officer (ISO) to oversee the day activities involved in maintaining a well-managed ISP. Though the Board is ultimately held responsible for the ISP, the ISO oversees day-to-day information security activities and reports to the Board at least annually on the overall status of the ISP. Additionally, the Board appoints an Information Technology (IT – or similarly named) Committee to oversee the day-to-day IT operations and information security risk management. The Board reviews and offers credible challenges to IT Committee minutes and reports provided, and as oversight, provides an acceptance or approval.

Much of proactive management is delegated to the ISO and the IT Committee; however, the Board sets the organizational culture regarding security (mindset) and provides the direction for investing in technology and protecting that investment. The Board ultimately determines, intentionally or unintentionally, whether an institution has a reactive or a proactive cybersecurity mindset.

## Reactive Mindset versus Proactive Mindset

Each institution chooses – knowingly or unknowingly – to take a stance when it comes to its cybersecurity mindset. The different types of mindsets, typically driven by a "sudden need," include:

- Passive: taking the compliance-driven approach by choosing only to meet regulatory standards, which does not offer protection from today's cyber threats.
- Reactive: a step beyond passive, but only to include reacting to findings and recommendations from IT exams and audits, which can provide some additional protection, but not enough to prevent or properly respond to a cyber incident.
- Proactive: strategic thinking that moves beyond basic compliance to understand today's threats and build an ISP that can get out in front of today's cyber threats and still meet regulatory compliance.
- Innovative: using IT and information security risk assessments to make better, more-informed decisions that can quantify risk and deploy the right controls to mitigate the most risk of a cyber incident.

> An institution with a proactive mindset strives not only to achieve a high rating for the management component of the CAMELS rating, but also to do whatever needs to be done to protect the investments it has made. The Board's responsibility for oversight of the ISP is better managed proactively.

Shifting from a reactive mindset to a proactive mindset is one of the key decisions a Board of Directors can make to protect the investments made in technology and an institution's confidential information.

### Results of a Reactive Mindset

When a Board continues to have a reactive mindset, the institution will lack good risk management practices, feel frustrated, and may respond to events without proper preparation, which can result in losing control of spending and costing more to recover from a cyber incident than necessary. The mindset is revealed when an audit or exam results in a long list of items not meeting regulatory guidance or industry-standard risk management practices. A reactive mindset can also reveal itself when a cybersecurity incident takes the institution out of operation for extended periods of time with significant financial impacts. The environment becomes inefficient, and the costs of managing the institution reactively become a guessing game.

### Benefits of a Proactive Mindset

An institution with a proactive mindset strives not only to achieve a high rating for the management component of the CAMELS rating, but also to do whatever needs to be done to protect the investments it has made. The Board's responsibility for oversight of the ISP is better managed proactively. Proactive management does not wait for an audit or exam to tell the institution what needs to be done. The proactive mindset takes control and regularly risk assesses all areas of the ISP to act and mitigate the identified risks before threats are realized.

There are many strategic advantages to managing the ISP with a proactive mindset, and some are easy to recognize. At the same time, some are intangible and not as easily recognized until there is reflection. The mindset to be proactive reveals itself in the results of an audit, exam, a cybersecurity incident or a disaster recovery event. A proactive mindset provides a member of the Board and senior management with clarity to handle situations. It allows for better sleep at night, knowing the institution has proactively identified and planned for information security risks.

### The Board of Directors Sets the Culture

The Board chooses to have a culture of a proactive mindset or stay in a reactive mindset. A proactive mindset will reduce financial losses, have more efficient processes, gain control of the challenges to the institution, and gain a competitive advantage over the competition.

Here are four questions to ask yourself to help determine your cybersecurity mindset:

1. Are we discussing cybersecurity as a Board regularly and growing in our ability to be a "credible challenge" to cybersecurity-related decisions (proactive), or are we just waiting to get through the minimum necessary cyber discussions so we can get back to "real business" (reactive)?

2. Are we measuring cybersecurity risk and using the results of our risk assessments to make more informed cybersecurity decisions (proactive), or are we checking the box when it comes to ISP-related risk assessments (reactive)?

3. Do we know what our most important IT assets, vendors and business processes are, as well as the top threats to our institution right now (proactive), or are we just reviewing the results of those risk assessments and moving along (reactive)?

4. Have we made the proper investments (people, resources, training, and/or money) when it comes to protecting our investments and confidential information (proactive), or do we still treat IT and cybersecurity as an expense (reactive)?

*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.*

# The Race is On — Keeping Up With the BSA

**Steve Manderscheid,** Compliance Alliance


DURING NORMAL TIMES, IT CAN BE CHALLENGING FOR BANKERS to get their arms around the regulatory requirements surrounding the Bank Secrecy Act (BSA) and anti-money laundering (AML) regulations. So, when you add a global pandemic, such as COVID-19, things can get a little dicey, especially when navigating competing priorities.

Fortunately for us, the Federal regulators have been proactive in providing the banking industry with up-to-date compliance guidance (although it is important to note the guidance did not extend the BSA regulatory reporting deadlines) relating to the pandemic. Furthermore, the Financial Crimes Enforcement Network (FinCEN) went as far as creating a webpage devoted to coronavirus updates. A brief scan of their webpage includes the following advisories:

- Advisory on Cybercrime and Cyber-Enabled Crime Exploiting the Coronavirus Disease 2019 (COVID-19) Pandemic
- FinCEN Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 (COVID-19)
- FinCEN Advisory on Medical Scams Related to COVID-19
- Companion Notice to FinCEN COVID-19 Advisories
- Paycheck Protection Program Frequently Asked Questions
- Updated FinCEN Notice to Financial Institutions Regarding COVID-19
- FinCEN Notice to Financial Institutions Regarding COVID-19

In these statements, FinCEN encourages financial institutions to communicate concerns related to the COVID-19 pandemic and to remain diligent in detecting related suspicious activity. Hopefully, by now, banks have passed the stage where concerns exist over the potential delays in filing required BSA reports – suspicious activity reports (SARs) and currency transaction reports (CTRs) – but know that risk was really for many.

So that brings us to suspicious activity monitoring and reporting, which is a staple of a safe and sound BSA program. By now, suspicious activity, including illicit fraudulent transactions, is not something that is particularly new to us, as we have dealt with many types of fraud – ACH, loan and identity theft fraud – just to name a few. But, since FinCEN has suggested that the banking community "remain alert about malicious or fraudulent transactions similar to those that occur in the wake of natural disasters," we should take a look at the emerging trends connected to COVID-19:

- Imposter Scams – Bad actors attempt to solicit donations, steal personal information, or distribute malware by impersonating government agencies (e.g., Centers for Disease Control and Prevention), international organizations (e.g., World Health Organization (WHO), or health care organizations.

- Investment Scams – The U.S. Securities and Exchange Commission (SEC) urged investors to be wary of COVID-19-related investment scams, such as promotions that falsely claim that the products or services of publicly traded companies can prevent, detect or cure coronavirus.
- Product Scams – The U.S. Federal Trade Commission (FTC) and U.S. Food and Drug Administration (FDA) have issued public statements and warning letters to companies selling unapproved or misbranded products that make false health claims pertaining to COVID-19. Additionally, FinCEN has received reports regarding fraudulent marketing of COVID-19-related supplies, such as certain facemasks.
- Insider Trading – FinCEN has received reports regarding suspected COVID-19-related insider trading.

When you throw in the reminder regarding the importance of detecting trends related to COVID-19 medical fraud, imposter scams and cyber-enabled crime, the banking industry has the daunting task of being the watchdog for fraudulent transactions.

Where do we start? Begin with the bank's system for identifying potentially suspicious activity. Most banks have multiple channels that funnel unusual activity to the appropriate party for research and reporting.

First, and likely most important, bank employee detection is key. During the course of day-to-day operations, employees may observe unusual or potentially suspicious transaction activity or requests. During this pandemic, it is important employees are aware of the FinCEN emerging trends so they can be aware of potential red flags that may be uncovered. Further, it would be appropriate to share the bank's own specific unusual activity trends, if any are identified based on the bank's customers, products and services, and geographic location.

Second, monitoring systems are designed to detect potential suspicious activity whether manual or automated. For manual monitoring, the goal is usually to identify higher-risk transactions, such as those involving large amounts of cash or those to or from certain geographies, which may need to be tweaked when considering the current FinCEN emerging trends relating to the coronavirus.

Automated account monitoring systems can certainly make it easier to identify individual transactions, patterns of unusual activity, or deviations from expected activity. These systems can capture a wide range of account activity, such as deposits, withdrawals, funds transfers, automated clearing house (ACH) transactions, and automated teller machine (ATM) transactions, directly from the bank's core data processing system. However, the program parameters and filters should be reasonable and tailored to the activity that the bank is trying to identify or control and may need some fine-tuning based on our current COVID-19 environment.

**Compliance Alliance** — continued on page 20

**Compliance Alliance** — continued from page 19

Remember, the battle against suspicious activity has only begun at the identification stage. Once identified, the bank still has the responsibility to review and research the activity and ultimately come to a final SAR decision. If a decision is made to file a SAR related to the COVID-19 pandemic, it is important to provide information with a high degree of usefulness for government authorities, including law enforcement. FinCEN has requested that appropriate information is included in any report to help identify the fraud, such as:

- If the suspicious activity is related to an ACH payment from a state unemployment insurance program, please clearly mention COVID19 UNEMPLOYMENT INSURANCE FRAUD in field 2 of the SAR (Filing Institution Note to FinCEN) as well as in the narrative. This will make it much easier for your SAR to get to law enforcement teams working with the states on unemployment fraud.

- Or if the activity involves a counterfeit check or ACH payment for the EIDL program, please also clearly mention COVID19 EIDL FUNDS FRAUD in field 2 of the SAR (Filing Institution Note to FinCEN) and state this in the narrative, as there are specific prosecutorial teams working on EIDL fraud.

Remember, financial institutions should provide all pertinent available information in the SAR and narrative. The better the story (i.e., the narrative), the more likely it will assist law enforcement to identify and act against COVID-19-related crimes.

Automated account monitoring systems can certainly make it easier to identify individual transactions, patterns of unusual activity, or deviations from expected activity.

As we continue to do our part to fulfill our BSA regulatory duties, it is important to remember those that may be impacted most – customers and community members. Continue the good fight and remain vigilant during these challenging times and help protect those most susceptible to being taken advantage of from those bad actors.

*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 the COVID-19 (Coronavirus) event recommendations and related schedule changes, please visit https://www.nebankers.org/education.html or call the NBA Education Center at (402) 474-1555 for the most current event calendar updates.**

## DECEMBER 2020

**Agriculture & Beyond Workshops**
December 8
Virtual Offering

## FEBRUARY 2021

**Mid-Winter IRA Essentials Workshop**
February 8-9
Virtual Offering

**Mid-Winter IRA Advanced Workshop**
February 10-11
Virtual Offering

**Health Savings Account Seminar**
February 12
Virtual Offering

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

## MARCH 2021

**Supervisor Bootcamp Conference**
March 2, 3, 16, 18
Virtual Offering

**Principles of Banking Seminar**
March 9-10
Virtual Offering

**Tri-State Marketing & Human Resources Conference**
March 18-19

## APRIL 2021

**Spring Agri-Business Conference**
April 6-7
Virtual Offering

## 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 may also visit the NBA website at https://www.nebankers.org/education.html.*

# Fighting Margin Compression in Today's Rate Environment

**Dale Sheller,** The Baker Group.

## How We Got Here

In 2009, some said interest rates had nowhere to go but up. Well, Treasury yields found a way to continue to go down and stay down. The Fed took seven years to increase the funds rate by a quarter point at the end of 2015, then another quarter point increase twelve months later, followed by seven more quarter point rate hikes in 2017 and 2018. All nine rate hikes were undone by the Fed in a short amount of time, with three of the rate cuts coming in the latter half of 2019 as part of a "mid-cycle adjustment." The remaining cuts came in March as part of a historic monetary response from the Fed.

## Interest Rate Risk

Since 2009, we have been looking at our interest rate risk models and fine tuning our assumptions in order to measure, monitor, and control interest rate risk. Our ultimate goal was to answer the question, how much risk is there to our earnings and capital position if interest rates rise? To answer that question, we made sure our balance sheets were well positioned to take advantage of rising interest rates. That strategy allowed net interest margins to expand slowly but surely for several years as the Fed engaged in its most recent tightening cycle. But that was then and this is now. The Fed has put rates back at zero, and it is highly unlikely we will see an increase in rates in the next few years, if not longer.

At the start of 2020, most banks were well positioned for a rise in interest rates, not a freefall back to zero. Interest rate risk has already taken its initial hit on margins and there is likely more to come. Institutions who were able to extend asset yields before rates hit zero will fare better in the near term, but a prolonged low interest rate environment will eventually take its toll on all.

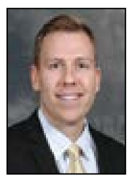
### Fighting Margin Compression

The quickest way for institutions to fight margin compression is through lowering their deposits rates and overall cost of funds. Most bankers have aggressively cut deposit rates as banks have already unwound about half the increase to their costs of funds experienced during the previous Fed tightening cycle. Most of the room left to cut will be on CD rates, which saw the biggest increase in the last few years. If you are worried about deposit runoff should you continue to lower rates, consider replacing those deposits with cheap wholesale funding.

Yields on earning assets have fallen since year-end 2019 for two reasons: lower interest rates and excess liquidity on the balance sheet. As of June 30, 2020, the average community bank was holding approximately eight percent of total assets in interest-bearing balances, with most of those dollars likely held at the Federal Reserve earning ten basis points. Most of that excess liquidity came in so fast that some bankers haven't had sufficient time to strategize on where to deploy it.

### Staying Fully Deployed

Holding on to too much cash and waiting for rates to go up is not the conservative play. Margins can't afford it. If quality loan demand is available, make the loan; if not, you need to earn more than ten basis points. Take a long look at your liquidity position and decide how much you are able to deploy into the investment portfolio. No one loves today's bonds yields, but don't compare them to where they were a year ago. Instead, compare them to the alternative, which is holding them in low earning cash. There are only so many levers we can pull to fight margin compression, and we need to start as soon as possible.



*Dale Sheller is Senior Vice President in the Financial Strategies Group at The Baker Group. He joined the firm in 2015 after spending six years as a bank examiner with the Federal Deposit Insurance Corporation. Sheller holds a bachelor's degree in finance and a master's degree in business administration from Oklahoma State University. He works with clients on interest rate risk management, liquidity risk management, and regulatory issues. Contact: 800-937-2257, dsheller@GoBaker.com.*


SELF-SERVICE BANKING
Now more than ever people want self-service options. With our core integrated ITMs we can make this a reality both in the lobby and in the drive-up of your branch.
MHM
MONEY HANDLING MACHINES
800.228.2581
MHM.INC


BANKERS' BANK OF THE WEST
IN BUSINESS TO FURTHER YOUR BUSINESS
YOUR ADVOCATES:
Nebraska's correspondent team
TARA KOESTER
KELLY MALONE
TRACI OLIVER
MARLENE WADE
411 South 13th Sreet | Lincoln, Nebraska | 402-476-0400
BBWEST.COM
WE CHAMPION COMMUNITY BANKING
Member FDIC



# ADVERTISER INDEX

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