WEST VIRGINIA BANKER

WINTER 2020

14

Ransomware — Additional Risks for Banks

16

Navigating the Pandemic — Where To From Here?

30

Cloud Computing: Security Considerations

The Baker Group Is Here to Help

The Baker Group

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

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

Baker's Software Solutions Service Package Includes:

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

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

Baker Bond Accounting® (BBA)

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

Investment Analysis – Advanced Portfolio Monitor (APM®)

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

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

Member: FINRA and SIPC

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

Ryan@GoBaker.com

www.GoBaker.com

800.937.2257

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

CONTENTS

The West Virginia Banker magazine was recognized with an Award of Distinction in the Overall Design Category.
The Communicator Awards are the leading international creative awards program honoring creative excellence for communication professionals. Founded over two decades ago, The Communicator Awards are an annual competition honoring the best in advertising, corporate communications, public relations and identity work for print, video, interactive and audio. The 24th Annual Communicator Awards received over 6,000 entries from top ad agencies, interactive agencies, production firms, in-house creative professionals, graphic designers, design firms, and public relations firms around the world.

6 **A Message From the Chief Executive: Suddenly, Virtual Learning Became a Necessity**
By Sally Cline

8 **community CORNER**

10 **Building Diversity, Equity and Inclusion in the Workplace**
By Ashley Hardesty Odell, Bowles Rice LLP

12 **Fighting Margin Compression in Today's Rate Environment**
By Dale Sheller, The Baker Group

14 **Ransomware — Additional Risks for Banks**
By Mark Mangano, Jackson Kelly PLLC

16 **Navigating the Pandemic — Where To From Here?**
By Gary Shook, Community Bankers' Bank

18 **Avoiding CCPA Debt Collection Traps — A Periodic Reminder**
By Russell Jessee and Sarah Ellis, Steptoe & Johnson PLLC

22 **Strategic Transactions With Outstanding PPP Loan and EIDL Obligations**
By Matthew Kingery, Lewis Glasser PLLC

26 **Six Ways the COVID-19 Pandemic Has Changed the Delivery of Financial Services**
By Nicholas P. Mooney II and Angela L. Beblo, Spilman Thomas & Battle

30 **Cloud Computing: Security Considerations**
By Chris Joseph, Arnett Carbis Toothman

34 **Calendar of Events**

A MESSAGE FROM THE CHIEF EXECUTIVE

By Sally Cline

Suddenly, Virtual Learning Became a Necessity

Few services offered by the West Virginia Bankers Association have been affected as dramatically by COVID-19 as our educational offerings. In mid-March, we began postponing and canceling in-person events to protect our banker's and staff's health and well-being. Practically overnight, WVBankers had to challenge the way we traditionally do business. We quickly had to shift gears and organize numerous educational offerings in a virtual setting. While we would have preferred the continuation of a face-to-face learning environment that facilitates networking opportunities, we were proud of the digital experience we were able to deliver.

Here are a few testimonials we received from participants:

- "(The instructor) was just as informative on the zoom call as she would have been in person with the convenience of not having to leave home for two days. I really enjoyed this new way of learning!"
- "I thoroughly enjoyed the zoom school. It was my first zoom experience!"
- "I thought it was great. I liked doing the class virtual better than I do in person. It was great to be word searching my policy as she was teaching what needs to be in the policy and emailing ideas to my staff as she was pointing out tips. Plus, NO THREE HOUR DRIVE!!!!"

We are slowly moving back to hosting in-person events, but only for those classes and seminars that have historically had 25 or fewer attendees, to comply with the Governor's Executive Order No. 70-20 and the West Virginia Department of Health and Human Resources' County Alert System. Events planned in-person between January and May 2021 include the Commercial Lending Development Program, Compliance School, Emerging Leaders, Credit Management Conference and Bank Security School. Should any county in which any of these events is planned be labeled red, orange or gold on the County Alert System, that event will move to a virtual learning environment.

We are very excited to offer our inaugural Commercial Lending Development Program. This comprehensive program emphasizes the entire commercial loan life cycle and provides participants with current lending approaches, including an updated focus on key analytics and regulatory issues. The program is designed for bankers already in the commercial lending field who would like to strengthen their credit skills, as well for those credit analysts moving into commercial lending. Through best practices and case studies, students will learn what it takes to compete in the highly competitive lending market successfully.

Whether virtual or in-person, WVBankers offers top-notch educational programming that helps to ensure employees, including those new to the industry, understand the business of banking. The WVBankers' education department offers a wide variety of classes, seminars, schools, and conferences designed to assist bankers at every level in developing their professional and technical skills. Each program is carefully designed under the direction of experienced bankers, regulators and industry consultants to ensure the highest level of programming and future-focused topics.

In addition to traditional classroom training, WVBankers offers live and recorded webinars and online self-paced learning opportunities. When looking for education, please look first to WVBankers. Your bank's participation in WVBankers programs provides vital support to the Association and ensures your staff and future leaders are well-positioned to confront the challenges of the future.

Please visit our online educational calendar at www.wvbankers.org. ■

CALHOUN BANKS

L-R: Nikki, Stephanie, Jenny, Tara, Regina, and (Rachael — not pictured) work together daily to ensure we have a safe environment for anyone who walks through the doors of our Elizabeth branch!

Employees from the Grantsville Branch being socially distant and wearing masks during their quarterly employee meeting.

Robert Rogers, Operations Representative, is smiling under his mask, thankful for the opportunity to work for a bank with employee and community safety as a top priority.

FNB BANK COMMUNITY PROJECT — GIVING BACK TO OUR GREAT COMMUNITY.

Team included: Chris Cooper, Sheila Hines, Maria Eversole, Travis Clower, Brett Berg, Travis Delaplain, Stacey Bowman, Barb Harris, Emma Snyder, Terra Ritter, Dennis Moore, Steve Hines and crew (TCC Sealcoating)

Our 2020 project team painted blacktop art & games and the basketball poles/backboards, replaced the nets, fixed cracks on the court and painted all court lines at Slanesville Elementary School.

CITY NATIONAL BANK

City National Bank employees took a break to volunteer for United Way of Central West Virginia's 2020 Day of Caring, helping local nonprofits with community projects and other service opportunities. The City National Bank teams spent the day at the Born Learning Trail at Little Page Terrace and Meeks Trail in Hurricane, West Virginia.

PEOPLES BANK

Huntington business photo: Pictured from left to right is Andre Joiner, Peoples Bank Government Guaranty Lending Specialist, Aaron Smith, Peoples Bank Commercial Banker, Kris Warner, West Virginia State Director of USDA Rural Development, and Rocky Meadows, Founder and Executive Director of The Lifehouse Inc.

Valerie Johnson, Ryan Welch, Steve Wayne and Tyler Wilcox from Peoples Bank with Cynthia Kirkhart from Facing Hunger Foodbank.

Parkersburg policemen and firefighters pictured with associates from Peoples Bank Parkersburg Division Street office.

Associates from Peoples Bank Point Pleasant office.

Building Diversity, Equity and Inclusion in the Workplace

By Ashley Hardesty Odell, Bowles Rice LLP

Employers know that a happy and thriving workforce is more productive and, consequently, more profitable. In today's workplace, more employers recognize that diversity, equity, and inclusion (DEI) play a key role in an organization's success. Increased diversity promotes ingenuity and creativity. Equity cultivates trust and a sense of fairness. Inclusion fosters loyalty and commitment. This is why employers today endeavor to implement and develop rich diversity, equity, and inclusion programs in the workplace.

It is not a simple undertaking, and it involves much more than written policies and plans (although such policies and procedures are a foundational component of any successful program). More importantly, a successful DEI program requires a meaningful shift in culture and a change in mindset, starting with the organization's top leadership. It is hard work. But the outcomes from a successful DEI program can be transformative for the organization.

There are countless opportunities to develop DEI in the workplace. To get started, however, here are five key concepts to consider:

1. Understand the business case for DEI;
2. Identify and empower DEI allies;
3. Measure the organization's current diversity and culture;
4. Audit the organization's policies; and
5. Educate all stakeholders.

As more fully explained below, these guiding principles are only building blocks for a thoughtful and comprehensive DEI program. The success of that program depends heavily on the organization's willingness to invoke and promote change.

First, be prepared to discuss DEI within your organization as more than a moral imperative. Promoting diversity, equity, and inclusion is, of course, the right thing to do. But it is also a business investment. And understanding the business case for DEI will capture more buy-in from more stakeholders.

A workplace that is not diverse, equitable, or inclusive is far less productive. Diverse teams are more innovative and create new and different opportunities. Millennials and Generation Z insist on DEI, so a comprehensive and meaningful DEI program can help with recruiting and retention. Finally, clients and customers want the businesses that they patronize to be more diverse and reflective of themselves. Framing discussions around the potential financial outcomes resulting in the organization's investment in DEI is essential to any DEI program's success.

Second, identify and empower DEI advocates in the organization. Make sure those allies are well represented in the organization's top leadership. Real DEI advocates and allies are agents of change, and they will push for more than lip service or a "check the box" DEI program. Empower those allies and change agents with meaningful programming designed to transform the organization's culture. Appoint a DEI officer and committee and give them measurable expectations.

It also is important to identify allies from outside the organization and use their influence. Perhaps some of your best customers are DEI advocates and could influence the organization to focus on the issue. Perhaps your competitors are investing in DEI and seeing positive outcomes. It is very unlikely that all stakeholders will support DEI, but knowing those who are supportive is critical to the program's long-term success.

Third, take note of the organization's current statistics and consider a culture survey. Measure the number of women and diverse stakeholders in leadership at each location or branch and each department. Identify where there are gaps in the representation of diverse stakeholders. Set the baseline and re-measure periodically. Let your employees know you are doing this. Doing so proves to them that the organization values diversity and equity. Talk to employees and ask them how they feel about their work and whether they feel valued and included in the organization's success. Do not wait for an employee's exit interview to find out what the employee thinks. Asking the workforce for input is a simple way to build inclusion.

Fourth, audit the organization's existing policies and adopt modifications or new policies that promote DEI. Do you have an anti-harassment policy, and is it broad enough? What is your parental leave policy? Allow for remote and flexible work options. As part of your ongoing culture survey, evaluate whether these policies are applied fairly and consistently and look for negative stigma associated with them. Consider adopting a comprehensive DEI plan and more discrete annual action plans. Set a budget for DEI programming. These efforts further demonstrate the organization's commitment to DEI.

Finally, educate all stakeholders about the organization's DEI program, starting with orientation, and include regular reminders in the form of DEI updates, learning opportunities, and celebrations of DEI related events. Educate all stakeholders on implicit bias and how it impacts everyone's decision making and judgment. Require implicit bias training for supervisors, recruiters, and anyone responsible for compensation decisions. Cultivate awareness of events like Martin Luther King, Jr.'s Day of Service, Equal Pay Day, Juneteenth, Pride Month, and Disability Awareness Month. Ensure your marketing department is thoughtful about incorporating and highlighting diversity and diverse stakeholders in internal and external communications. Keep the conversation going — DEI is a long game.

Again, the ways to incorporate and build DEI into the workplace are wide-ranging. This article outlines some foundational ideas for developing DEI. But there is no single, static DEI program that will work in every organization. DEI programs will (and should) vary from organization to organization. They will (and should) evolve. They will (and should) transform the industry and business community, all for the better. ■

Ashley Hardesty Odell serves as the Diversity Partner at regional law firm Bowles Rice. Practicing from the firm's Morgantown office, her work focuses on employment law and first-party/extra-contractual insurance defense. A 2019 Fellow of the Leadership Council on Legal Diversity and Chair of the West Virginia Chamber of Commerce's Diversity Working Group, she regularly counsels organizations and clients on DEI in the workplace. Contact Ashley at 304-285-2522 or ahardestyodell@bowlesrice.com.

Fighting Margin Compression in Today's Rate Environment

By 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 12 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 reductions 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

The quickest way for institutions to fight margin compression is through lowering their deposits rates and overall cost of funds.

there is likely more to come. Institutions who could 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.

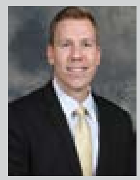
Fighting Margin Compression

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 cost of funds experienced during the previous Fed tightening cycle. Most of the room left to cut will be on CD rates, which saw the most significant 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 held approximately 8% of total assets in interest-bearing balances. Most of those dollars were likely held at the Federal Reserve, earning 10 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 10 basis points. Take a long look at your liquidity position and decide how much you can 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. We can pull only so many levers 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.

Ransomware — Additional Risks for Banks

By Mark Mangano, Jackson Kelly PLLC

Banks are exposed to ransomware risks that extend beyond cyberattacks on their systems. Banks participating in ransomware payments by victims may expose the bank to penalties for violations of Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) regulations. On Oct. 1, 2020, the United States Treasury, through FinCEN and OFAC, issued advisories related to the risks and obligations of those dealing with ransom demands.[1] The advisories apply to a variety of businesses and victims impacted by a ransomware event. This article focuses on considerations for depository institutions (Banks).

FinCEN defines ransomware as a form of malicious software (malware) designed to block access to a computer system or data, often by encrypting data or programs on information technology (IT) systems to extort ransom payments from victims in exchange for decrypting the information and restoring victims' access to their systems or data. In some cases, in addition to the attack, the perpetrators threaten to publish sensitive files belonging to the victims, which can be individuals or business entities (including financial institutions). The consequences of a ransomware attack can be severe and far-reaching — with losses of sensitive, proprietary, and critical information or loss of business functionality.

The challenges of dealing with ransomware payments are not confined to large banks. It is increasingly likely that community Banks will be called upon to deal with requests to facilitate ransom payment. According to the Federal Bureau of Investigation, reported ransomware cases and losses are rapidly increasing. Also, cyber-actors are launching ransomware attacks against increasingly diverse targets.

Payment of ransom often involves transferring money through a chain of entities. Ransoms are generally paid in convertible virtual currency (CVC) such as Bitcoin. The payment may be initiated by the victim or a cyber insurance company, or other representatives of the victim. Money is transferred from a

Bank to a CVC account provided by a money services business (MSB). From there, it may be transferred to accounts at other MSBs designated by the cyber-actor. The funds are then often laundered before being received by the cyber-actor.

There are two key concerns for Banks; identifying when a customer is requesting that it facilitate a ransom payment and avoiding direct or indirect participation in a transaction that violates OFAC regulations. FinCEN requires procedures to ensure that an appropriate suspicious activity report (SAR) is filed related to a ransomware transaction. OFAC requires banks to implement procedures to ensure that the Bank does not violate OFAC regulations.

OFAC Advisory

The purpose of the OFAC advisory is to highlight the sanctions risks associated with ransomware payments. OFAC discourages payment of ransoms. OFAC's concerns with ransom payments include encouraging further attacks and funding other illicit activities of the United States' criminals and adversaries. OFAC continues to identify and sanction cyber-actors benefiting from ransomware attacks.

The purpose of the OFAC advisory is to highlight the sanctions risks associated with ransomware payments. OFAC discourages payment of ransoms. OFAC's concerns with ransom payments include encouraging further attacks and funding other illicit activities of the United States' criminals and adversaries.

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a Bank may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a prohibited person under sanctions laws and regulations administered by OFAC. However, OFAC will consider the existence, nature, and adequacy of a sanctions compliance program as a factor in determining an appropriate enforcement response. OFAC encourages Banks to implement risk-based compliance programs to mitigate exposure to sanctions-related violations.

It is possible to pay a ransom to a sanctioned person through a license issued by OFAC. But, the presumption is that OFAC will deny license requests.

FinCEN Advisory

The FinCEN advisory discusses the role of financial intermediaries in processing ransomware payments, trends of ransomware and associated payments, ransomware-related financial red flag indicators, and reporting and sharing information related to ransomware attacks. The advisory also provides helpful references to regulations, guidance, and resources.

The red flag indicators of ransomware-related illicit activity are provided to assist Banks in detecting, preventing and reporting suspicious transactions associated with ransomware attacks. The red flags address suspicious activity related to a Bank's systems as well as financial transactions.

The advisory discusses SAR filing requirements related to both attempted and successful extortion transactions and suspicious cyber events. The advisory reminds Banks to incorporate all relevant information available in SAR reporting.

Conclusion

The advisories do not introduce new legal requirements, but they provide a clear statement of the agencies' expectations regarding how Banks should address ransomware situations and transactions. Banks should review their anti-money laundering policies and procedures to ensure that their systems include adequate monitoring for ransomware transactions, enhanced risk management procedures when ransomware events are detected, and appropriate and detailed reporting procedures. Banks should also ensure they have clear response plans for ransomware attacks directed at the Bank. Well documented procedures can substantially decrease a Bank's regulatory risk from ransomware events. ■

[1]Financial Crimes Enforcement Network, United States Treasury, FIN-2020-A006, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments (2020); https://www.fincen.gov/sites/default/files/advisory/2020-10-01/Advisory%20Ransomware%20FINAL%20508.pdf;

Office of Foreign Assets Control, United States Treasury, Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments (2020); https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

Mark Mangano is counsel with Jackson Kelly PLLC. Mark is an attorney focusing on strategic planning and bank regulatory issues. He has 26 years of experience as the CEO and owner of a community bank. You can contact Mark at mark.mangano@jacksonkelly.com or 304-284-4104.

Navigating the Pandemic — Where To From Here?

By Gary Shook, Community Bankers' Bank

In sitting down to write this article, I am reflecting upon what a year 2020 has been. We know 2021 will be different from 2020 but cannot predict the highs, the lows and the challenges coming our way next year.

We, as individuals, are fortunate to be living in a resilient democracy. We, as U.S. citizens, are resilient. Because of our resiliency, our banking system is also resilient. Regardless of the ups and downs of economic cycles and the effects they elicit, our banking system has always, in the end, remained a source of financial strength. With that said, we at Community Bankers' Bank (CBB) were curious as to how our bankers in the Fifth Federal Reserve District are processing the moving parts and pieces that 2020 has handed us thus far.

In late September, using an independent moderator, CBB convened several Zoom focus group calls consisting of banking executives from across the 5th District. We were eager to hear what they have experienced. We wanted to hear where they think the industry is going. In general, we wanted to listen to the good, the bad, and even the ugly, and that's what we heard. I want to share their opinions about our current circumstances, coupled with some reflection and forward-thinking.

CARES ACT/Payroll Protection Program

There was universal agreement within our focus groups that the Payroll Protection Program (PPP) brought new business opportunities to the community banking sector. Community banks offered a much-needed lifeline to small businesses within their communities, despite evolving PPP guidelines that were difficult to navigate the issues with the SBA loan application portal. Banks sprinted to deploy capital to small businesses when they needed it most. Bankers who participated in PPP were grateful to fellow employees, as well as their boards, for the nimbleness they exhibited by pivoting quickly to meet PPP demand.

We inquired whether our focus group institutions limited PPP loans to existing customers or opened the process to all qualified applicants. Responses ranged from 100% existing customers to 80% of applicants being new to the bank. With that said, a significant percentage of PPP loans were made to existing customers among our participants.

Bankers are working hard to "onboard" new relationships. With many retail and commercial banking offices being closed (due to COVID-19), keeping these new customers might be problematic. Some banks have tied sales goals to retaining new PPP customers. Others send weekly newsletters and various marketing communications to draw in new prospects and generate interest in a broader array of products and services.

When we questioned our focus groups as to guidance on PPP loan forgiveness, there was generally a dim view about the process. Some have elected to utilize technology to assist with forgiveness, but most banks plan to use existing resources. The SBA has made allowances for smaller loans of $50K or less. Our bankers are hopeful these loans will be forgiven, but there has been no legislative fix to ensure that. They hope small businesses and community banks are not put through more undue stress and aggravation. All focus group participants were eager to get the forgiveness aspect behind them.

Bricks and Mortar Branches Versus Mobile Banking

Most of the bankers said that considering the changes in delivery brought about by COVID-19, they would need to take advantage of growth opportunities. These may exist in branch structure and delivery.

We inquired whether our focus group institutions limited PPP loans to existing customers or opened the process to all qualified applicants. Responses ranged from 100% existing customers to 80% of applicants being new to the bank.

Early in the pandemic, all focus group participants closed their retail banking offices to foot traffic. Our bankers indicated that there had been little complaint in many cases, mostly because drive-up or walk-up banking options remained open. Many of our bankers said their customers were comfortable with "by appointment only" hours, and they would probably continue to offer that option on a go-forward basis. Customers welcomed and moved quickly to adopt mobile technology.

This begs the question as to changes in branch staffing going forward. Are there changes that need to be made? Do we need to outsource processes and procedures more aggressively? This appeared to present the great conundrum. Concerns were expressed as to the difficulty of maintaining culture with many staff members working remotely. Employee engagement and productivity on a go-forward basis is yet to be determined. Historically, attracting experienced and qualified talent can present challenges. Our focus group participants voiced concern about reducing headcount now because quality staff will be critical when banks return to more normal business operations post-pandemic. Focus group participants noted that mortgage and commercial bankers are in incredibly high demand.

One of the lasting effects on the banking model after COVID-19 will likely be an increased reliance on technology, especially for internet and mobile banking applications. Technology investments appear especially attractive for payments, lending, and security to ensure consumer data remains safe.

Budgeting and Liquidity

As you would expect, there was quite a bit of discussion on this topic within our focus group as leadership teams are currently building their 2021 Budgets and Strategic Plans. Higher liquidity levels in 2020 vs. 2019 have created challenges in deploying those new funds and maximizing returns. Should excess funds be directed toward loans and securities or retained in cash reserves?

Our bankers and board members at their respective institutions understand these decisions have implications for the net interest margin and income.

The loan portfolio mix was a topic of discussion, especially surrounding hospitality and non-owner-occupied office buildings. Those segments are under particular stress at present. Further discussion centered around loss reserves. Most of our focus group participants are not currently applying CECL standards in the determination of reserves. For now, our bankers' "gut" instincts were to increase reserves, even given the current resiliency in loan portfolios. This was deemed prudent, given the number of credit unknowns in 2021 and beyond.

How long current rates remain in place was another conversation topic, with the FRB signaling rate hikes are unlikely before 2023. Questions also exist as to budgeting on both sides of the balance sheet. While there was no agreement on every topic, there was agreement among our focus group participants that most banks will present three budget scenarios for 2021 — Maximum, Most Likely, and Minimum.

While we learned a great deal from our focus group participants, these are the key takeaways:

1. Community banks obtained new commercial customers because of PPP loans;

2. Bankers are unsure how sticky these new commercial relationships will be and have little confidence in the SBA forgiveness process;

3. PPP loans provided an opportunity for community banks to demonstrate their concierge approach to customer service versus the big bank approach;

4. Budgeting for 2021 is a challenge. It will be difficult for management to provide reliable numbers and projections to their Boards. Creating multiple budget scenarios seems to be the best approach; and,

5. Managing the personnel piece during COVID-19 has been one of the most challenging elements.

The final takeaway is that we must all be adaptable, flexible, and willing to embrace change as we move forward into what will undoubtedly be uncharted waters. It is possible that we must be even more proactive and creative in the face of that uncertainty. However, community bankers have demonstrated their resilience and devotion to serving their communities, customers, employees, and shareholders ■

Gary R. Shook currently serves as president and CEO of CBB Financial Corp and Community Bankers' Bank, which serves the Fifth Federal Reserve District; namely, South Carolina, North Carolina, Virginia, West Virginia, Maryland, and the District of Columbia. He is a trustee and member of the Executive Committee of the Virginia Foundation for Independent Colleges and a director and audit chair of Shrine Mont, The Cathedral Shrine of the Transfiguration and Conference Center. Mr. Shook holds a Bachelor of Arts degree from the University of Virginia.Contact Gary at gshook@cbbonline.com or 804.794.5885.

Avoiding CCPA Debt Collection Traps — A Periodic Reminder

By Russell Jessee and Sarah Ellis, Steptoe & Johnson PLLC

"Knowing where the trap is — that's the first step in evading it."

— Frank Herbert, Dune

Even after amendments over the past five years, the West Virginia Consumer Credit and Protection Act (the "CCPA") still has traps for the unwary creditor. Many times, when a debtor gets so far behind that he or she hires a lawyer, the lawyer combs the loan documents and scrutinizes the creditor's debt collection efforts to find technical CCPA violations. Creditors cannot always avoid these claims of technical violations but being aware of the following fertile areas for debtor claims is an excellent first step.

Late fees. West Virginia may be the only state that has a statutory dollar-amount cap on late fees. A monthly late fee can be no more than 5% of the installment amount and never more than $30. (W. Va. Code § 46A-3-112(1)(a) (precomputed loans); W. Va. Code § 46A-3-113(1) (non-precomputed loans).)

The key to avoiding charging more than permitted is to follow your contracts. The statutory dollar-amount cap increased to $30 from $15 in 2015. However, simply because the statute changed does not mean that you can now charge $30 (if 5% of the installment is more than that). Presumably, your post-2015 loan contracts reflect the increase to $30. If so, you get to charge up to the $30 cap. Pre-2015 loans likely reflect the then-effective $15 cap, and older loan documents may have even lower caps. For all pre-2015 loans, you're still limited to the contracted-for cap amount.

Default charges. West Virginia Code § 46A-2-115 establishes West Virginia's limits on default charges. Subsection (b)(2) lists the default charges that a consumer loan may include. One key thing to be aware of is that legal fees (other than specified trustees' fees) are not recoverable. Do not have any reference in your loan documents to recovering legal fees in the event of a default. Plaintiffs' lawyers will pounce on that, alleging that the very presence of the language is unconscionably coercive.

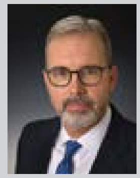
Subsection (b)(3) of the statute, listing the circumstances under which authorized default charges may be collected, has an interesting twist. A creditor cannot assess or collect authorized and contracted-for default charges unless, among other requirements, the charge is incurred after the last day allowed for a cure and "the holder of the consumer loan and the consumer have agreed to cancel any pending trustee's sale or other foreclosures on the real property securing the consumer loan." (W. Va. Code § 46A-2-115(b)(3)(C)-(D).) Those are curious requirements taken together. Read literally, a creditor may collect default charges incurred only after it is too late to cure and only if the foreclosure sale is canceled.

No reported decision construes the most recent amendments to the default charges statute, so this is an area to tread very, very carefully. The safest course is to reflect in your loan contracts the statutory language in subsection (b)(2) about which default charges are permissible and then assess and collect them only if you can comply with all the requirements of subsection (b)(3).

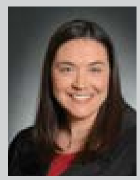
Debt collection calls. The CCPA now has safe harbors on debt collection calls. So long as you (i) make no more than 30 calls per week, (ii) speak to the debtor (or anyone) no more than 10 times per week, and (iii) call only between 8 a.m. and 9 p.m., you are presumptively safe. (W. Va. Code § 46A-2-125(d).) Of course, do not use any profane, obscene, or abusive language, and make sure that your callers identify themselves at the beginning of calls. (W. Va. Code § 46A-2-125(a)-(b).)

Also, if a debtor hires a lawyer in an effort to stop your debt collection, the debtor must notify you in writing (on paper or electronically) and identify their lawyer. (W. Va. Code § 46A-2-128(e).) You have 72 hours to stop debt collection after receiving such written notice, but you may continue to send regular account statements and required notices.

Requests for statements. A final trick to be aware of is that a distressed debtor may send a request for an account statement. West Virginia Code § 46A-2-114(2) requires that a creditor provide one free annual account statement upon written request. Rather than ignore such a request, assuming that the monthly account statements should be enough, it is best to respond with a full statement covering the previous 12 months promptly. ■



Russell Jessee is a member of the Charleston office of Steptoe & Johnson PLLC. He heads the firm's Business Litigation Group. Russell defends banks and other businesses in all manner of disputes and strives to reach resolutions that make business sense for his clients. He does not litigate for the sake of litigation. Rather, he seeks efficient resolution so clients can focus on what they do best — running their businesses. He can be reached at Russell.Jessee@Steptoe-Johnson.com or (304) 353-8103.



Sarah Ellis also is a member of the Charleston office of Steptoe & Johnson PLLC. Her love of business transactions stems from her childhood when she accompanied her dad, a real estate developer and contractor, to his office almost daily. In addition to transactions, Sarah works closely with banking clients on collateral, bankruptcy and collection issues. She can be reached at Sarah.Ellis@Steptoe-Johnson.com or (304) 353-8127.

Strategic Transactions With Outstanding PPP Loan and EIDL Obligations

By Matthew Kingery, Lewis Glasser PLLC

As readers of this article are well aware, borrowers will sometimes engage in strategic transactions (e.g., mergers, asset sales, membership or stock redemptions, etc.). The Paycheck Protection Program (PPP) and the Economic Injury Disaster Loan program (EIDL) require special attention when borrowers engage in strategic transactions. This article considers the role of the lender and the role of borrowers in strategic transactions involving these loan programs.

PPP

PPP provided short term financial assistance to small businesses dealing with the impact of the COVID-19 pandemic. The program originated in Congress in March 2020 as part of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and was intended to guarantee eight weeks of payroll and other costs to help those businesses remain viable and allow their workers to pay their bills. PPP restarted on April 24, 2020, following the appropriation of new funding, and the PPP Flexibility Act of 2020 relaxed many PPP loan guidelines. The original deadline to apply for a PPP loan was June 30, 2020, but was extended through Aug. 8, 2020, by legislation signed on July 4, 2020.

The PPP loan forgiveness process has begun. Important changes to PPP loan forgiveness came with the PPP Flexibility Act of June 5, 2020. All or part of a PPP loan could be forgiven provided the borrower kept all full-time equivalent employees on the payroll or rehired them within 24 weeks of receiving the loan or by Dec. 31, 2020, whichever comes first. To be eligible for forgiveness, payroll costs must be 60% or more of the amount forgiven. Eligible non-payroll expenses may only constitute 40% of the amount forgiven, and forgiveness will not occur until the end of the 24-week period of employment following receipt of the loan.

EIDL

PPP is one of two programs designed to help small businesses during the COVID-19 pandemic. In addition to PPP, the Economic Injury Disaster Loan program (EIDL) is also intended to help struggling businesses weather the COVID-19 pandemic. As opposed to being designed to help companies retain workers, EIDL helps small businesses overcome the loss of revenue during a declared disaster such as an extreme weather event, a fire, or recently become the case of the COVID-19 pandemic. The program was initially open only to agricultural businesses. The EIDL program reopened to eligible borrowers on June 15, 2020. Many small businesses were eligible for both loan programs subject to specific rules about the use of loan proceeds.

The impact of strategic transactions on PPP and EIDL loans

In addition to spending many long days entering application data into the portal, interpreting rules and regulations, and beginning the forgiveness process, many of the readers of this article have been

While there is no formal guidance from the SBA, PPP borrowers need to determine if a consent or waiver of default on the PPP loan is necessary when considering a strategic transaction. The PPP loan program is a product of the SBA's 7(a) business loan program governed by Section 7(a) of the Small Business Act, the SBA Standard Operating Procedures, SBA regulations and SBA Procedural Notices.

contacted by borrowers about various transactions and the impact of having a PPP or EIDL loan. As can be expected, some borrowers under these programs have contemplated or engaged in mergers, asset sales, membership or stock redemptions and other transactions.

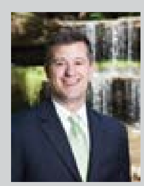
While there is no formal guidance from the SBA, PPP borrowers need to determine if a consent or waiver of default on the PPP loan is necessary when considering a strategic transaction. The PPP loan program is a product of the SBA's 7(a) business loan program governed by Section 7(a) of the Small Business Act, the SBA Standard Operating Procedures, SBA regulations and SBA Procedural Notices. Many of these rules also apply to the PPP loan program, in addition to the rules established specifically for the PPP loan program. SOP 50 57 2 provides that, after the full disbursement of loan proceeds, certain actions will require SBA's prior written approval. These actions include a "(c)hange in the ownership of a Borrower in the first 12 months after the final disbursement." This requirement applies to "any adjustment to or change in the ownership of a Borrower, including a change in percentage of ownership, for 12 months after final disbursement on any loan." Assumptions of PPP loans that release the original borrower also require SBA approval. In the absence of consent or a waiver of a default, a PPP borrower could potentially forfeit its ability to obtain loan forgiveness.

The EIDL loan program has been in existence for decades and is governed by Section 7(b) of the Small Busines Act and carries a different set of regulations from the Section 7(a) rules that govern PPP loans. Also, unlike PPP loans, which involve a private party lender, EIDL loans are funded and administered by the SBA. EIDL loans also have a loan term of up to 30 years, unlike the short-term PPP loans, making it more likely that a strategic transaction involving the borrower will arise during the life of the EIDL.

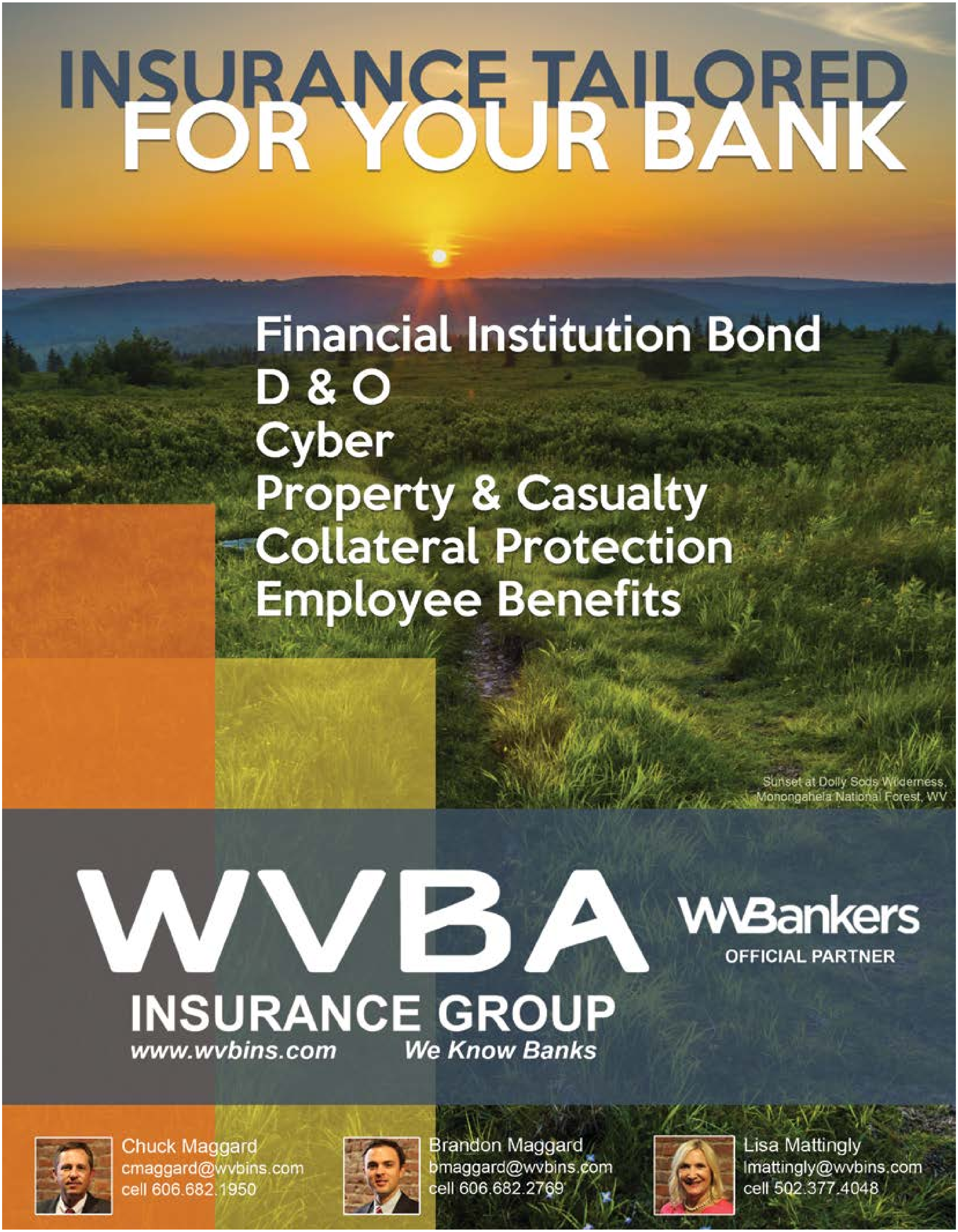
EIDL promissory notes provide that the borrower is in default if it "(r)eorganizes, merges, consolidates, or otherwise changes ownership or business structure without SBA's prior written consent." Also, the SBA requires collateral to secure all EIDLs over $25,000.00, often taking a blanket security interest in all of the borrower's tangible and intangible personal property, in addition to any real estate collateral. The EIDL security agreement provides that the borrower "will not sell, lease, license or otherwise transfer (including by granting security interests, liens, or other encumbrances in) all or any part of the Collateral or Borrower's interest in the Collateral" without SBA's written approval. EIDLs under $200,000 do not require personal guarantees. Still, for transactions of $200,000 or more, under SOP 50 30 9, the addition or deletion of a guarantor is a material change to an EIDL that requires SBA's approval and possibly a loan document modification.

Summary

All parties to a strategic transaction involving a small business with an outstanding PPP loan or EIDL, including the PPP lender, have a stake in ensuring the SBA has been notified of and has approved the transaction when required. As you might expect, the SBA has been overwhelmed with PPP loan and EIDL requests and forgiveness applications. Accordingly, contacting the SBA from the outset of a strategic transaction should be one of the first due diligence tasks engaged in by the parties to the transaction. ■



Matthew Kingery is of counsel with Lewis Glasser, PLLC, in Charleston, West Virginia. Matt devotes his practice to commercial transactions, lender representation, commercial development, distressed assets and real property matters with an emphasis on title, acquisitions, sales and financing issues. Matt has been recognized for his work in the legal industry and community and has received numerous awards, including being selected multiple times in Super Lawyers® in the practice area of real property law; named the 2010 West Virginia State Bar Young Lawyer of the Year; honored as a recipient of the 2009 Generation Next 40 Under 40 award by The State Journal, and named a Young Gun by the West Virginia Executive in 2017. He can be reached at mkingery@lewisglasser.com.

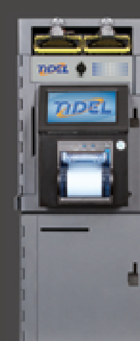

INSURANCE TAILORED
FOR YOUR BANK
Financial Institution Bond
D & O
Cyber
Property & Casualty
Collateral Protection
Employee Benefits
Sunset at Dolly Sods Wilderness, Monongahela National Forest, WV
WVBA
INSURANCE GROUP
www.wvbins.com
We Know Banks
WVBankers
OFFICIAL PARTNER
Chuck Maggard
cmaggard@wvbins.com
cell 606.682.1950
Brandon Maggard
bmaggard@wvbins.com
cell 606.682.2769
Lisa Mattingly
lmattingly@wvbins.com
cell 502.377.4048

The Single Source Provider for ATM and Armored Car Needs

We are helping financial institutions drive efficiencies, lower risk and liability burdens, control cost and grow business. We deliver these benefits to you by competently and effectively providing the following end-to-end solutions:

- **Cash Replenishment / Courier Services**
- **First and Second line ATM maintenance**
- **ATM Management and Total Outsourcing** (We own and operate the ATM Fleet for you, including vault cash and transaction processing)
- **ATM Rentals** (Events like county fairs, festivals, etc.)
- **ATM, ITM, TCR Sales/Service**
- **Smart Safe Program** (Remote Deposit Capture for Cash)

Over the years ATM Solutions has evolved into a leading provider of turnkey solutions. These solutions combined with owning and operating our own armored fleet create a uniquely good experience for your customers, and employees alike.



ATM Solutions Inc.™ One Source, One Solution

Frank Peagler | 724-771-3213 | **frank.peagler@atm-solutions.com** | www.atm-solutions.com

Six Ways the COVID-19 Pandemic Has Changed the Delivery of Financial Services

By Nicholas P. Mooney II and Angela L. Beblo, Spilman Thomas & Battle

The COVID-19 pandemic has touched virtually every facet of life. It isn't surprising that it also has changed the way banks deliver financial services to their customers. Below are six ways the pandemic is reshaping banking.

1 Forbearance and related debt relief. The CARES Act, passed in March 2020, provided protections to borrowers with federally backed mortgages. Those include mortgages held or backed by the Federal Housing Administration, the United States Department of Veterans Affairs, the United States Department of Agriculture, the Federal National Mortgage Association (also known as Fannie Mae), and the Federal Home Loan Mortgage Corporation (commonly known as Freddie Mac). There are two important aspects of the CARES Act with respect to mortgages:

First, servicers and lenders are prohibited from foreclosing from March 18, 2020, until Dec. 31, 2020. This includes both judicial and non-judicial foreclosures. Further, it includes any foreclosure in process on March 18, 2020, as lenders and servicers are prohibited from finalizing any foreclosure judgment or sale. This is a mandatory provision, and there are no steps a homeowner must take to obtain this relief.

2 Second, homeowners may affirmatively request forbearances for their loans. If a homeowner is experiencing financial hardship due to COVID, the homeowner may request a forbearance for up to 180 days. Also, a homeowner may request a second forbearance of up to 180 additional days. Thus, in total, a homeowner may request a forbearance for up to 360 days. The burden is on the homeowner to make the request to the servicer or lender. If a homeowner requests a CARES Act forbearance, there "will be no additional fees, penalties or additional interest (beyond scheduled amounts) added to" the loan. Homeowners are not required to submit documentation to prove a COVID-related hardship other than the initial claim that financial hardship is related to COVID. There is a Dec. 31, 2020, deadline for the initial request to be made for some of the federally backed mortgages.

The way people bank has changed. As the pandemic hit and states forced their citizens into lockdowns, peoples' banking choices were necessarily affected. For many, the ability to visit a physical branch was greatly curtailed, if not altogether prohibited. As a result, they turned to their banks' digital offerings. One commentator reported a 200% jump in new mobile banking registrations in the early days of the pandemic, coinciding with an estimated 50% drop in branch traffic during the same period. While millennials traditionally have led the charge on digital banking, older generations aren't being left behind. Indeed, according to Donna Turner, COO of Early Warning, which operates the popular Zelle peer-to-peer payment app, since the onset of the pandemic, baby boomers have "been the faster-growing demographic."

3 "The end of cash has never been closer." As reported by a recent EY Future Consumer Index, the use of cash has been on the decline, but the onset of the pandemic has quickened it. Consumers have a concern over whether handling physical cash can spread the coronavirus. That concern has translated into a sizable drop in cash usage. Further, EY reports that this drop may not be temporary. Of those who responded to the EY survey, at least 20% expect to continue using less cash for the foreseeable future. This drop will likely be attributed to the rise in mobile and contactless payments, which we discuss next.

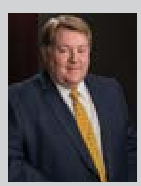
4 The rise of contactless payments. Before the pandemic, contactless and mobile payments were already on the rise. The onset of the pandemic accelerated their adoption. VISA's Back to Business Survey, a global survey of small businesses and consumers, demonstrates how customers' payment habits have changed due to the pandemic. The survey reported that 78% of consumers changed how they pay for an item to reduce contact. Nearly half of consumers (46%) responded that contactless payment methods are among the most critical safety measures they look for when deciding how to shop and what payment methods to use. About the same amount (48%) would not shop at a store that only offers payment methods that require contact with a cashier or shared device.

The way people bank has changed. As the pandemic hit and states forced their citizens into lockdowns, peoples' banking choices were necessarily affected.

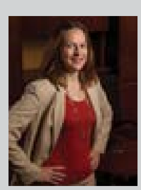
5 Remote online notarization and digital mortgages. Digital mortgage originations and closings were already in the works before the pandemic hit. The move toward digitizing the mortgage process started years ago as states began passing laws permitting remote online notarization (RON). The passage of those laws gained steam last year, while lenders also began investing in technology to compete with those already in the digital mortgage space. The pandemic has prompted states to accelerate their adoption of RON laws. However, there still are hurdles to overcome before completely digital mortgage originations and closings can be a standard in the industry. RON laws vary from state to state, and some are temporary legislation meant only to bridge the gap during the pandemic.

6 Changes in attitude toward debt. The pandemic has forced consumers to consider financial basics like how they handle debt. Although consumers still use credit cards, their uncertainty about potential job loss or pay cuts has caused them to use those cards differently. According to the Federal Reserve's Survey of Consumer Finances, in 2019, 45% of American families had outstanding credit card debt. Since the pandemic onset, consumers have focused on shedding as much of that debt as possible. At the start of 2020, Americans owed approximately $1.09 trillion in credit card debt. By July 2020, that amount was down to $99.5 billion as consumers reduced discretionary spending and used part or all stimulus checks to reduce credit card debt. ■

Nick Mooney and Ang Beblo serve as co-editors of Spilman's financial litigation-focused e-newsletter, All Consuming.



Nick's primary area of practice is consumer financial services litigation in federal and state courts. He also co-chairs the firm's technology law practice group and serves as co-editor of the firm's technology law-focused e-newsletter, Decoded. He can be reached at 304.340.3860 or nmooney@spilmanlaw.com.



Ang's primary areas of practice are consumer finance and litigation. She is counsel in the firm's Charleston, West Virginia office. She can be reached at 304.340.3852 or abeblo@spilmanlaw.com.


yhb
CPAs & Consultants
COMMITTED TO COMMUNITY
YOUR PARTNER IN COMMUNITY BANKING & BEYOND


DR. POLING


DR. MARSHALL


DR. HURST

Executive Health exams go far beyond an annual physical. We combine the very latest in advanced technology and wellness planning to design a personalized program that an individual simply can't find in a physician's office or hospital setting.

Our mission is to provide busy individuals with an efficient way to receive a confidential, comprehensive, whole body assessment with a focus on preventative medicine in a relaxing, resort atmosphere. The focus on prevention facilitates early detection of disease. Earlier detection leads to a significant improvement in the rate of cure. Staying ahead with preventive health care makes better sense than ever before.

FOR MORE INFORMATION

To book an appointment, call 1-800-362-7798, Ext. 372
or email us at info@greenbrierclinic.com

The Greenbrier
EXECUTIVE HEALTH®

40823 Midland Trail, East, White Sulphur Springs, WV 24986 | GreenbrierClinic.com

Cloud Computing

Security Considerations

By Chris Joseph, Arnett Carbis Toothman

Introduction. Cloud computing services have been a part of financial institutions for several years. The reasons for utilizing cloud computing services have been discussed over those years, so we are not going to address the reasons in this article. We are going to focus on the security considerations, as the use of cloud computing services has increased significantly in the delivery of products and services in the financial services industry.

With the increased use comes risk. Recognizing the risks, the FFIEC recently issued a joint statement titled "Security in a Cloud Computing Environment." The statement indicated, "Financial institution management should engage in effective risk management for the safe and sound use of cloud computing services. Security breaches involving cloud computing services highlight the importance of sound security controls and management's understanding of the shared responsibilities between cloud service providers and their financial institution clients." The statement does not contain new regulatory expectations but addresses risk management practices that should be considered.

Background. As with other vendor arrangements, when engaging a cloud service provider, the financial institution should conduct effective vendor management over the relationship. As indicated by the FFIEC, "Due diligence and sound risk management practices over cloud service provider relationships help management verify that effective security, operations, and resiliency controls are in place and consistent with the financial institution's internal standards. Management should not assume that effective security and resilience controls exist simply because the technology systems are operating in a cloud computing environment." The vendor management entails the contract review that documents the services, expectations, uptime requirements, controls, etc.

Continued on page 32

Continued from page 30

When entering into a cloud service provider relationship, the financial institution and the cloud service provider share the responsibilities. However, the protection of customer information resides with and is the responsibility of the financial institution.

Ongoing management and monitoring of the cloud service provider's overall service is critical for the financial institution's overall risk management process.

Cloud computing environments utilize virtualization in the delivery of cloud services. Different cloud computing environments are used by financial institutions, including private cloud computing environments, public cloud computing environments or a hybrid of the public and private computing environments. There are three cloud service models:

- **Software as a Service (SaaS)** — The software application used by the financial institution (i.e., the applications) operates on the cloud service providers cloud infrastructure. The financial institution's primary responsibility is for the user-specific application configuration settings, user access, risk management of the overall relationship, etc. The application updates and cloud infrastructure maintenance is the responsibility of the cloud service provider.

- **Platform as a Service (PaaS)** — The PaaS model adds additional responsibilities to the financial institution. The PaaS model is used when the financial institution "deploys internally developed or acquired applications using programming languages, libraries, services, and tools supported by the cloud service provider," as indicated in the FFIEC joint statement. In addition to the risk management that exists with SaaS, the financial institution is responsible for providing and configuring the cloud platform resources. The financial institution's responsibilities include controls over the development, deployment and administration of the applications. The cloud service provider's primary responsibilities include network, servers, operating systems, storage, etc.

- **Infrastructure as a Service (IaaS)** — The cloud service provider supplies the IaaS model's infrastructure. The financial institution implements the system software, including the operating system. The financial institution is responsible for most of the items related to the solution, including the cloud platform resources configuration. The financial institution is also responsible for implementing and managing controls over operations, applications, operating systems, data and data storage. The cloud service provider is primarily responsible for the overall infrastructure, including the physical data center.

When entering into a cloud service provider relationship, the financial institution and the cloud service provider share the responsibilities. However, the protection of customer information resides with and is the responsibility of the financial institution.

Risks Management. When a financial institution executes outsourcing arrangements, it is critical that the financial institution clearly understand the roles and responsibilities of both the outsourced vendor (i.e., cloud service provider) and the financial institution. The understanding of the duties will assist the financial institution with its overall risk management program. As indicated previously, the overall responsibility of protecting customer information is with the financial institution.

Several areas should be included in the risk management process when utilizing a cloud service provider. Many controls need to be considered, some of which are common in other areas, including:

- **Governance** — The overall cloud computing services strategic plan should support and work in conjunction with the overall strategic plan.

- **Cloud Security Management** — As indicated previously, ongoing oversight and monitoring of the cloud computing service provider is part of the financial institution's vendor management program. The monitoring should be based upon the terms of the contract with the cloud service provider that was negotiated and reviewed in detail before executing the contract. Other areas of Cloud Security Management include:
  - Inventory process for systems and information assets residing in the cloud computing environment
  - Security configuration, provisioning, logging and monitoring
  - Identity and access management and network controls
  - Security controls for sensitive data
  - Information security awareness and training programs

- **Change Management**
  - Change management and software development life cycle processes.
  - Microservice architecture — Utilizes smaller, lighter-weight code to facilitate faster software development and ultimate deployment. The financial institution needs to ensure that they understand the overall security requirements and concerns with microservices.

The financial institution is also responsible for implementing and managing controls over operations, applications, operating systems, data and data storage. The cloud service provider is primarily responsible for the overall infrastructure, including the physical data center.

- **Resiliency and Recovery**
  - Business resilience and recovery capabilities — The business resilience and recovery should be appropriate for the cloud computing service's risk.
  - Incident response capabilities, including the challenges introduced in a cloud computing services arrangement (how to address technology assets owned and managed by the cloud service provider).

- **Audit and Controls Assessment**
  - Regular testing of financial institution controls for critical systems (should be included in the standard audit schedule).
  - Oversight and monitoring of cloud service provider-managed controls. The financial institution should evaluate and monitor the cloud service provider's applicable controls. As in other vendor management arrangements, while the responsibility to perform controls can be outsourced, the accountability for protecting customer information is with the financial institution.

There are also some controls unique to cloud computing services, including:

- **Management of the Virtual Infrastructure** — Secure virtual infrastructure is managed through cloud security tools. The control over those tools is the responsibility of the cloud service provider. The financial institution should gain an understanding and verify the cloud service provider controls are working as intended.

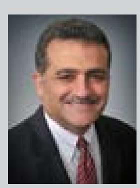
- **Use of Containers in Cloud Computing Environments** — Use of containers provides many advantages, including portability and less demand on resources. However, containers share the same kernel presenting potential security risks.

- **Use of Managed Security Services for Cloud Computing Environments** — Consider leveraging other security tools and services.

- **Consideration of Interoperability and Portability of Data Services** — Interoperability and portability capabilities should be considered related to the financial institution's overall strategic plan and risk appetite.

- **Data Destruction or Sanitization** — Financial institutions should ensure the data destruction and sanitization policies and procedures follow their policies and documented in the service level agreement.

Conclusion. With the continued increase in cloud computing services, financial institutions should ensure that their overall risk management program considers the services outsourced and the various risks associated with the cloud computing service. Understanding the controls at both the financial institution and the cloud service provider should be understood, tested and monitored. ■



Chris Joseph is a partner of Arnett Carbis Toothman LLP, located in the Charleston, West Virginia office. A Certified Public Accountant, Certified Information System Auditor, certified in Risk and Information Systems Control and certified as an Information Technology Professional, Mr. Joseph has over 35 years of experience in information technology audit and security services in the financial institutions industry.Mr. Joseph can be contacted at 800-642-3601 or through email: chris.joseph@actcpas.com.

Calendar of Events

January

28 & 29	Commercial Lending Development Program (CLDP) (Stonewall) – Parts 1 & 2

February

3	IRA Basics (Virtual)
4	IRA Advanced (Virtual)
23	Legislative Day (Charleston Marriott)
25 & 26	Commercial Lending Development Program (CLDP) (Stonewall) – Parts 3 & 4

March

8 & 9	Compliance School (Four Points/Charleston)
10	Emerging Leaders (Sam Bowling)
24 & 25	Commercial Lending Development Program (CLDP) (Stonewall) – Parts 5 & 6
30 & 31	Branch Management School Series (Virtual)

April

21	A/L Investments Seminar (Sam Bowling)

May

3 & 4	Credit Management Conference (Stonewall)
5 & 6	Bank Security School (Stonewall)
13	Financial & Estate Planning (Edgewood Country Club/Charleston)
13 & 14	Commercial Lending Development Program (CLDP) (Stonewall) – Parts 7 & 8
23 - 28	West Virginia School of Banking (University of Charleston)
23 – 28	Lloyd P. Calvert Graduate School of Banking (University of Charleston)

July

25 - 27	WVBankers/Ohio Bankers League 2021 Joint Convention

August

30	Emerging Leaders (Stonewall)
31 & Sept 1	Branch Management School Series (Stonewall)

September

16	Human Resource Management for Bankers (Sam Bowling)
24	Disaster Preparedness (Stonewall Resort)

October

4 & 5	BSA/AML School Fundamentals (Stonewall)
6 & 7	BSA/AML School Advanced (Stonewall)

November

TBD	CEO Conference
15 & 16	Consumer Lending Conference (Beginner) (Four Points)
17	Consumer Lending Conference (Advanced) (Four Points)
TBD	CFO Conference (Charleston Marriott)

Webinars — Live and Recorded

Visit our website for specific dates and topics.

www.wvbankers.org

Graduate School of Banking Online Senior Management Seminars

Visit **www.gsb.org** or our website as updates are added.

WEST VIRGINIA

BANKER

Advertiser Index

Arnett Carbis Toothman....IBC
ATM Solutions....25
Baker Group....IFC
Bankers Bank of Kentucky....11
Bankers Healthcare Group....20
Boenning & Scattergood....19
Bowles Rice....3
Community Bankers Bank....13
Deluxe....5
Greenbrier....29
Spilman Thomas & Battle....OBC
S.R. Snodgrass....31
Suttle & Stalnaker....7
WVBA Insurance Group....24
YHB....28
Zeno, Pockl, Lilly and Copeland....21

WEST VIRGINIA
BANKER

3601 MacCorkle Avenue, SE, Suite 100
Charleston, WV 25304

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