WEST VIRGINIA

BANKER

WINTER
2021

5
The West Virginia Young Banker of the Year Award

18
What are Consumers' Top Cybersecurity Concerns?

28
Checking In on the Banking Industry

The Baker Group Is Here to Help

FREE TRIAL

The BakerGroup

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.

Bond Accounting – 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 financial institution, contact Ryan Hayhurst with our Financial Strategies Group at **800.937.2257**, or Ryan@GoBaker.com.

Member: FINRA and SIPC

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

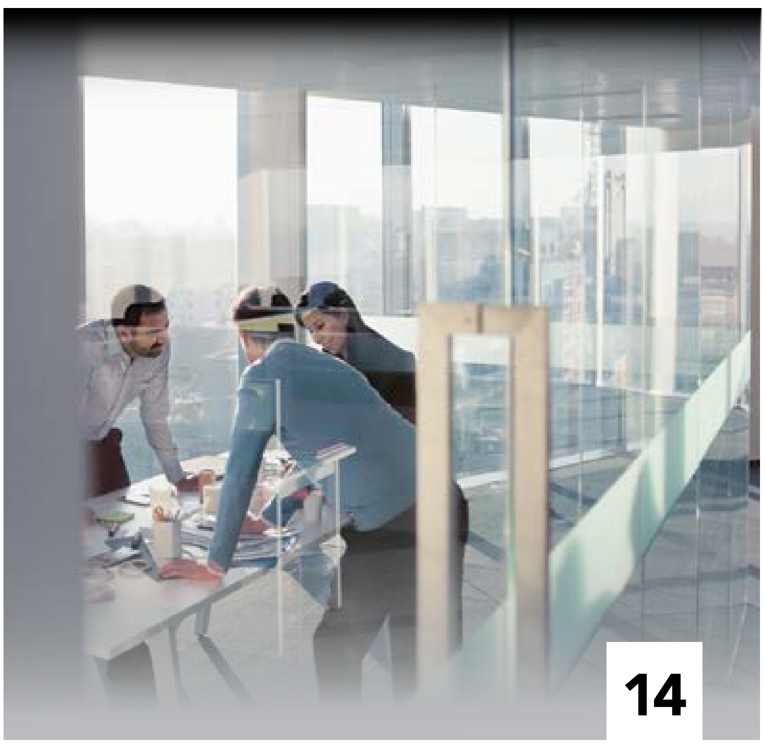
Ryan@GoBaker.com

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



A MESSAGE FROM THE CHIEF EXECUTIVE

By Sally Cline

West Virginia Young Banker of the Year Award

The West Virginia Bankers Association has embarked on an exciting effort to grow the next generation of banking leaders.

Recognizing a need to assist our member banks in developing high-potential employees with the leadership skills and tools necessary to address the challenges facing our industry, WVBankers formed an Emerging Leaders Program in 2014. The program has been quite successful: 95 talented and motivated individuals have graduated and positively impacted their organization – financially, socially, and intellectually. The 12-month blended learning program, which requires online participation and attendance at full-day programs, is designed to develop the next generation of financial leadership. Focus areas include leadership, communication, influence, advocacy, individual development planning, and community service.

A small group of Emerging Leader graduates who had developed relationships through the program approached us in 2017 about forming a Future Leaders Council to encourage sustained commitment, loyalty and active engagement in matters that affect the banking industry and its customers. The Future Leaders Council consists of 10 members. I'd like to recognize them individually for their passion and dedication to identify and promote educational opportunities for developing leaders across the state:

Brian Cayton, *Community Bank of Parkersburg, Past Chairman*

Chris Davis, *Community Bank of Parkersburg*

Hoy Ferguson, *Davis Trust Company*

Erika Lee, *Poca Valley Bank*

Jared Moncman, *Pleasants County Bank, Chairman*

Gabby Newcomer, *FNB Bank*

Felicity Ours, *Summit Financial Group*

Holly Terrell, *First Neighborhood Bank, Secretary*

Chase Thomas, *Clear Mountain Bank, Treasurer*

Angie Zirk, *Summit Financial Group*

The Future Leaders Council provides its members the opportunity to share ideas with their peers, gain valuable career insight from member bank CEOs, and learn from industry speakers. In addition to furthering leadership skills and career development, the Council's events provide a fantastic opportunity to get to know other bankers and build relationships within the industry. Members are also encouraged to meet and foster relationships with their legislators at events such as the WVBankers Legislative Day in Charleston and the WVBankers/ABA Government Relations Summit in Washington, D.C.

The Future Leaders Council meets quarterly and recently presented a proposal to WVBankers board of directors to establish a West Virginia Young Banker of the Year award. This award will recognize one outstanding West Virginia banker employed by one of the Association's member banks. The award will officially identify a young banker who has excelled in learning, leadership, and service. Candidates must be under the age of 40 with more than one year of banking experience, and must be nominated by a member bank executive officer between January 1 and April 30, 2022. The winner, selected by the WVBankers board of directors, will be recognized and honored at our 2022 Annual Meeting and Convention.

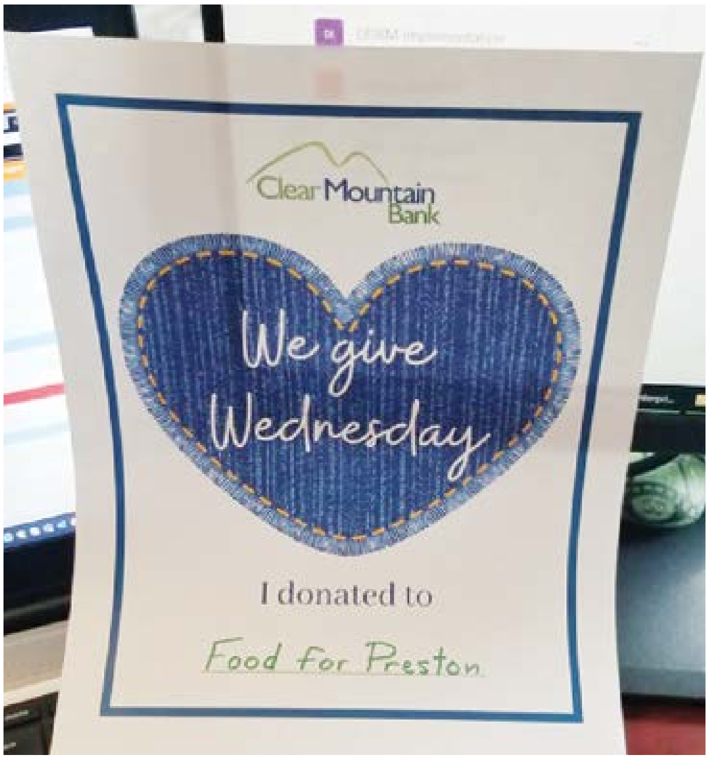
I am sure each of you can identify a rising star within your organization. They are high performers who demonstrate the desire, capacity, and initiative to make a significant contribution to the success of your bank. They are forward-thinking, adaptable, and innovative and have an innate ability to inspire and influence others toward achieving a common goal. They are driven to accomplish remarkable things.

WVBankers is doing exciting work to develop, connect and engage the next generation of banking leaders. Our goal is to deepen the connection between emerging leaders and the Association, deepen connections within the banking industry, and foster connections with industry professionals and elected officials.

Engaging and developing the next generation of bank leaders is critical to our industry's success. The future of our industry depends on having bright, energetic, and qualified individuals leading our banks well into the future, which is why our emerging leader engagement is one of our top priorities. ■

CLEAR MOUNTAIN BANK

Clear Mountain Bank recently had a Team Member Appreciation Week with each day having a theme. Wednesday was "We Give Wednesday." Each team member was given $30 to donate to a local United Way agency of their choice. On this day, the bank donated a total of $5,000.



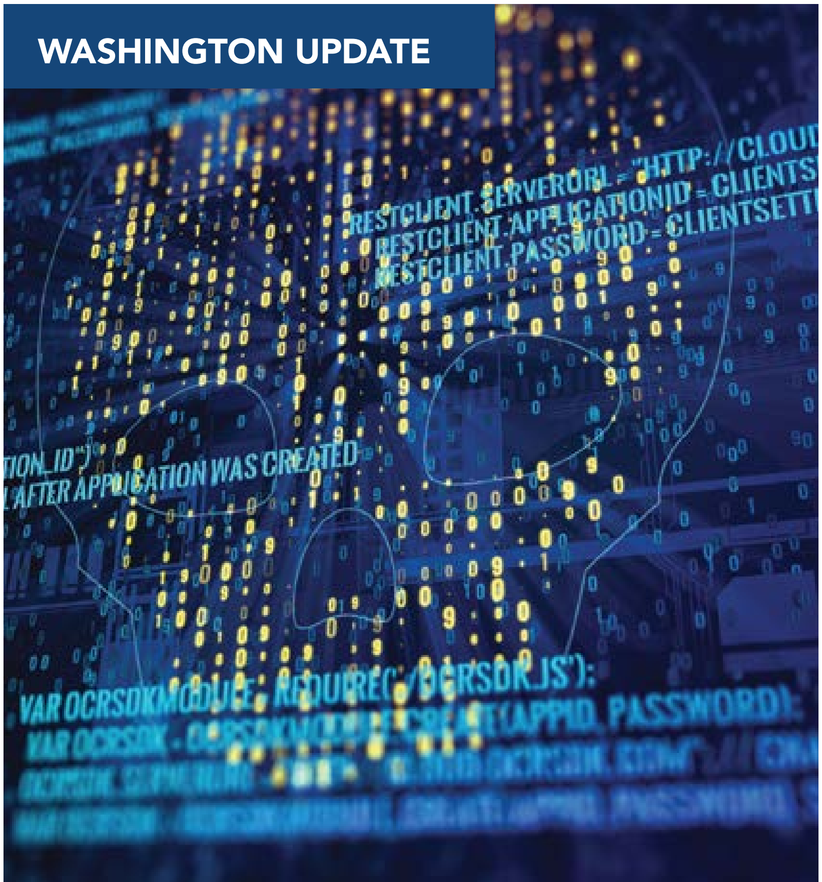
PEOPLES BANKS

Peoples Bank partnered with Mountaineer Food Bank on a $40,000 donation campaign in September, which is Hunger Action Month, and to celebrate Mountaineer Food Bank's 40th. Anniversary and Peoples Bank's acquisition of Premier Bank. Peoples Bank matched the first $20,000 in donations. A grand total of over $42,000 was raised in the campaign.

Pictured (left to right): Tyler Wilcox, Peoples Bank EVP, Community Banking, Ben Toller, Peoples Bank AVP, Gassaway Branch Manager, Staci Matheney, Peoples Insurance Agency President, Chad Morrison, Mountaineer Food Bank CEO, Ryan Welch, Peoples Bank VP, Huntington Regional Manager, and Heather Lloyd, Peoples Bank Flatwoods Branch Manager.

FARMERS BANK

The employees at Farmers Bank purchased and delivered gift baskets of snacks for healthcare workers at our area hospitals, ERs and urgent cares as a gesture of support and encouragement as they face such difficult challenges



To Pay or Not to Pay:

Ransomware Attacks Offer an Unsavory Choice

By Rob Nichols, American Bankers Association

It's the message a CEO never wants to receive: "We've got your data and you need to pay up if you want it back."

Unfortunately, that message is landing in CEO inboxes increasingly often, as ransomware attacks ramp up in the U.S. In just the first six months of 2021, the Financial Crimes Enforcement Network identified $590 million in ransomware-related Suspicious Activity Reports – a 42% increase from the 2020 total of $416 million. And FinCEN reports that we could be on track to see a higher transaction value for ransomware-related SARs than we've seen in the past 10 years combined.

Ransomware attacks – which use malware to encrypt files on a computer or mobile device and render it unusable until a ransom is paid – present companies with an unsavory dilemma: pay a ransom to a criminal actor, or lose a potentially devastating amount of data, which could seriously compromise business operations.

These kinds of attacks are evolving quickly in sophistication and scope, and virtually any business could be targeted at any time. What's perhaps most concerning is that criminal actors are increasingly targeting critical infrastructure entities, as we saw in the Colonial Pipeline incident earlier this year that caused a shutdown of a major East Coast oil provider. They've also begun branching out into "extortion-ware," in which the hacker not only encrypts sensitive data but then goes the extra step and threatens publicly to release it unless the institution complies with their demands.

Given the potential operational and reputational consequences of these types of cyberattacks, banks need to have a plan in advance for how they'll respond. There are a number of factors to consider.

First, while most companies choose to pay – cyber insurer Marsh McLennan reports that more than 60% of ransomware victims pay the requested ransom – it's not always guaranteed that the encrypted data will be fully restored. In fact, one survey of more than 5,000 I.T. decision-makers worldwide found that about half of those who did pay a ransom only recovered 65% of their compromised data. Twenty-nine percent said they only recouped about 50%.

And even if a company's ransom hacker unlocks all the encrypted data after the ransom is paid, the company will still need to take steps to clean that data and ensure it can't be easily re-encrypted.

On the other hand, there are also several good reasons not to pay a ransom. There are the societal costs to consider – paying the ransom could perpetrate attacks on other institutions or

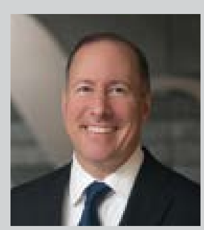
ABA in October released a new Ransomware Toolkit, which provides helpful guides for protecting your bank against ransomware attacks, responding in the event of an attack, and determining whether to pay a ransom.

entice the hacker to hit you again for more money. Paying a ransom could also erode trust from customers and business partners, as payment could signal a lack of continuity planning and preparation.

Either way, the first time you think about ransomware attacks and how to handle them should not be after your bank has fallen victim to one. To that end, ABA in October released a new Ransomware Toolkit, which provides helpful guides for protecting your bank against ransomware attacks, responding in the event of an attack, and determining whether to pay a ransom. The toolkit can be downloaded at aba.com/ransomware.

Ransomware represents a serious threat to all businesses. But the good news is that the financial sector is ahead of the game when it comes to cybersecurity, given the rigorous regulatory framework to which banks adhere. After all, as we found in a recent ABA/Morning Consult poll, consumers overwhelmingly trust banks the most to keep their personal information safe and secure.

By addressing the problem of ransomware head-on and taking prudent steps to prepare, we can help our industry maintain its reputation as the "gold standard" for data protection. ■



Rob Nichols is the president and CEO of the American Bankers Association, which represents banks of all sizes and charters and is the voice for the nation's $20 trillion banking industry. Rob joined ABA in August 2015 following ten years at the helm of the Financial Services Forum, a non-partisan financial and economic policy organization. Before joining the Forum, Rob served in the George W. Bush administration as the assistant secretary for public affairs at the Treasury Department, a position requiring confirmation by the United States Senate. Contact American Bankers Association at 1-800-226-5377 or support@aba.com. Or email Rob at nichols@aba.com.

ARE YOU READY FOR GROWTH?
ADVERTISE IN THIS MAGAZINE TO
ROCKET YOUR BUSINESS FORWARD.
THE newsLINK group
727.475.9827 | 855.747.4003
kris@thenewslinkgroup.com

Cryptocurrency and the Future of Banking

By Patrick McGraw, Baker Tilly

In June 2021, El Salvador's Legislative Assembly voted to become the first country to accept Bitcoin as legal tender, with Cuba following suit in August 2021. While Bitcoin is widely regarded as the premier cryptocurrency, the rise in Bitcoin's use over the past decade has paved the way for numerous other cryptocurrencies to come to fruition. The rise in the price of Bitcoin has helped legitimize cryptocurrency in the eyes of those who once thought it was nothing more than a financial fad.

In May 2021, the Federal Deposit Insurance Corporation (FDIC) issued a press release announcing it is gathering information and soliciting comments from interested parties about the insured depository institution's current and potential digital asset activities. The FDIC issued a request for information (RFI) to help inform its understanding of the industry's and consumer's interest in this area. In the release, FDIC Chairman Jelena McWilliams said, "At the FDIC, we are laying the foundation for the next chapter of banking by ensuring we have a regulatory framework that allows responsible innovation to flourish. Digital assets are one area in which we have seen rapid expansion and innovation in recent years. This RFI allows us to gain additional insight into the market and what role banks might play in the future." The press release provides evidence that the FDIC is seriously beginning to consider what cryptocurrency's role will be in the future of banking.

According to a December 2020 study survey performed by Cornerstone Advisors, 15% of U.S. consumers own some form of cryptocurrency, and 60% of those cryptocurrency owners said they would use their bank if it offered them the opportunity to invest in cryptocurrencies. Banks have been hesitant thus far to provide cryptocurrency investment services, in part because of its volatility and reputation of being associated with criminal acts. However, this chain of thought would infer that banks do not offer investments with significant volatility and that cash has never been used in criminal activities, which we know is not the case.

The hesitancy of banks to offer cryptocurrency investment services has helped pave the way for platforms like Coinbase, whose initial public offering in April 2021 valued them at $85.8 billion, to offer these investment services directly to consumers. In addition to providing cryptocurrency consumers with an investment platform, Coinbase also offers its customers the use of a debit card that automatically converts cryptocurrency to U.S. dollars at the time of purchases and ATM withdrawals. While it is still only the minority of consumers who invest in cryptocurrency, the creation of companies like Coinbase should at least begin making banks wary of future competition.

I've listed some pros and cons of using cryptocurrency from the perspective of users:

Pros:

- *Twenty-four-hour instant access* – cryptocurrency can be accessed 24 hours a day and managed on mobile devices, allowing for instant international transfers without the

It is important for leaders of financial institutions to get ahead of the curve in learning how cryptocurrency might impact their operations in the future and researching guidance released by regulatory bodies.

need for intermediaries or the need to convert to foreign currencies.

- *Growth* – cryptocurrency has been growing in popularity since it was introduced and is becoming more widely used for both transactions and as an investment tool. This has the value of certain cryptocurrencies (particularly Bitcoin) to increase in price substantially since its introduction.

- *Unregulated currency* – holding an anonymous currency not bound by political changes can be both positive and negative. While anonymity limits the risk of identity theft, it also is inviting to criminal enterprises.

Cons:

- *Volatility* – the prices of cryptocurrency have been subject to extreme volatility. While the price of the most popular cryptocurrencies has largely trended upward since its introduction, the extreme volatility makes it riskier than many traditional investments.

- *No FDIC Insurance* – unlike cash held in depository institutions, the FDIC does not insure money invested in cryptocurrencies. However, this is not much different from other traditional investments like stocks and bonds.

Now that I have provided an introduction to cryptocurrencies and discussed the pros and cons to users/holders of cryptocurrencies, I would like to discuss ways that financial institutions can take advantage and provide services to users of cryptocurrencies. Financial institutions have opportunities to profit from cryptocurrencies by providing the following services:

- Processing payments

- Providing an exchange for customers to convert cash to cryptocurrencies

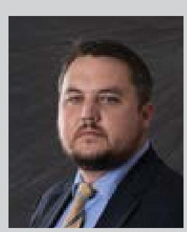
- Facilitating international transfers

- Opening new accounts by partnering with crypto companies

- Providing loans

In addition, some financial institutions have begun accepting cryptocurrency as collateral for loans. However, due to the volatility involved, it is necessary for financial institutions accepting cryptocurrency as collateral to have adequate loan-to-value ratios in place to protect them in the event of value decreases.

In conclusion, there is still plenty to be learned before financial institutions (particularly community banks) determine whether it is feasible to begin offering crypto services. However, there is little doubt the use of cryptocurrency will continue to grow. It is important for leaders of financial institutions to get ahead of the curve in learning how cryptocurrency might impact their operations in the future and researching guidance released by regulatory bodies. It is likely that cryptocurrency technology will play a prominent role in the future of financial institutions. ■



Patrick McGraw, CPA, is a Senior Manager with Baker Tilly, focusing on internal & external audit and consulting. He can be reached at patrick.mcgraw@actcpas.com or 304-225-6000.

Corporate Transparency Act

By Matthew Kingery, Lewis Glasser, LLC

Congress passed the Corporate Transparency Act ("CTA") on Jan. 1, 2021, as part of the National Defense Authorization Act ("NDAA") for fiscal year 2021. The purpose of CTA is to "better enable critical national security, intelligence, and law enforcement efforts to counter money laundering, the financing of terrorism, and other illicit activity" by creating a national registry of beneficial ownership information for "reporting companies." CTA requires every limited liability company, corporation, or similar entity to report the beneficial ownership of an entity to the U.S. Department of Treasury's Financial Crimes Enforcement Network ("FinCEN") unless the entity qualifies for one of the CTA's 24 exemptions.

The information will not be publicly available, but FinCEN is authorized to disclose the information to the following:

- U.S. federal law enforcement agencies
- Certain other enforcement agencies
- Non-U.S. law enforcement agencies prosecutors or judges based on a request from a U.S. federal law enforcement agency
- Financial institutions and their regulators, with consent of the reporting company

The CTA represents a change in the responsibilities of financial institutions. Prior to the implementation of the CTA, the burden of collecting beneficial ownership information fell on financial institutions, which are required to identify and verify beneficial owners through the Bank Secrecy Act's customer due diligence requirements. CTA shifts that responsibility to reporting companies.

Regulations

The CTA requires the Secretary of the Treasury to prescribe regulations by Jan. 1, 2022. The anticipated regulations will govern the timing for filing under CTA. On April 2, 2021, FinCEN issued an advance notice of proposed rulemaking ("ANPRM"). FinCEN received 241 comments, of which 215 were made public and are available for review at regulations.gov. Parties that commented included secretaries of state, legal associations, law enforcement officials, and business associations. This ANPRM was the first in a series of regulatory actions that FinCEN has undertaken to implement the CTA. There should be another comment period after FinCEN issues its proposed regulations.

What is a reporting company?

A "reporting company" is broadly defined by CTA as any corporation, limited liability company, or similar entity that is (1) created by filing a formation document with a secretary of state or similar office; or (2) formed under the law of a foreign country and registered to do business in the United States. There are 24 exemptions to what entities qualify as reporting companies.

A reporting company does not include, among other types of companies:

1. An issuer of securities registered under Section 12 of the Securities Exchange Act of 1934 ("Exchange Act") or that is required to file supplementary and periodic information under Section 15(d) of the Exchange Act
2. An entity established under the laws of the United States, a state, or a political subdivision of a state, or under an interstate compact

between two or more states and that exercises governmental authority on behalf of the United States or any such state or political subdivision

3. A bank

4. A federal or state credit union

5. A bank or savings and loan holding company

6. A broker or dealer registered under Section 15 of the Exchange Act

7. An investment adviser that has made certain filings with the SEC

8. An insurance company as defined in the Investment Company Act of 1940

9. A public accounting firm registered under the Sarbanes-Oxley Act of 2002

10. A public utility

11. A tax exempt Section 501(c) corporation, political organization, charitable trust or split-interest trust exempt from tax

12. An entity that:

    (i) Employs more than 20 employees on a full-time basis in the United States

    (ii) Filed in the previous year federal income tax returns in the United States demonstrating more than $5,000,000 in gross receipts or sales

    (iii) Has an operating presence at a physical office within the United States

Who is a beneficial owner?

A "beneficial owner" under the CTA is defined as an individual who, directly or indirectly, exercises substantial control over the entity or owns or controls not less than 25% of the ownership interests of the entity.

A beneficial owner does not include:

(i) a minor child if the information of the child's parent or guardian is reported

(ii) an individual acting as a nominee, intermediary, custodian or agent on behalf of another individual

(iii) an individual acting solely as an employee of the entity and whose control over or economic benefits from such entity is derived solely from the employment status of the person

(iv) an individual whose only interest is through a right of inheritance

(v) a creditor of the entity, unless the creditor exercises substantial control over the entity or owns or controls not less than 25% of the ownership interests of the entity

What is required to be reported and when?

Reporting companies must deliver a report to FinCEN containing the full legal name, date of birth, current residential or business street address, and unique identifying number from an acceptable identification document or FinCEN identifier. If an entity is formed before the effective date of the regulations, that entity has two years to deliver its beneficial ownership report. Entities formed after the effective date of the regulations must comply with CTA upon the formation of the entity. If there are changes to the information to be included in the report, the entity has one year after the date of the change to submit an updated report. Noncompliance with the CTA or providing inaccurate or misleading information to FinCEN can result in $500 per day penalties, not to exceed $10,000. It could result in up to two years in prison for any person committing a reporting violation.

How will beneficial ownership information be maintained?

Beneficial ownership information provided to FinCEN will be kept in a confidential national registry that will be maintained for at least five years after termination of the reporting company. The Secretary of the Treasury must maintain information security protections for all beneficial ownership information.

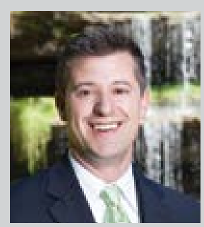
Takeaways

- CTA shifts certain reporting obligations away from financial institutions

- CTA largely applies to foreign-owned shell companies, but all companies should determine if they are a reporting company under CTA

- Greater access to beneficial ownership information will be granted to federal and state agencies and state and local law enforcement agencies, and such agencies will be able to share such information with international agencies to combat money laundering, financing of terrorism, and other illicit activity; and

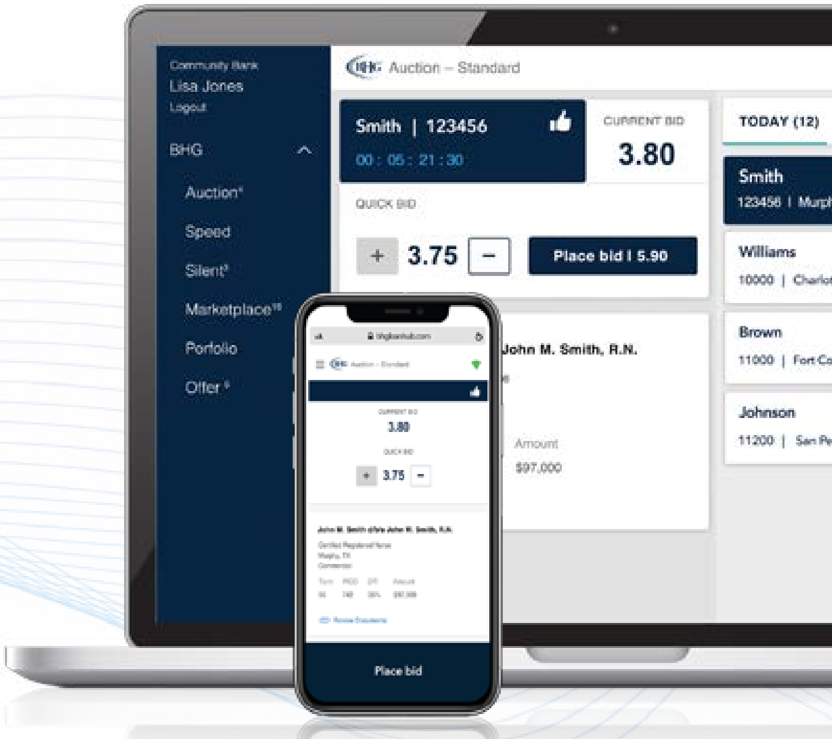
- Companies should pay close attention to implementing regulations once promulgated.



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.

THE BHG LOAN HUB

#1 Source for Time-Tested & Proven Assets



More than **1,300 banks have earned nearly $1B in combined interest income**.

BHG PROFESSIONAL CHARACTERISTICS

FICO*	INCOME*	AVG. LOAN SIZE	YRS IN INDUSTRY*
737	$293,500	$125,800	20

WHAT YOUR BANK CAN EXPECT

2.00–4.75% return for your bank

$0 Historical Loss on the BHG Core Loan Program

~$10MM in loans available for purchase daily

TO LEARN MORE ABOUT BHG, PLEASE CONTACT:

Brian Mullett, SVP, Institutional Relationships

bmullett@bhgbanks.com • (315) 400-6192

BHGLoanHub.com/WV

BHG | BANK GROUP

*weighted average

What are Consumers' Top Cybersecurity Concerns?

Find out how your bank can address key issues and build trust among your customers

By Sean Martin, CSI

To understand how U.S. consumers view cybersecurity risks, CSI – a leading provider of fintech, regtech and cybersecurity solutions – worked with The Harris Poll to survey more than 2,000 U.S. adults aged 18 and above.

Respondents were asked to identify their primary financial institution, providing a look into the perceptions of big bank customers (e.g., Chase, Wells Fargo, etc.), community bank customers, credit union members and those without a primary institution. The data from this online survey was then analyzed and used to create an executive report to help financial institutions understand consumers' cybersecurity perceptions and expectations.

This executive report provides key insight into this year's survey results and offers a comparison to data from a similar survey conducted on behalf of CSI by The Harris Poll in 2019, exploring how cybersecurity concerns have shifted among Americans.

How is Consumer Perception of Cybersecurity Issues Changing?

Although a substantial number of consumers (85%) reported cybersecurity concerns pertaining to their personal confidential data, 15% are not particularly worried – a surprising number considering the surge in pandemic-related cyberattacks.

By comparison, in 2019, 92% of consumers reported cybersecurity concerns pertaining to their personal confidential data, so this year's decrease could signal that Americans are becoming desensitized to cybersecurity risks. It's likely that the size, scope and frequency of cybersecurity events have made breaches appear somewhat abstract and distant to the average consumer. And the constant barrage of media coverage on this topic could be contributing to greater risk tolerance among consumers – potentially leading to adverse effects for banks and making effective cybersecurity education even more important.

Key Takeaways from the Consumer Cybersecurity Poll

To gauge shifting perceptions, consumers were asked their thoughts regarding password habits, payments security, data breaches and more. Here are a few takeaways for banks:

- **Top Cybersecurity Concerns:** Identity theft and stolen credit or debit card information tied as the top cybersecurity concerns among consumers, at 60%. This is down significantly from 2019, when identity theft topped the list of concerns at 73%, followed closely by stolen card information (72%). These changing perceptions among Americans indicate that institutions should prioritize educating customers on these evolving risks.

- **Risks of a Data Breach:** Nearly half of respondents (48%) would leave their institution if it suffered a data breach, and 51% of community bank customers agreed that a breach would cause them to leave. To mitigate the risk of customer attrition, institutions should have an incident response plan in place to direct their actions in the event of a breach.

- **Strong Authentication:** 30% of Americans agree it is okay to use the same password for an online bank account that they use for other online accounts, representing an increase of six percentage points from 2019 (24%). To mitigate risks associated with lax security habits, banks should provide and promote multi-factor authentication and reinforce the importance of strong passwords.

- **What to do Post-Breach:** Most Americans (69%) believe they know what to do if their personal confidential data is compromised. While this result is encouraging, a clear opportunity exists for banks to continue educating customers on the necessary steps to take after their information is potentially compromised. A community financial institution that prioritizes cybersecurity education for its customers could become the go-to institution for advice, which could help expand market reach.

- **Perceptions of Secure Payments:** Half of Americans (50%) believe a person's payment information (i.e., account number) is more likely to be compromised when using a physical card versus a digital payment such as a contactless card or digital wallet. Banks should embrace the latest payments technology and provide customers with resources on best practices for using secure digital payments.

- **Importance of Building Trust:** More than three in four consumers (76%) agree their financial institution can protect their personal and payment information from hackers. In fact, 78% of community bank customers agree with this, indicating that institutions should continue building trust among consumers by explaining how to safeguard data and hosting cybersecurity awareness training.

Prioritizing Cybersecurity Awareness and Education

As Americans become increasingly desensitized to the risk of security breaches, it is critical for your bank to break through the noise and educate your customers on cybersecurity best practices. Providing valuable education and promoting good cyber hygiene will mitigate cybersecurity risk for both your institution and customers while increasing the potential for new business through knowledge sharing.

Nearly half of respondents (48%) would leave their institution if it suffered a data breach, and 51% of community bank customers agreed that a breach would cause them to leave.

To really capitalize on this opportunity, your bank should be intentional and strategic in its planning:

- **Determine the Needs of Your Customers:** Avoid a one-size-fits-all approach; different customers have varying needs and concerns.

- **Tailor Your Approach:** Create campaigns to reach different groups, tailoring based on age, work schedules, etc.

- **Get Creative:** Think creatively about how best to communicate with your customers and deliver a compelling message.

- **Go Digital:** Leverage digital channels to reach a broader audience – don't limit the size and scope of events to physical locations.

- **Deliver Actionable Tips:** Inspire confidence in your bank and motivate customers through actionable tips, such as best practices for creating strong passwords, etc.

Gain Additional Insight from CSI's Consumer Cybersecurity Poll

To strengthen defenses against evolving cyber threats, institutions should embrace a layered approach to cybersecurity, a key component of which includes providing customers with continued education. Download the full executive report for a deep dive into consumers' perceptions surrounding cybersecurity. ■

Download the full executive report:

(https://www.csiweb.com/cybersecurity-poll-2021/?utm_source=association&utm_medium=article&utm_campaign=wp_ms_cybersecuritypoll21)

Sean Martin serves as a product manager for CSI Managed Services and has extensive knowledge on implementing effective systems security and network management practices. He speaks and writes frequently on security-related topics affecting the financial services industry and holds Cisco CCNA and CCIE written certifications.

ZPLC

CERTIFIED PUBLIC ACCOUNTANTS & ADVISORS

Zeno, Pockl, Lilly and Copeland, A.C. (ZPLC) is a West Virginia based firm whose principals have spent most of their public accounting careers providing services to financial institutions. ZPLC possesses a great deal of experience, dedication, trust, and even more personality. We believe in providing exceptional service with a high level of personal attention!

Community-based financial institutions throughout West Virginia, Ohio, and Pennsylvania have relied on the principals of ZPLC for solutions to their audit, tax, and regulatory compliance needs for over 40 years. Each of the firm's founders has extensive experience in solving complex issues for community banks, collectively over 80 years of experience at your service. Over 20 such institutions have joined with us as we build upon our reputation as being a valued resource for the industry.

Whether you need assistance in the implementation of a complex financial reporting standard or a practical and efficient approach to internal auditing that can stand up to regulatory scrutiny, you can be secure in knowing that ZPLC professionals have the skills and the savvy on which you can rely. As members of the Private Companies Practice Section of the AICPA, as well as the PCAOB, we have extensive qualifications and experience to meet your audit service needs.

Contact us today if you need services in any of the following:

- Financial statement audits
- Internal audit outsourcing or co-sourcing arrangements
- Income tax planning and preparation
- Trust department examinations
- Regulatory compliance audits, including BSA, NACHA, OFAC
- Merger and acquisition assistance
- New bank formations
- Going public or going private transactions
- SEC reporting assistance
- Interest rate risk analysis

Michael A. Zeno, Principal

Mary C. Pockl, Principal

Timothy M. Copeland, Principal

980 National Road, Wheeling WV 26003 and
511 N. Fourth Street, Steubenville, OH 43952
304-233-5030 / www.zplcaccounting.com

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

Regulators Move Closer to Incorporating Climate-Related Risks into Oversight of Banks and Other Institutions

By Nicholas P. Mooney II, Spilman Thomas & Battle, PLLC

In the Fall 2021 issue of West Virginia Banker magazine, we discussed three issues and opportunities facing banks in the post-pandemic world, one of which was the concept of Sustainable Banking. Also called Environmental, Social, and Governance (ESG) banking, this concept sometimes is labeled "banking with a purpose." It focuses on banking in a way that considers the economic, social, and environmental effects of the bank's products and services.

Although banks in the United States are sometimes criticized as being slow to adopt sustainable banking when compared to their European counterparts, they recently began stepping into this realm in a big way. In the fall issue, we discussed the initiatives banks such as JPMorgan Chase, Wells Fargo, Bank of America, and Fifth Third have developed in this arena. It is clear that smaller, newer players also view sustainable banking as an opportunity. For example, Aspiration Financial is going all-in with internet websites that boldly proclaim, "You can change Climate Change," "Leave your bank, save the planet," and "Aspiration is 100% committed to Clean Money." They also offer a credit card that "rewards you for erasing your carbon footprint."

Since our last article, regulators have taken steps that signal sustainable banking is not only a potential opportunity banks may want to consider but may soon become a directive from regulators. Earlier in 2021, President Biden issued an "Executive Order on Climate-Related Financial Risk." That order stated a global shift was currently underway from carbon-intensive energy sources and industrial processes, which according to the order, presented both "transition risks to many companies" as well as "opportunities to enhance U.S. competitiveness and economic growth." The order highlighted what the president saw as "[t]he failure of financial institutions to appropriately and adequately account for and measure these physical and transition risks." This failure "threatens the competitiveness of U.S. companies and markets, the life savings and pensions of U.S. workers and families, and the ability of U.S. financial institutions to serve communities."

The order directed Treasury Secretary Janet Yellen, as Chair of the Financial Stability Oversight Council (FSOC), to consider the following actions:

- Assessing the climate-related financial risks to the stability of the U.S. financial system.
- Issuing a report to the president on the efforts of FSOC member agencies to integrate consideration of climate-related financial risks into their policies and programs.
- Reporting on the necessity of any actions to enhance climate-related disclosures by regulated entities.
- Reporting on approaches to incorporating the consideration of climate-related financial risks into their regulatory and supervisory activities.
- Reporting on any other recommendations to mitigate climate-related financial risk, including through new or revised regulatory standards.

Secretary Yellen and FSOC have taken steps to fulfill those directives. In late Oct., FSOC issued its "Report on Climate-Related Financial Risk," in which FSOC for the first time identified climate change as an "emerging and increasing threat to U.S. financial stability." The report includes more than 30 recommendations to financial regulators on actions that it believes are necessary to identify and address climate-related risks to the U.S. financial system. Those include:

- Prioritizing investments to expand members' capacities to define, identify, measure, monitor, assess, and report on climate-related financial risks.
- Reviewing members' public communications about climate-related efforts, including in annual reports, and updating them to promote consistent, comparable, and useful information on climate-related risks and opportunities.

FSOC's report and recommendations signal an important step by member agencies to fulfill the president's Executive Order and Secretary Yellen's statement earlier this year that FSOC will address "a whole-of-government process to assess climate risk to the U.S. financial system and federal government."

- Issuing requirements for climate-related disclosures and considering whether those disclosures should require information related to greenhouse gas emissions.

- Investing in staffing, training, modeling, and monitoring to address climate-related risks.

- Ensuring that members have consistent and reliable data to assist in assessing climate-related risks, including performing internal audits of data and developing plans for acquiring any necessary additional data.

- Developing consistent data standards, definitions, and relevant metrics as well as coordinating among members on these items.

- Reviewing existing regulations, guidance, and regulatory reporting requirements that are relevant to climate-related risks to determine whether amendments or updates are required to appropriately address those risks.

- Determining whether additional regulations are necessary to clarify expectations for regulated or supervised institutions regarding the management of climate-related risks.

In addition to the above recommendations to member agencies, the FSOC report announced the creation of a Climate-Related Financial Risk Committee to be formed within FSOC. The committee's mission is to enhance coordination and consistency among FSOC members. Also, it needs to identify areas for mitigating climate-related risks and act as a coordinating body to share information; facilitate the development of common definitions, standards, and approaches; and foster communication among FSOC members. They will be aided in these missions by another new committee created within FSOC: the Climate-Related Financial Risk Advisory Committee.

The FSOC report highlighted several initiatives already underway by member agencies that focus on climate-related financial risks and stability, including the following:

- The Securities and Exchange Commission has begun working on a rulemaking proposal on climate risk disclosures by public issuers, which rule it previously announced would be issued in late 2021 or early 2022.

- The Federal Reserve Board has established committees to address climate-related risks.

- The Commodity Futures Trading Commission's Market Risk Advisory Committee has issued a report on climate-related risks and established a Climate Risk Unit to focus on the role of derivatives in understanding and addressing those risks.

- The Federal Housing Financing Agency has requested information on climate-related risks from the public.

- The Office of the Comptroller of the Currency has formed a Climate Risk Implementation Committee to identify climate-related risks to institutions it supervises. It will also provide recommendations on OCC's policies to address those risks consistent with Acting Comptroller of the Currency Michael Hsu's recent statement that "managing climate change risk is a safety and soundness issue."

FSOC's report and recommendations signal an important step by member agencies to fulfill the president's Executive Order and Secretary Yellen's statement earlier this year that FSOC will address "a whole-of-government process to assess climate risk to the U.S. financial system and federal government." That step, for now, appears to focus on information gathering and creating uniform standards and processes. Banks should be mindful of the recommendations in FSOC's report and consider how climate-related risks appear in their business lines, as this issue likely will receive greater attention in the short-term. ■

Nicholas P. Mooney II is a Member attorney in Spilman Thomas & Battle's Charleston, West Virginia office. His primary area of practice is consumer financial services litigation in federal and state courts. He has devoted all of his time for more than 20 years to that practice area. He can be reached at (304) 340-3860 or nmooney@spilmanlaw.com.

Federal Agencies Focus on Community Bank-Fintech Partnerships

By Elizabeth Frame and Drew A. Proudfoot, Bowles Rice, LLP

Financial technology, or fintech, refers to the broad set of financial innovations that apply new technologies to a financial service or product. Although potential competition from fintech companies initially raised concerns for the banking industry, as consumer and regulatory demand for better technology increased, banks quickly recognized and adapted to the changing market. Today, banks have implemented fintech solutions for both back-end processes (monitoring of account activity) and consumer-facing products (applications to apply for loans and pay bills online). Many community banks now partner with fintech companies, often through their core processing service providers, to provide modern platforms and services to their customers, obtain data about their customers, provide individualized products and services, and increase security.

The COVID-19 pandemic also forced banks and customers to innovate, often changing how banking transactions were conducted. Banks rushed to provide solutions to open accounts and close loans remotely. These critical fintech solutions heightened banks' awareness of the need to analyze their fintech strategy, including the processes and products that need to be changed and the best model to pursue that change.

Recognizing that innovation and evolving customer preferences are changing the financial services landscape, in August, the Federal Reserve Board, the OCC and the FDIC (the "Agencies") jointly published Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks (the "Guide"). Intended to assist community banks in assessing the risks when partnering with fintech companies, the Guide draws on existing regulatory requirements and supervisory guidance on third-party relationships. It is consistent with recent proposed interagency guidance on how banks should manage the risk inherent in their third-party relationships. More importantly, the Guide likely signals that management of this risk will receive increased scrutiny and focus in the bank examination process.

The Guide emphasizes that "[e]valuating a fintech['s] business experience, strategic goals, and overall qualifications allows a community bank to consider a fintech['s] experience in conducting the activity and its ability to meet the bank's needs." The scope and the depth of the diligence process should be properly calibrated based on the degree of risk posed to the bank and the nature and criticality of the contemplated relationship. Although the Guide specifically addresses community banks (i.e., banks with less than $10 billion in assets), the Agencies note that it can provide useful guidance to banks of all sizes.

The Guide provides relevant considerations and helpful examples of how community banks may identify and mitigate risks through appropriate due diligence. Specifically, the Guide covers six areas of due diligence

Through partnerships with fintech companies, community banks gain access to innovative technologies that can increase operational efficiencies, improve customer experiences, and bolster competitiveness.

that community banks can consider when exploring relationships with fintech companies:

- **Business experience and qualifications,** including the fintech company's business strategies and plans and the qualifications and experience of its company directors and principals. This area is important since it may be an indication of the company's ability to adequately comply with a bank's regulatory obligations while still providing a satisfying customer experience.

- **Financial condition** of the fintech company, including analysis of the fintech company's financial reports, funding sources, and market position. A comprehensive understanding of a fintech company's financial condition is important to ensure that it is and will remain financially healthy and fulfill its obligations to the bank.

- **Legal and regulatory compliance** of the fintech company. Before partnering with a fintech company, banks should assess the company's knowledge and understanding of the regulatory and compliance environment for banks. Banks should also evaluate any legal or regulatory issues faced by the fintech company and review the company's compliance strategies and programs relating to consumer protection, privacy, and anti-money laundering.

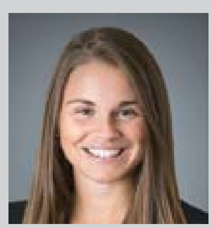
- **Risk management and controls** of the fintech company. Understanding the fintech company's risk appetite and its internal risk framework is an essential component of due diligence. In some cases, a bank may learn the fintech company's risk profile and the bank's risk tolerance does not align.

- **Information security,** including the fintech company's information security program and information systems. The ability of a fintech company to protect sensitive customer and bank information is critical in a fintech-bank partnership. Fintech companies should be willing and able to provide comprehensive information about their information security program and information systems.

- **Operational resilience,** including the fintech company's business continuity planning, incident response plan, and service level agreements. Banks should assess the fintech company's ability to provide service in the face of technology failures or cyber incidents. Threat detection procedures should also be examined and evaluated.

Through partnerships with fintech companies, community banks gain access to innovative technologies that can increase operational efficiencies, improve customer experiences, and bolster competitiveness. However, these partnerships also introduce risks that must be evaluated through an appropriate due diligence investigation. The Guide provides a roadmap for regulatory expectations and issues that should be addressed during the due diligence process.

To read the Guide in its entirety, visit: https://www.federalreserve.gov/publications/conducting-due-diligence-on-financial-technology-firms.htm.



Elizabeth Frame is a partner in the Charleston, West Virginia office of Bowles Rice. She advises clients on regulatory and securities work, as well as mergers and acquisitions, and has advised clients on issues regarding the CARES Act, Paycheck Protection Program and Small Business Administration Loan Relief. Contact Elizabeth at (304) 347-1715 or eframe@bowlesrice.com.

Drew Proudfoot is an associate attorney in the Morgantown, West Virginia office of Bowles Rice. He focuses his practice on corporate and financial services transactions, including commercial lending, mergers and acquisitions, and business succession planning. Contact Drew at (304) 285-2566 or dproudfoot@bowlesrice.com.

OFAC Issues New Guidance Directed at Virtual Currency Industry:

What You Need to Know

By Roger Morris, Compliance Alliance

In October, the Office of Foreign Assets Control (OFAC) published more targeted guidance for digital asset companies related to compliance with sanctions and best practices for mitigating risks. OFAC's virtual currency guidance is directed at the entire industry, including "technology companies, exchangers, administrators, miners, wallet providers, and users." It aims to "help the virtual currency industry prevent exploitation by sanctioned persons and other illicit actors," according to the press release issued with the guidance. Essentially, the guidance emphasizes that anyone subject to U.S. sanctions laws and regulations must continue to abide by them when engaging with virtual currencies.

The guidance provides several best practices that entities involved in virtual currency activities should follow to remain in compliance and to mitigate penalties in instances of compliance failures. These practices will be familiar to anyone with experience in sanctions compliance and best practices that apply to other industries. This said, the document notes, compliance solutions should reflect a risk-based approach and should be tailored to the type of product or business involved, its size and level of sophistication, its clients and counterparties, and the locations it serves. OFAC also expects companies to implement these practices sooner rather than later in the company's existence before any products and services are released. While there is no single compliance program to suit all scenarios, implementing OFAC's best practices, as follows, can prevent sanctions violations and serve as a mitigating factor should any violations occur.

Management Commitment

Management should commit to enforcing a culture of compliance throughout the organization from the company's earliest days. OFAC recommends specific actions that management can take to set an appropriate tone from the top, including reviewing and endorsing compliance procedures, allocating adequate resources to compliance, delegating autonomy and authority to the compliance department, and appointing an experienced sanctions compliance officer.

Risk Assessment

Regular and ongoing risk assessments should be conducted to identify risks associated with sanctions compliance. Activities and relationships associated with foreign jurisdictions or foreign persons should be assessed for their potential to expose a company to sanctioned persons or places.

A virtual currency company's risk assessment process should be tailored to the types of products and services offered and the locations in which such products and services are offered. Appropriately customized risk assessments should reflect a company's customer or client base, products, services, supply chain, counterparties, transactions, and geographic locations, and may also include evaluating whether counterparties and partners have adequate compliance procedures.

Internal Controls

Internal controls should be able to "identify, interdict, escalate, report (as appropriate), and maintain records for" prohibited activities. Useful internal controls include sanctions screening, geolocation tools, know your customer

Companies should conduct training for relevant employees at least annually. The best practices for the virtual currency industry are not new, nor are they unique to the industry.

("KYC") procedures, and transaction monitoring and investigation to identify virtual currency addresses and other data associated with sanctioned individuals, entities, or jurisdictions. OFAC includes virtual currency addresses as identifying information for designated persons, so these should be used in screening as well. While OFAC does not require the virtual currency industry to use any particular in-house or third-party software, OFAC states that such software can be a helpful tool for an effective sanctions compliance program.

Testing and Auditing

Testing and auditing procedures can include ensuring that screening and IP blocking are working effectively. Companies that incorporate a comprehensive, independent, and objective testing or audit function within their sanctions compliance program are equipped to ensure that they are aware of how their programs are performing and what aspects need to be updated, enhanced, or recalibrated to account for a changing risk assessment or sanctions environment.

The size and sophistication of a company may determine whether it conducts internal and external audits of its sanctions compliance program. Some best practices for testing and audit procedures in sanctions compliance programs for the virtual currency industry include sanctions list screening, keyword screening, IP blocking, investigation and reporting.

Training

Companies should conduct training for relevant employees at least annually. The best practices for the virtual currency industry are not new, nor are they unique to the industry. However, the recent guidance from OFAC indicates that the industry will be a particular focus for enforcement. Companies in the industry should implement these measures as soon as possible if they have not already. The scope of a company's training will be informed by the size, sophistication, and risk profile. OFAC training should be provided to all appropriate employees, including compliance, management, and customer service personnel, and should be conducted periodically and, at a minimum, annually. A well-developed OFAC training program will provide job-specific knowledge based on need, communicate the sanctions compliance responsibilities for each employee, and hold employees accountable for meeting training requirements through the use of assessments.

Remedial measures

Where a sanctions violation has occurred, OFAC can consider the remedial measures a company has taken as a mitigating factor in a penalty determination. Remedial measures can include adding and/or strengthening the tools listed above to fill gaps and repair weaknesses in the compliance program.

Conclusion

OFAC is placing much greater scrutiny on the virtual currency industry. Industry members should be mindful of implementing and maintaining robust compliance measures early and often. ■

Roger Morris serves Compliance Alliance as Associate General Counsel. He brings a combination of unique experiences to C/A that he uses to provide guidance on a wide variety of regulatory and compliance issues. Contact him at Bankers Alliance, (833) 683-0701 or info@bankersalliance.org.

Checking In on the Banking Industry

By Dale Sheller, The Baker Group

2020 was a year of challenges in many aspects of life, business, and the economy. The start of 2021 brought a close to a tumultuous year and opened the door to a year of economic recovery and hope for more normal times. In March 2020, the banking industry was rocked when the Fed funds rate was cut to zero at an unprecedented speed, and Treasury yields tumbled to all-time lows. Additionally, the massive influx of stimulus-related deposits that flowed into the banking system greatly changed the size and structure of balance sheets. As a former bank examiner, I am taking a chapter from my previous regulatory career by looking at the banking industry as it relates to the Uniform Financial Institutions Rating System and its six components, known as CAMELS.

Capital – A wise person once told me that capital cures a lot of ills. While this statement is very true, not properly leveraging your capital may leave some additional earnings and shareholder returns on the table. Before the pandemic hit, leverage ratios were very strong, with only 14 banks on the "less than well-capitalized" list. For the most part, leverage ratios haven't been stressed in the traditional sense with loan losses; however, many institutions have seen a reduction in their leverage ratios as asset growth has dramatically outpaced capital growth. Additional pressure on leverage ratios could continue.

Asset Quality – This is likely the biggest unknown of all the components. When the COVID-19 pandemic forced many states to shut down to varying magnitudes, many businesses struggled, and millions lost their jobs. As we continue into the next year, the delta variant is pushing its way throughout the country, but in general, we haven't seen massive asset quality problems materialize. Asset quality is likely to vary significantly from bank to bank and region to region. Some institutions have more exposure to the most hard-hit industries, while others have little to no exposure. We know that extensions, deferrals, and government stimulus have propped up some businesses and kept loans from going bust. Time will tell which businesses and customers will be able to get back on their feet and which won't.

Management – Management is easily the most subjective component of all the CAMELS components. Bank management has been extra busy with the many challenges being thrown their way due to the pandemic. Community

Today, the vast majority of institutions are well-positioned for rising interest rates as their stockpiles of short-term liquidity have pushed them even further asset-sensitive than before.

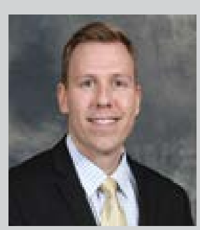
banks have continued to shine bright, providing us a friendly reminder of just how important they are to the communities of this country.

Earnings – The industry was riding high in 2018 and 2019 after record years of profitability through expanding net interest margins, low provision expenses, and lower tax rates. However, zero-bound short-term interest rates, combined with high levels of low earning cash liquidity, have put margins back under pressure. The average community bank has seen significant margin compression in 2020 and 2021. In 2020, many institutions were aggressive in providing for their allowance for loan losses, given the uncertainty of the economy throughout the year. Going forward, many predict low-interest rates are here to stay; therefore, some level of margin compression will likely continue. Many banks are likely well reserved against future loan losses, and the absence of more near-term provision expenses will be welcomed.

Liquidity – Higher loan-to-deposit ratios and less on-balance sheet liquidity were the consistent themes for many institutions over the last several years; however, the pandemic quickly changed them. A combination of massive government stimulus via direct payments and the PPP loan program, coupled with higher personal savings rates and a flight to quality, boosted the industry's deposit base and overall liquidity picture extremely fast. Institutions are now flush with more liquidity than they have been in years, and this excess liquidity doesn't seem to be going away anytime soon. Having excess on-balance sheet liquidity 18 months ago was generally a good thing as loan demand was consistently outpacing deposit growth. The pandemic has completely flipped that narrative. Excess liquidity is now the enemy, with short-term interest rates near zero and a lack of loan demand (outside of PPP loans) plaguing the industry.

Sensitivity to Market Risk – Once the financial crisis sent short-term rates to zero, most bank examiners tended to associate interest rate risk only if interest rates increased. However, the pandemic quickly reminded us that most banks perform better when interest rates rise. During a rising rate environment, the economy experiences growth and expansion, and margins tend to expand due to stronger loan demand, higher loan and bond yields, and deposit costs that lag market rates. Institutions spent most of the last decade preparing their balance sheets for rising interest rates; therefore, they were not as well prepared for the pandemic-induced zero interest rate environment. Margins contracted hard and fast in 2020 and are currently at historic lows. Today, the vast majority of institutions are well-positioned for rising interest rates as their stockpiles of short-term liquidity have pushed them even further asset-sensitive than before. As we find ourselves near historically low-interest rates, we must remind ourselves that the risk of rates not rising is a risk not to ignore.

Bank balance sheets have been dealt a tough hand with all the deposits flowing into the banking system at historically low-interest rates. Community banks have once again shown their resiliency during tough times and will continue to push forward. ■



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. He can be reached at (800) 937-2257 or dsheller@GoBaker.com.

WEST VIRGINIA

BANKER

Advertiser Index

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

Chuck Diulus | 412-215-9581 | chuck.diulus@atm-solutions.com | www.atm-solutions.com

2022 Calendar of Events

(All events scheduled are live and have a recorded backup online)

January

25 Legislative Day/Emerging Leaders (Marriott – Charleston Town Center)

February

TBD Law of Deposits | Jackson Kelly (Sam Bowling Conference Center)

23 & 24 IRA (Basic/Advanced) | Patrice Konarik (Stonewall Resort)

March

2 & 3 Branch Management School | Christie Drexler (Four Points by Sheraton Charleston)

10 Emerging Leaders | Chuck Stump (Sam Bowling Conference Center)

15 & 16 Compliance School | Compliance Alliance – Julie Gutierrez (Four Points by Sheraton Charleston)

April

TBD Disaster Recovery

19 A/L Investments | The Baker Group (Sam Bowling Conference Center)

21 Key Ratio Analysis | David Osburn (Four Points by Sheraton Charleston)

22 Basic Personal & Business Tax Return Analysis | David Osburn (Four Points by Sheraton Charleston)

May

3 & 4 Credit Management Conference | KPN Consulting (Stonewall Resort)

5 & 6 Bank Security School | Jim Rechel (Stonewall Resort)

12 F&E Planning Conference | TBD

22 – 27 WV School of Banking (University of Charleston)

June

6 & 7 Commercial Lending Development Program (CLDP) Sessions I & II | Jeffrey Johnson (Stonewall Resort)

July

19 & 20 LDP Sessions III & IV | John Barrickman (Stonewall Resort)

25 – 27 128th Annual WVBankers Convention (The Greenbrier)

August

TBD Emerging Leaders (Stonewall Resort)

22 & 23 CLDP Sessions V & VI | Jeffrey Johnson (Stonewall Resort)

20 Branch Management School | Christie Drexler (Stonewall Resort)

September

8 HR for Bankers | AlignHR – Lenny Hannigan (Stonewall Resort)

22 & 23 CLDP Sessions VII & VIII | David Osburn (Four Points by Sheraton Charleston)

20 New Accounts & Documentation | Suzie Jones (Sam Bowling Conference Center)

October

18 – 19 BSA/AML Fundamentals | Dianne Barton (Stonewall Resort)

20 – 21 BSA/AML Advanced | Dianne Barton (Stonewall Resort)

November

TBD CEO Forum

TBD CFO Conference

7 – 8 Consumer Lending | David Kemp (Four Points by Sheraton Charleston)

9 Consumer Lending Advanced | David Kemp (Four Points by Sheraton Charleston)

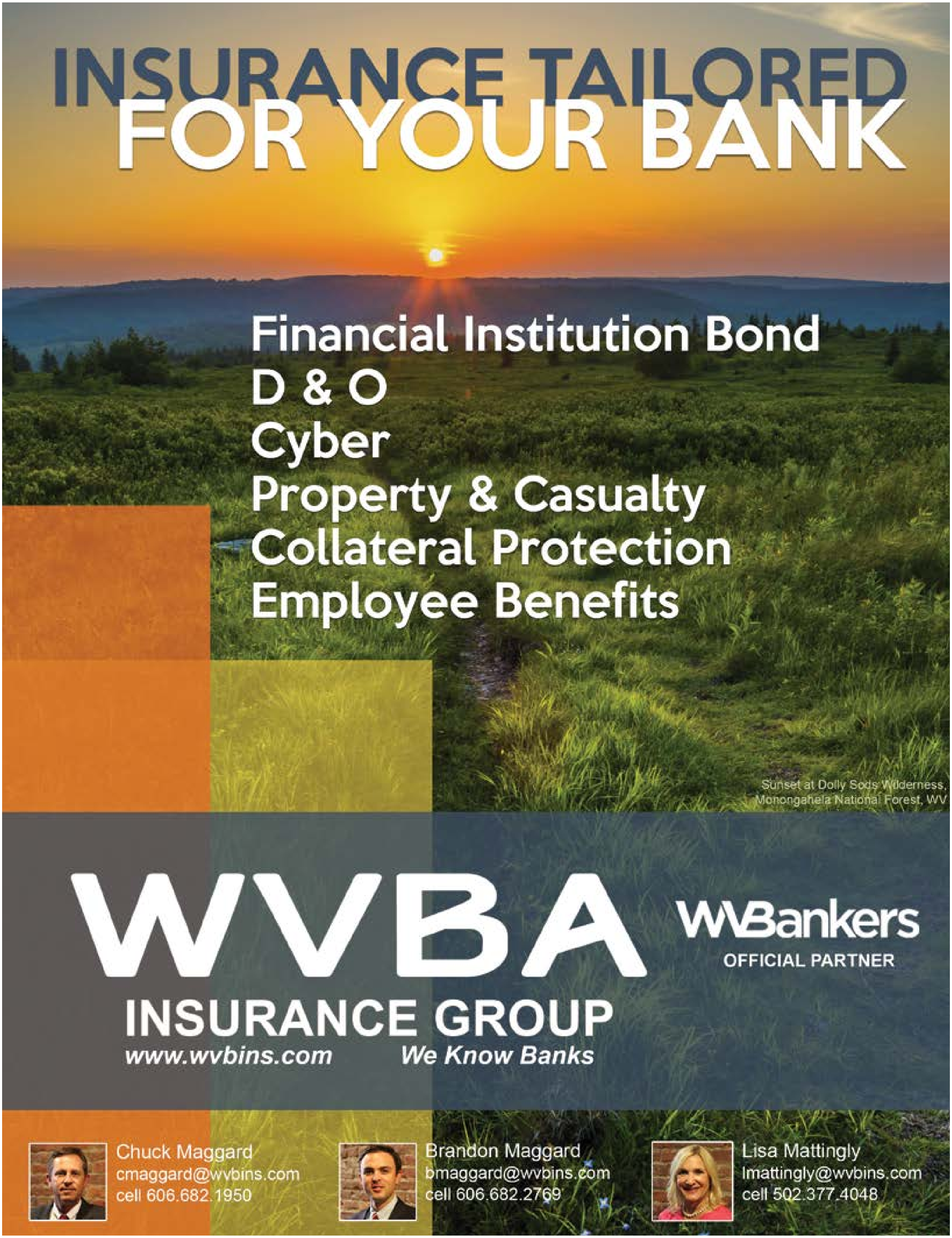
Webinars — Live and Recorded

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.


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

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