COLORADO Banker

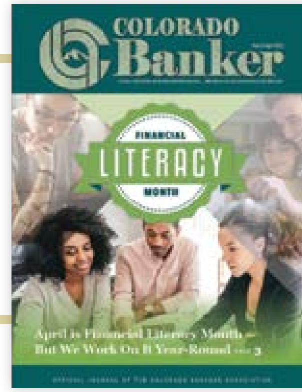
March/April2021

OVER A CENTURY: BUILDING BETTER BANKS — HELPING COLORADANS REALIZE DREAMS

April is Financial Literacy Month – But We Work On It Year-Round PAGE 3

OFFICIAL JOURNAL OF THE COLORADO BANKERS ASSOCIATION

Contents



Don Childears
CEO

Jenifer Waller
President

Amanda Averch
Director of Communications

Brandon Knudtson
Director of Membership

Lindsay Muniz
Director of Education

Margie Mellenbruch
Bookkeeper*

Craig A. Umbaugh
Counsel*

Jim Cole
Lobbyist*

Melanie Layton
Lobbyist*

Garin Vorthmann
Lobbyist*

* Outsourced

Amanda Averch, CBA Director of Communications,
Averch@coloradobankers.org
140 East 19th Avenue, Suite 400
Denver, Colorado 80203
voice: 303.825.1575 — fax: 303.825.1585

Websites:
www.coloradobankers.org
www.smallbizlending.org
www.financialinfo.org
https://colorado-banker.thenewslinkgroup.org/

A WORD FROM CBA

Public Banking: High Risk, No Reward

BY JENIFER WALLER, PRESIDENT, COLORADO BANKERS ASSOCIATION

In recent months, interest has again been percolating around a public bank concept: a bank funded with and operated using taxpayer dollars. This idea is a dangerous answer in search of a question, and it is fraught with risk.

While potential legislation to create such an institution appears to have died on the vine this year, it's important to remind anyone who will listen that the residents of Colorado and the rest of the nation are well served by a thriving and robust financial services industry. In our state, banks employ 20,000 proud professionals dedicated to their customers and help them protect and grow their wealth.

Colorado banks pay taxes to support their neighbors and communities. A public-owned bank would spend tax dollars to offer financial services that Colorado's banks already provide. It would not improve upon our existing financial services system. Instead, it would jeopardize state and local revenues and unnecessarily strap Colorado's budget, rather than contributing to the state's coffers as traditional banks do.

Forming and running a bank is expensive. It would likely involve a very sizable bond issuance, and the minimum it takes to capitalize on a small bank is at least $20 million. Capital is the safety net should something go wrong. Colorado does not have the money to spare, especially now when economic stimulus and education funding are critical to the state's post-pandemic recovery.

While existing banks are required to have FDIC insurance to protect customers' deposits, a public-owned bank may not offer such protection. Should the bank make a loan that ends up in default, Colorado taxpayers would be left holding the bag.

Taxpayer dollars are meant to support our residents and communities' shared needs, not to bail out a state- or city-owned bank that gambled with residents' money.

Additionally, the formation of such a bank is against the law. The Colorado Constitution expressly prohibits the state, any county, city or town from becoming an owner or a shareholder of any corporation or company.

It's true that one public-owned bank exists in the country: The Bank of North Dakota. Whatever the economic, political or social situation was in 1919 that led to a state-owned bank, no similar situation exists today in Colorado or any other state. That is why no other state or municipality has created a state-owned bank, despite a law that would allow California municipalities to conduct a vote to do so.

Proponents of the concept often point to the Bank of North Dakota as a functioning example of what they seek to create here in Colorado. Still, it does not serve any of the purposes that proponents cite when arguing the need for a state-owned bank. Instead, the Bank of North Dakota operates like a bankers' bank. Banker's banks have developed over time and currently serve the Bank of North Dakota's role; rather than offering direct consumer lending or accepting general deposits, a bankers' bank makes loans to banks and assists them with cash management.

COVID-19 indeed has taken an excruciating toll on our communities, our economy and our loved ones. Keeping in mind that the thousands of Coloradans are facing financial hardship due to the pandemic, the resources they rely upon to stay afloat should not be put at risk on an irresponsible and unnecessary proposal.

CBA will continue to fight this dangerous concept in any form on behalf of taxpayers and their banks that take very seriously the task of keeping finances protected. ■

CHAIRMAN'S MESSAGE

April is Financial Literacy Month – But We Work On It Year-Round

BY NATHAN EWERT, REGIONAL VICE PRESIDENT OF FNBO (FIRST NATIONAL BANK OF OMAHA) FOR COLORADO AND WESTERN NEBRASKA 2020-2021 CBA CHAIRMAN

April is Financial Literacy Month across the country, during which banks and community partners redouble efforts to assist consumers in becoming more financially savvy by drawing attention to ongoing programs and available products toward that end. This year, our communities need our help more than ever as they emerge from the COVID-19 pandemic.

Here in Colorado, bankers and their institutions take that work extremely personally, giving their time and treasure to help educate their customers and communities and help them achieve their financial goals. That happens through a number of efforts, both inside and out of the bank, and I want to make sure bankers are well versed with information on some valuable efforts and programs to share.

Much of the content offered during virtual MoneySmart Week 2021 (MSW) — beginning April 10 — will focus on supporting the needs of low-to-moderate income communities, those hit worst by the pandemic and its related job loss. If you're not familiar, MSW is a national public education program coordinated by the Federal Reserve Bank of Chicago and delivered by a network of supporters — including many here in Colorado. You can learn more at moneysmartweek.org.

You may recall earlier this year that our national counterpart, the American Bankers Association, announced it was making a concerted effort to grow the number of banks participating in the Bank On program to increase the number of safely banked households in the country.

Many of our institutions have long been partners of Colorado-based Bank On efforts in Denver and, more recently, in Boulder County. But for those who don't know about the program — it's a movement driven by more than 90 coalitions to connect people with safe and affordable bank accounts and credit-building opportunities.

continued on page 4

continued from page 3

The coalitions help match consumers with financial institutions in their community that offer "certified" accounts: low-cost, basic accounts that meet the Bank On initiative's National Account Standards, including low or no fees, no overdraft charges, online bill pay and other basic attributes. To date, approximately 24,000 financial institution branch locations in the U.S. offer a Bank On-certified account.

By doing so, participating banks offer to demonstrate a commitment to financial inclusion while also adding new customers in the process. To learn more or get involved, go to bankondenver.com and bankonbouldercounty.com. It's important to note that while those programs are Denver and Boulder-based, you don't have to be. Go to: joinbankon.org/certify.

Colorado's Jump$tart coalition is another localized national effort in which banks participate, working to improve the financial capability of prekindergarten through college-age youth by providing young people with tools to succeed with money, including budgeting, earning, spending, saving, investing and credit. That happens via support of educator professional development, cooperation among coalition members and support of personal financial literacy education initiatives. You can learn more and get involved at colorado-jumpstart.org.

While the Colorado Bankers Association serves on boards and steering committees for Bank On and Jump$tart, input from banks and individual bankers cannot be supplanted. These efforts need you.

Last but not least, CBA has led the charge to promote financial education in the community and in the classroom for decades. This year, our successful advocate has spearheaded additional legislation supported by other advocacy groups to increase financial literacy standards in secondary classrooms across the state. If passed, it will institute required education around student loans, credit cards, mortgage lending and saving for retirement for districts that already provide financial literacy content to students. As of press time, the bill has passed through its first committees unanimously and appears well on its way to becoming law.

Our communities must be made of the resources available to them and their banks' and bankers' efforts on their behalf. While the 30 days of April are when we narrow our focus on financial literacy, we know that work takes place year-round. If you're not already, I encourage you to get involved as early and as often as you can. Our communities look to us bankers to guide them on their journey of personal financial security and success. Let's make sure we're ready for them. ■

While the Colorado Bankers Association serves on boards and steering committees for Bank On and Jump$tart, input from banks and individual bankers cannot be supplanted. These efforts need you.

Nathan serves as Regional Vice President, responsible for leading teams that work with businesses in eastern Colorado and western Nebraska. His primary role is to fulfill client needs quickly and efficiently. He focuses on building relationships that last. In his experience, this is the best way to understand customer needs and to proactively help them meet their financial and life goals.

Employer-Paid Sick Leave In Colorado:

Important Paid Sick Leave Requirements Under Colorado's Healthy Families and Workplaces Act ("HFWA")

BY JULIE TRENT, SENIOR ATTORNEY, COAN, PAYTON & PAYNE, LLC

With the COVID-19 pandemic raging, the Colorado Legislature passed the Healthy Families & Workplaces Act, C.R.S. § 8-13.3-401, et. seq. (the "HFWA"or the "Act"), went into effect January 1, 2021. The law requires employers to provide paid sick leave to their employees.

The far-reaching changes set out in the HFWA affect most Colorado employers. Employment manuals and policies — even "pro-employee" policies — are likely in violation of at least some of the provisions set forth in the HFWA and should be carefully reviewed and revised to ensure compliance. This article sets forth some of the major requirements of the HFWA. For specific questions or issues, please contact the author.

First, the HFWA requires that employers with sixteen (16) or more employees provide paid sick leave to all full- and part-time employees in 2021. Beginning in 2022, all employers must do so, regardless of size.

Second, the HFWA requires employers to provide no less than forty-eight (48) hours of accrued paid sick leave per year for full-time employees and a prorated amount for part-time employees. Accrual requirements are strict. Employers must allow accrual of paid leave to begin on the date of hire (i.e., no more waiting periods for accrual of paid leave to begin). The Act also requires a minimum of one hour accrued for every thirty hours worked, up to the required forty-eight (48) hours of paid leave.[1] Employers must allow 100% of any accrued and unused paid sick leave to be carried forward into subsequent years. However, employers do not have to "payout" accrued but unused sick leave at the end of each year or upon separation or grant an employee more than 48 hours of paid sick leave in any given year (except in the case of a public health emergency, [2] as discussed below).

Under the HFWA, employees may use paid sick leave for their own or a family member's[3] need to seek care for:

- a mental or physical illness, injury or health condition which prevents them from working;
- a medical diagnosis, care or treatment of that condition;
- preventative medical care; or
- a medical or mental health condition or injury resulting from domestic abuse, assault or harassment, counseling, use of services from a victim services organization, or time to relocate or seek legal services due to the abuse, assault or harassment.

Paid sick leave may also be used if, due to a public health emergency, a public official has ordered the closure of the employee's place of business or the school or care center of the employee's child and the employee needs to care for their child.

There are numerous provisions regarding how an employee may request leave, procedures an employer may implement to address leave, and how accrual and use of the leave may occur. For example, employers must allow employees to use sick leave in no more than hourly increments, employers cannot require an employee to find a replacement worker to use the leave, and employers may require "reasonable documentation" if an employee needs four (4) or more consecutive days of leave unless the leave is requested pursuant to a public health emergency, in which case documentation may not be required.

Third, if a public health emergency is declared, in addition to providing the forty-eight (48) hours of accrued paid sick leave, employers must provide an additional eighty (80) hours of paid sick leave for full-time employees and a prorated additional amount of hours based on a 14-day work period for part-time employees. Employers can count accrued, unused, paid sick leave towards the additional eighty (80) hours. This "supplemental" paid sick leave may be used by an employee to self-isolate or care for themselves or a family member due to the diagnosed illness that caused the public health emergency, to self-isolate or care for themselves or a family member if the employee/family member has symptoms of such illness, to seek medical diagnosis, care or treatment of that illness for themselves or a family member, or to seek preventative care regarding that illness for themselves or a family member.

It should be noted that employees are only entitled to one supplemental paid sick leave of up to eighty (80) hours per public health emergency. So, for example, if an employee used eighty (80) hours of paid sick leave in 2020 because they had to care for a spouse with COVID-19 and months later — in 2021 — they are diagnosed with COVID-19, the employee is not entitled to the eighty (80) hours of supplemental paid leave again. However, the employee would be entitled to 2021 accrued paid leave, up to forty-eight (48) hours.

Additional requirements of the HFWA include the employer maintaining records regarding hours worked and paid sick leave accrued and used and posting a notice to employees of their HFWA rights. This requirement can be met by posting a Colorado Department of Labor and Employment poster (specifically, the Colorado Workplace Public Health Rights Poster: Paid Leave, Whistleblowing, & Protective Equipment poster) in an "easily accessible" place.

Based on the numerous requirements and restrictions briefly (and necessarily incompletely) described above, many employers may be in violation of the HFWA already. Even employers who already meet the minimum paid sick leave hourly requirements, many of the "how" and "when" requirements may conflict with employers' current policies. All such policies should be reviewed and revised. ■

1 It should be noted that the HFWA provides a "floor" for paid sick leave and specifically encourages employers to provide more paid leave if they are able and willing to do so.

2 A "public health emergency" is defined in the statute as an act of bioterrorism, pandemic influenza, epidemic caused by a novel and highly fatal infection agent, or highly infectious illness or epidemic or pandemic potential for which an emergency is declared by a federal, state or local public health agency or a disaster emergency declared by the governor.

3 A family member is broadly defined as an immediate family member, a child/person to whom the employee stands, or stood, in loco parentis, or a person for whom the employee is responsible for providing or arranging health care, who needs the employee's help in getting the listed care.

Julie Trent is a senior attorney with Coan, Payton & Payne, LLC. She practices in all areas of general commercial litigation and employment law, assisting many types of businesses and financial institutions in a wide range of cases.

FEATURE ARTICLE

2021 Could See More Retirement and Health Legislation

BY MIKE RAHN, CISP

Despite political partisanship that has marked much of the 116th Congress in 2019 and 2020, there have been some notable exceptions with bipartisan outcomes. The Setting Every Community Up for Retirement Enhancement (SECURE) Act of 2019 proved that cooperation is possible. That legislation, enacted in December 2019, made significant enhancements to tax-advantaged savings arrangements.

The enactment of the Coronavirus Aid, Relief, and Economic Security (CARES) Act in March 2020 was a unified response to the pandemic that has disrupted many Americans' lives in both economic and health terms. In December 2020, Congress was able to put aside differences in crafting legislation combining additional pandemic relief with needed last-minute federal agency appropriations.

What 2021 will bring is yet to be determined. The Democratic majority in the House of Representatives narrowed in the 2020 general election, and control of the U.S. Senate shifted to Democratic control by the narrowest of margins. A Democrat also now resides in the White House. His legislative agenda has yet to be revealed in detail but — based on campaign messaging — may include the broadly defined goal of "equalizing benefits across the income scale." This ambition aside, it can be difficult for any president to accomplish legislative objectives with such a narrowly divided Congress.

Unless, that is, these objectives align with those of a majority of lawmakers. Fortunately, tax-advantaged savings legislation has a history of being able to gather bipartisan support. It has win-win dimensions that tend to unify rather than divide. For this reason, there is optimism that one or more savings-focused bills could be enacted in 2021. Several introduced during the past two years will likely be re-introduced in the 117th Congress.

Securing a Strong Retirement Act

This legislation — called SECURE 2.0 by some, referring to 2019's SECURE legislation — is a further example of bipartisanship. It is jointly sponsored by House Ways and Means Committee Chairman, Representative (Rep.) Richard Neal (D-MA) — and GOP Ranking Member Kevin Brady (R-TX). Due to the prominence of these sponsors, the legislation is considered to have favorable prospects. It includes the following provisions:

- Require employers — with exceptions for certain new and small businesses — to establish an automatic enrollment deferral-type retirement plan, such as a savings incentive match plan for employees of small employers (SIMPLE) IRA plan.
- Provide an enhanced small employer plan startup tax credit for such new plans.
- Enhance the "saver's credit" for IRA contributions and deferral-type employer plan contributions, such as those made to a SIMPLE IRA plan.
- Exempt up to $100,000 of accumulated IRA and employer-sponsored retirement plan assets from required minimum distribution (RMD) calculations.
- Increase the RMD onset age from 72 to 75.

- Reduce penalties for RMD failures.

- Provide a second (age 60), higher IRA catch-up contribution limit.
- Index IRA catch-up contributions for inflation.

- Increase the limit for IRA and retirement plan assets that are exempt from RMD calculations under qualifying longevity annuity contract (QLAC) rules.

- Reduce certain IRA error penalties and permit more self-correction.

- Permit matching contributions, e.g., to SIMPLE IRAs — based on student loan payments.

Automatic IRA Act

It is widely accepted that up to 40% of American workers do not have access to a workplace retirement plan. A concept that dates back more than a decade proposes universal, automatic saving to an IRA through a worker's place of employment if no other retirement plan is available. This is the concept embodied in the Automatic IRA Act, which has been introduced in several previous Congress sessions.

In the absence of action at the federal level, many states have acted independently to establish automatic IRA-based saving programs, which — while beneficial for those covered — have left geographic gaps and a patchwork with differing program rules. A uniform national automatic IRA program could close these gaps and address differences.

- Employers in business less than two years or employing fewer than 10 employees would be exempt.

- Employees would be automatically enrolled and contributions withheld from pay, but they would be able to opt-out.
- Accounts would be Roth IRAs unless a Traditional IRA was elected.

- Contributions would likely begin at 3% of pay, but with latitude to range between 2% and 6%.

- Investments would include balanced, principal preservation and target-date funds, as well as guaranteed insurance contracts.

Past sponsors of automatic IRA legislation have included Rep. Richard Neal (D-MA) and U.S. Senator Sheldon Whitehouse (D-RI).

HSA Enhancements

Affordable health insurance for Americans continues to be an extremely challenging goal. One increasingly common option — an alternative to the comprehensive "major medical" health insurance model — is a high deductible health insurance plan linked to a saving and spending account known as a health savings account or HSA.

This approach is intended to offer a path to lower health insurance premiums and allow individuals to save in a tax-advantaged manner for expenses below their health plan deductible and copay amounts they owe. What initially began as a temporary test program under medical savings account (MSA) nomenclature later evolved into the HSA we know today.

With many U.S. employers offering employees an HSA-based program as one — or perhaps the only — health insurance option, much focus has been on how the HSA might be tweaked to improve its usefulness. Following are some of the proposed HSA modifications, a composite of provisions from several bills introduced in the 116th Congress. Some, or all, could be presented again in the 117th Congress that has just been sworn in.

- Increase maximum annual HSA contributions; some have proposed doubling the limits.

- Expand the treatments for which a plan's high deductible need not be met before benefits commence, such as chronic care services and more medications, including nonprescription drugs.

- Permit care at an on-site employer or retail clinics without forfeiting HSA contribution eligibility.

- Treat costs of participating in a fixed-fee primary care arrangement as HSA-eligible expenses.

- Allow coverage of offspring under a parent's HSA-compatible health plan to age 26; would mirror the Affordable Care Act (ACA).

- Define ACA bronze-level and certain catastrophic health insurance plans as HSA-compatible.

- Treat a defined portion of HSA accumulations spent for "fitness and health" as HSA-eligible expenses.

- Allow a fixed amount from health flexible spending arrangements (health FSAs) and health reimbursement arrangements (HRAs) remaining at year's end to be rolled over to an HSA.

- Allow Medicare-eligible individuals enrolled only in Part A (Medicare-provided hospital care) to remain HSA contribution-eligible.

Other Legislative Ambitions

Beyond the possibilities noted above, other initiatives that may be in play in the 117th Congress could include getting closer to universal availability of 401(k)-type workplace retirement plans and addressing the solvency of under-funded defined benefit pension plans. These could be more contentious, carrying as they might the stigmas of "mandate" and "bailout," both of which draw resistance from a substantial number of lawmakers. ■

Visit ascensus.com for more industry news.

FEATURE ARTICLE

Strengthening Your Defenses Against Emerging Cyber Threats

BY TYLER LEET

Over the past year, cybercriminals have proven they are adept at taking advantage of the vulnerabilities stemming from changing work environments and increased digital channel usage. As institutions continue navigating the risks and challenges of remote workforces, it is imperative to stay informed of existing and emerging cybercrime trends.

A variety of scams have made recent news, many of which opportunistically seize upon pandemic-related topics. Your institution must be prepared to recognize and mitigate evolving cyber threats, including:

- **Social Engineering:** We've seen a stark increase in social engineering campaigns as cybercriminals leverage the hardships of the pandemic, including increased levels of stress among employees. Many of these campaigns masquerade as being related to stimulus checks, unemployment benefits or even vaccines. CSI's 2021 Banking Priorities Executive Report revealed more than 80% of bankers identified some form of social engineering as the top cybersecurity threat of 2021.

- **Ransomware:** Once installed, ransomware locks out the authorized user and encrypts the available data to hold for ransom. Since ransomware attacks pose little risk to hackers, provide a speedy payout for criminals and are perpetuated with relative ease and anonymity, institutions should remain on high alert to identify and combat these attacks. Ransomware can be crippling for institutions, especially if regular data backups are not maintained. Because this type of malware continues to be an attractive method of extortion, incidents of ransomware are growing — along with the maliciousness and sophistication of attacks.

- **Increased Surface Area for Attacks:** Due to the size of today's remote workforce, attackers are targeting home networks — which are typically much weaker than in-office networks — to gain access to corporate data. Employees' personal devices are also often targeted, providing attackers with a base to operate from within home networks and allowing them to monitor or intercept secure traffic.

- **Credential Stuffing Attacks:** In this type of attack, botnets conduct brute-force password attacks using compiled lists of stolen credentials against login interfaces. Recently, the FBI reported that credential stuffing accounted for 41% of financial sector cyberattacks.

- **Point of Sale (POS) Skim Attacks:** POS skim attacks occur when a criminal copies card payment information using POS processing devices, which are used everywhere from ATMs to gas station pumps. Despite the massive transition to e-commerce during the pandemic, these types of attacks have continued as criminals use digital skimmers to steal payment information from e-commerce websites.

Emerging Cybercrime Trends for 2021

Although the threats discussed above indeed pose a risk to financial institutions and other organizations, there are several emerging cyber threats to consider as well. Institutions must stay vigilant, especially as many employees continue working remotely.

- **Supply Chain Attacks:** This attack occurs when a bad actor targets a software vendor to deliver malicious code through seemingly legitimate products or updates. The recent SolarWinds breach is an example of a supply chain attack, which is becoming an increasingly popular method to distribute malware.

- **Virtual Private Network (VPN) Attacks:** As remote work becomes the norm for many organizations, cybercriminals will likely continue VPN attacks in an attempt to gain access to corporate networks and data. Many home networks do not have strong passwords set up or lack security protocols, presenting vulnerabilities for criminals to target.

- **Cloud-Based Attacks:** Many organizations are migrating more of their infrastructure to the cloud, prompting cybercriminals to shift more of their efforts to cloud-based attacks. Institutions must ensure their cloud infrastructure is securely configured to prevent harmful breaches.

Strengthening Security for Your Institution

Financial institutions should consider the following strategies to protect their networks and customers while strengthening their cybersecurity posture.

- Create Stronger Passwords: Institutions should enforce stronger password requirements for employees and customers to prevent unauthorized account access. Many organizations previously recommended 8-character, frequently changed passwords, but current best practices dictate using passwords consisting of 14 characters or more and changing them once per year or as needed.

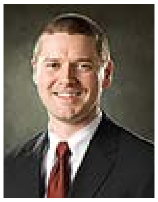
- Utilize Multi-Factor Authentication (MFA): True MFA — not just double passwords — should be used whenever possible. With MFA, multiple authentication factors are required to verify a user's identity. This verification strengthens resiliency and prevents fraudsters from accessing an account solely by obtaining or cracking a password.

- **Enhance Employee Education:** Your institution should enhance employee and customer education efforts. Instead of one annual training, provide frequent information that delivers basic security principles and news about timely issues. Focused trainings are also recommended based upon an employee's responsibilities and access rights. Employee education will also reinforce proper online conduct and normalize communicating with IT after encountering a potentially malicious link or other risks.

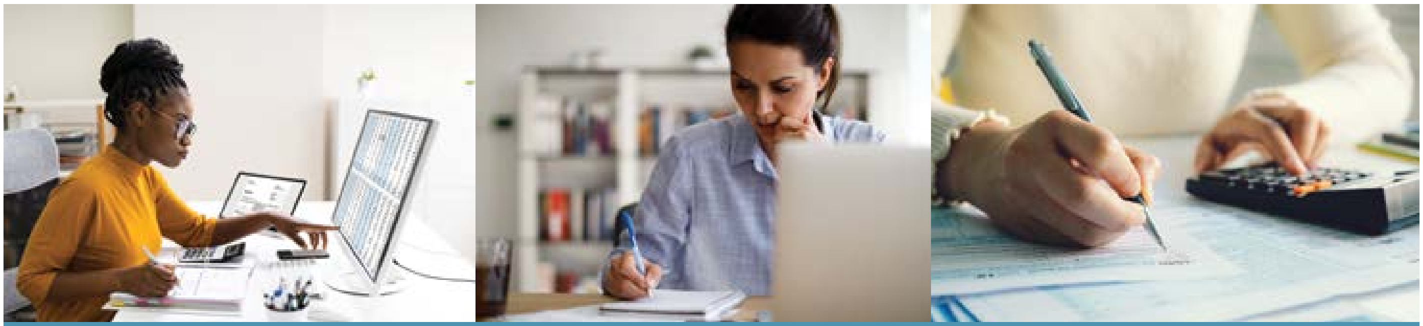
- **Secure Internet Access:** It is critical to ensure proper network security for employee VPNs and their home networks. Encourage employees to use high-quality routers with strong network passwords, run current security protocols and install up-to-date virus and malware protection on personal and corporate devices. Your institution should also review your VPN access and removal policies, acceptable use of business devices, and any other relevant corporate policies.

Facing Future Cyber Threats

As your institution navigates this new landscape, ensure the proper security controls are in place to enhance your risk mitigation and stay one step ahead of emerging cyber threats. ■



Tyler Leet serves as director of Risk and Compliance Services for CSI's Regulatory Compliance Group.



Bank Exam Prep Center

Dear valued member:

As America hopefully exits the pandemic soon, bankers will begin to deal with the economic and regulatory aftermath of our historic response to COVID-19. Your Colorado Bankers Association is taking unprecedented, proactive steps to assist you in this high-stakes process to anticipate issues and face unique challenges during upcoming regulatory examinations.

The general public and our public officials relied on banks' critical role in the pandemic response. And to deliver crucial support to small businesses, banks relied on regulators' commitments. You stepped up on PPP and other programs, and your reaction to this pandemic's economic crisis presents challenges for your next exam. Anticipating the essence of that next exam will have a big impact on the future of your bank and our industry. As you continue to work with customers, it is critical that regulators take a consistent and fair approach and that your bank is prepared for success. We all need to know the focus of examiners.

CBA proudly joins other state bankers associations across the country in announcing a new powerful resource to assist you in preparing for your upcoming regulatory exams. It is called the Bank Exam Prep Center, and it has been developed in association with the Regulatory Feedback Initiative (RFI), presented by the Coalition of Bankers Associations (Coalition). For 10 years, the RFI has asked banks to complete an anonymous Post Exam Survey after each exam and visitation. The data from those surveys provides us with critical exam insights that allow us to 1) help you prepare for your next exam; 2) work with regulators to ensure that bank exams are fair and consistent from agency to agency and region to region; and 3) assist us in auditing regulators' practices.

The Coalition, made up of state bankers associations from across the U.S., unveiled the new Bank Exam Prep Center website the week of March 22nd through a series of webinars for bankers. We urge you and your team members to join us for the webinar that fits best into your schedules.

In the meantime, if you have had an exam or visitation in the past 12 months and have not completed a Post Exam Survey, please go to allbankers.org and anonymously take the 15-minute Post-Exam Survey. The information you provide about your exam experience is confidential and cannot be traced back to your institution, but it will make the resources available at the Bank Exam Prep Center even more helpful to the industry. For more information, go to allbankers.org.

Thank you for considering the following action steps:

- Participate in a webinar on the new Bank Exam Prep Center website: register.gotowebinar.com
- Go to allbankers.org and review the background about RFI and its resources
- Provide your anonymous exam feedback after each exam or visitation
- Utilize the Bank Exam Prep Center resources to prepare for future exams
- Sign up for Bank Exam Prep Center updates as they are released in the future

The new Bank Exam Prep Center is a great resource for preparing for your next exam. However, it will only work to its fullest if we all provide our exam feedback through the anonymous RFI survey.

Thank you for joining us in this critically important effort. Bank Exam Prep Center resources are available from our website coloradobankers.org/or at allbankers.org. Please contact Lindsay Muniz (lindsay@coloradobankers.org) or Becky Wilkes (bwilkes@uba.com) if you have questions or concerns.

Knowledge is power — especially as we face unique challenges together. ■


Are you monitoring a trouble spot for your institution?
Find out how community bankers are connecting their banks with experienced compliance officers who are ready to help however they're needed with Review Alliance's Virtual Compliance Officer service.
Talk with our team today and prepare to move ahead by calling (833) 683-0701 or info@bankersalliance.org
B/√A BANKERS ALLIANCE
Holding Company of Compliance Alliance and Review Alliance
bankersalliance.org

Uncovering Fee-Income and Yield Opportunities in a Challenging Market

BY KEITH GRUEBELE

The pandemic has brought a lot of change to financial institutions, including how to engage with your borrowers, serve their needs, and drive additional revenue into your bank. For many, this includes looking at partnering with alternative lenders.

With the right lending partner, community banks can strengthen and diversify their loan portfolio through new income opportunities. A strategic partnership can provide you with access to quality loans that align with your business goals and enable you to work toward your growth plans — without additional time or cost.

These five questions can help you quickly uncover a potential partner's credibility and commitment so you can focus on increasing your revenue while mitigating your risk:

1. What is your track record of success?

Gauge how the lender has endured market changes. The economy is still recovering and this won't be the last downturn — seek to understand how they navigate uncertainty. You want a resilient partner that can originate quality loans for your portfolio at any time, has a track record of success and can adjust its business model to meet your needs.

2. How do you make lending decisions?

Quantitative analytics and historical borrower data are key, as they uncover variables that predict risk. Utilizing data is commonplace today, but a partner that dives deep into the analytics can make better predictions when originating loans, resulting in a stronger return on the portfolio you purchase.

3. How do you attract borrowers?

You want access to expertise and experience. The best way to attract the highest quality borrowers is through selective targeting and investing in marketing. Partners that execute innovative, highly targeted campaigns across every marketing channel and are precise in who they lend to, offer a unique advantage in the marketplace. This ultimately creates a better loan offering for your bank.

4. How does your underwriting process create efficiencies for our bank?

Evaluating credit files is time-consuming. Your partner should offer a simplified underwriting process with consistent loan packages, so you can quickly and easily analyze files to make informed purchasing decisions.

5. What is your commitment to service?

Borrowers seek out their local community bank because of the personalized level of service you provide. Your partner should also place a high value on service to ensure a positive borrower experience every step of the way.

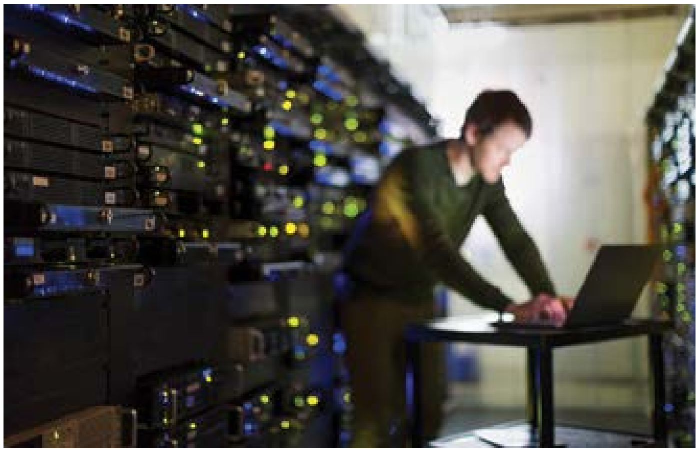
The pandemic has been challenging for community banks across the country. It has also posed a new opportunity for banks to partner with alternative lenders to drive fee income and new revenue streams into your business. Adding high-performing assets and maximizing yields can help boost your profitability for those who are willing to seek out new partners this year. ■

Keith Gruebele is Executive vice president of Institutional Relationships at Bankers Healthcare Group. BHG has been lending for nearly 20 years and is the #1 source for medical and professional loans across the country. More than 1,200 banks have partnered with BHG and see a $0 loss on the BHG Core Loan portfolio, record volume available and a 3.25-6% return. For more information, visit BHGLoanHub.com.

Six-degree Hacker Assessment: Is Your Information at Risk?

BY JOE OLEKSAK, PLANTE MORAN

There are six key layers of control separating your data from unauthorized access or hackers. Leaders need to understand how effective each layer is in protecting your organization.



Organization leaders and stakeholders are asking: "Are we vulnerable to hackers?" A six-degree hacker assessment will provide answers by testing each layer based on current hacking trends and real-world threat scenarios.

1. Internet: Internet-accessible information and systems are the public face for every organization. Unfortunately, this information and these systems can be used by hackers to gain unauthorized access to your internal network, or worse, your most critical data.

2. Social: Users are an organization's critical line of defense in securing and protecting information and assets. They can intentionally or unintentionally pose a risk to an organization by not exercising due care. Social attacks target staff who do not properly understand their role and responsibilities regarding information security. Not to be outdone (but often overlooked), physical building and network controls are just as important for thwarting many common social attack organizers responsible for several recent well-known breaches.

3. Peripherals: Today's decentralized physical and logical security models give staff responsibility for critical physical devices and data 24/7 through firewalls and VPNs. Our mobile workforces are armed with laptops, mobile phones and tablets, which could result in a significant data breach if left uncontrolled. If configured improperly, our firewalls and VPNs create potential tunnels into the core of an organization.

4. Passwords: Currently, passwords are the single most important line of defense when controlling access to data and systems. Passwords grant access to remote access VPNs, networks, applications, databases and sensitive file shares. Practices of password sharing, password reuse and poorly chosen word combinations have resulted in many of the breaches we hear about in the daily news. Password construction, use, and protection practices are, without question, one of the most important security control layers for organizations today.

5. Systems & databases: Applications, databases, and networks share house critical organizational data, including security controls critical to protecting an organization's vital data assets. Improper access controls, system configurations, older versions, or missed patches often result in unwanted holes, which, if left unaddressed, can lead to a system compromise, or worse, a breach of critical company data or confidential customer information.

6. Network: Networks allow users, customers, and vendors to communicate effectively and operate efficiently. When designed with security in mind, networks can limit hackers, viruses, ransomware, and malware to move freely between systems. Also, hackers compromise networks an average of 90 days before being discovered. Often, this is the direct result of weak or nonexistent detective controls. In today's world, a proper network, one designed with security in mind, is essential for any company, regardless of industry.

Cybersecurity includes applying administrative, technical, and physical controls to protect against threats to the confidentiality, use, and integration of technology throughout organizations. Today, those threats affect more than just IT — they affect the entire organization. With that in mind, an organization-wide security strategy is essential for successfully protecting confidential data throughout the organization. A six-degree hacker assessment can help you focus on developing solutions for the areas that present the most risk to your organization. ■

The National Defense Authorization Act: BSA/AML Initiatives

On Jan. 1, 2021, the Senate voted to override President Trump's veto on the National Defense Authorization Act (NDAA or Act). It was previously overridden by the House back on Dec. 28, 2020. The NDAA included over 200 pages of significant reforms to the Bank Secrecy Act (BSA) and other anti-money laundering (AML) laws putting forth the most comprehensive set of BSA/AML reforms since the USA PATRIOT Act of 2001. The continuing question is, what are the implications of this Act? How will this impact not only financial institutions but also U.S. companies and companies doing business in the United States at large?

For starters, certain U.S. companies and companies doing business in the U.S. ("reporting companies") will be required to provide FinCEN with information regarding their beneficial owners. This includes names, addresses, dates of birth, and unique identifying numbers. Newly incorporated companies will be required to do so at the time of incorporation. Exempt companies include public companies, as well as companies that: (i) have more than 20 full-time employees, (ii) report more than $5 million in yearly revenue to the Internal Revenue Service, and (iii) have an operating presence at a physical office within the United States. Changes in beneficial ownership will require reporting companies to provide FinCEN with updated information within a year. FinCEN has stated it will maintain a registry of this beneficial ownership information, but it will not be public. However, this does not prevent FinCEN from sharing this information with federal, state, local and tribal law enforcement agencies if there is appropriate court approval. FinCEN can also share the beneficial ownership information with financial institutions for customer due diligence purposes, but only with the reporting company's consent.

Second, this NDAA creates a new whistleblower program and establishes a private right of action for whistleblowers who have experienced retaliation. Aiming to incentivize reporting of BSA/AML violations, this program will award whistleblowers who give tips with as much as 30% of the monetary penalties assessed against the company if it leads to monetary penalties in excess of $1 million. This will depend on the significance of the information, the degree of assistance provided, and the government's interest in deterring BSA violations through these awards. Additionally, a private right of action for whistleblowers who suffer retaliation will be available — whistleblowers can file complaints with the Occupational Safety and Health Administration (OSHA) where, if OSHA fails to issue a decision within 180-days, the whistleblower will be free to file a claim in federal district court.

Third, the Act considerably increases the penalties for BSA/AML violations for both companies and individuals. For repeat violations, additional civil penalties of either (i) three times the profit gained or loss avoided (if practicable to calculate) or (ii) two times the otherwise applicable maximum penalty for the violation are now in play. A new BSA provision will allow for fines "equal to the profit gained by such person by reason" of the violation. It will also include bonuses paid out the year in which the violation occurred or the following year for financial institution directors and employees. Those who have been determined to have engaged in "egregious" violations of BSA/AML provisions may even be barred from serving on the board of directors of a U.S. financial institution for 10 years from the date of the conviction or judgment. Lastly, the Justice Department will, for the next five years, submit reports to Congress on the use of non-prosecution and deferred prosecution agreements during BSA/AML concerns.

Fourth, the NDAA will also require the Treasury, in conjunction with the Justice Department and other agencies, to evaluate how it plans to streamline SAR and CTR requirements, thresholds and processes. Within one year of the NDAA's enactment, the Treasury must propose regulations to Congress to reduce burdensome requirements and adjustment thresholds accordingly, with the expectation of these threshold adjustments taking place once every five years, for the next 10 years.

Fifth, the Act highlights the importance of law enforcement's involvement with international AML issues. FinCEN's mission requires working with foreign law enforcement authorities to safeguard the U. S's financial system. To assist, the Treasury will be required to establish a Treasury Attachés program at U.S. embassies abroad and work with international organizations including the Financial Action Task Force, International Monetary Fund, and Organization for Economic Cooperation and Development to promote global AML frameworks. Additionally, FinCEN will appoint Foreign Financial Intelligence Unit Liaisons at U.S. embassies to engage with their foreign counterparts. Over $60 million per year has been allocated between 2020 and 2024 to the Treasury to provide technical assistance to foreign countries promoting compliance with international standards and best practices for establishing effective AML and counter-terrorist financing (CTF) programs.

Additionally, the NDAA expands financial institutions' ability to share SARs with foreign branches, subsidiaries and affiliates, and requires the Treasury and FinCEN Secretary to create a pilot program to achieve this objective. Currently, financial institutions are only permitted to disclose SARs to foreign affiliates that are a "head office" or "controlling company." This has posed as a roadblock for enterprise-wide compliance within global banks. It is important to note that the Act does prohibit participants in this pilot program from sharing SARs with branches, subsidiaries and affiliates in China, Russia, and other specific jurisdictions.

Lastly, the NDAA significantly modifies the U.S. BSA/AML program in the following areas:

- Introduces several studies relating to (i) artificial intelligence, blockchain and other emerging technologies; (ii) beneficial ownership reporting requirements; (iii) trade-based money laundering; and (iv) money laundering by the People's Republic of China.

- Modifies various definitions relative to virtual currencies and other nontraditional cash substitutes;

- Introduces antiquities dealers (but not art dealers) to BSA's applicable scope;

- Expands ability to subpoena foreign banks' records that maintain correspondent accounts in the U.S.;

- Creates a "FinCEN Exchange" to oversee voluntary public-private information sharing between law enforcement, national security agencies and financial institutions; and

- Envisions a no-action letter process for FinCEN;

Apart from these topics, the NDAA reincorporates an emphasis on risk-based approaches to AML program requirements and discusses prior proposed rulemaking from FinCEN. It even includes discussions on the Treasury being required to periodically publish on national AML and CTF initiatives.

There is no doubt that the NDAA's initiatives will be extended over several years and require continued efforts by public and private sectors. The cost of these initiatives to the financial industry and small businesses has yet to be determined and remains a cry of protest from those against the reform. But this does appear to be the start of a more globally-centric effort to combat financial terrorism and money laundering crimes. ■

Elizabeth K. Madlem Vice President of Compliance Operations and Deputy General Counsel

Elizabeth is the Vice President of Compliance Operations and Deputy General Counsel at Compliance Alliance. In the past, she served as both the Operations Compliance Manager and Enterprise Risk Manager for Washington Federal Bank, a $16 billion organization headquartered in Seattle, WA. She has the industry expertise and real-world solutions surrounding bank-enterprise initiatives and knowledge of contract law and bank regulatory compliance. An attorney since 2010, Elizabeth was a Summa Cum Laude, Phi Beta Kappa, Delta Epsilon Sigma graduate of Saint Michael's College in Burlington, VT, and a Juris Doctor from Valparaiso University School of Law in Indiana.

As the Vice President of Compliance Operations, Elizabeth will be overseeing C/A's day-to-day operations of the Hotline and leading our Education initiatives. Elizabeth plays an important part in all operational areas of C/A.

Today for Tomorrow – Proactive, Risk Mitigating Steps for Lenders

BY LUCAS L. SCHNEIDER, OF COUNSEL

Special asset groups, already confronted by the portfolio's challenges bestowed upon them, face additional hurdles unique from their colleagues at lending institutions. Today's current economic climate, combined with the novel ways in which business must be conducted to safely distance, adds yet another complexity. Valuable face time in meetings with customers, reasonably foreseeable business and social climates in the relatively short term are factors that are no longer predictable. Several pieces of reminder guidance, structured around communication, diligence in managing loan files, and the tools for addressing the alternative paths the lending relationship may head, help position special asset groups and loan officers in mitigating lender liability risks and managing their loans and workouts, especially during a downturn in the economy.

Communication

The seminal theme is that clear, retained, and timely communication with borrowers, even when the information may be generally unpalatable or explain undesirable potential consequences, is critical to mitigate the risk of lender liability claims. Communication, or its evil counterpart miscommunication, is a paramount consideration toward reducing such risk. By way of example, in the case In re POC Properties, LLC, 580 B.R. 504, 507 (Bankr. E.D. Wis. 2017), a lender going through its own acquisition quietly downgraded loans with a longtime borrower and had its special assets management unit review the loans, all without informing the borrower's principals. This precipitated months of negotiations that were not fruitful, culminating in the borrower's principals filing a state court action against the lender alleging bad faith and misrepresentation, which then became the basis for objections to the lender's successor's Proofs of Claim in bankruptcy court.

Now that is the worst-case scenario — a lender working through the middle of its own acquisition, adapting to changing policies and personnel, while also performing its day job of managing its borrower relationships — unfortunately resulting in principals of the borrower claiming that had they known sooner of the troubled cloud over their loans, they would have had time to refinance and fully compensate the lender. Ultimately, the bankruptcy court gave credence to the borrower's lender liability claims, offsetting and reducing the lender's successor's claims.

For a local example, the Tenth Circuit Court of Appeals in a case from 1993 upheld a jury's finding that the bank breached an implied covenant of good faith and fair dealing when the bank under the contractual terms, exercised an assignment provision for funds derived from good operators, without first notifying the borrower and giving the borrower an opportunity to cure. These notice and cure "rights" were not derived from the contractual arrangement but from the relationship and course of dealing between the borrower and lender, as the case further elaborated. This leads to the next logical question of both what a SAG or loan officer anticipates in today's business environment, including risks and how they should proactively do so?

Loan File Review

From an anticipation standpoint, when a special asset group, or better yet, the loan officer on a still-healthy loan that is up for renewal, has an opportunity to review the loan file for any potential problems sooner rather than later, that diligence can yield dividends in risk management. The following is an exemplar overview of what to review:

- Review all loan documents to confirm that all have been signed by all parties (including all notary blocks) and that all documents have been properly dated;
- Review all loan documents to confirm that all referenced exhibits have been attached (especially legal descriptions);
- For loans secured by real property, ensure the file contains the final Lender's Title Insurance Policy and that the legal description in the policy matches the legal description in your deed of trust. Also, review to confirm there were no additional exceptions to title added after closing and before issuance of the policy;
- Conduct a UCC search to confirm that liens that were paid at closing have been released and that no new junior liens have been filed without your permission. If there is a junior lienor, consider whether an inter-creditor agreement might be appropriate if there is overlapping collateral; and
- Obtain updated good standing certificates from the state where the entity is registered and from the state(s) where the entity does business.

By way of example for "why" this is important in risk management, in a 1996 Colorado Supreme Court case, the creditor, in line with its strategy, successfully relied upon the lack of signatures on several credit agreements to win its case. The case emphasized the strength of the credit agreement statute of fraud in Colorado, codified at § 38-10-124(2), which generally precludes either a debtor or a creditor maintaining an action or a claim relating to a credit agreement where the credit agreement is unsigned by the opponent and for more than $25 thousand. That partially executed guaranty in a loan file, when everyone can recall seeing the borrower sign it, but no one can find the borrower-signed copy, creates the lender's risk of being unable to enforce the guaranty. Resolution, through the execution of a new and retroactive guaranty, can be collaborative and amiable, though, when the borrower is seeking a deferral or extension on maturity, and the creditor performs a loan file review understand such issues. The adage that a stitch in time saves nine is certainly applicable, especially in or near the down portion of the economic cycle when the potential of having to rely upon guarantees and first position in a bankruptcy is a real possibility.

Then, with the borrower and lender in sync on communication and all of the boxes checked in the loan review, the lender still may have to revisit workout routes with its borrower with the loan file in good form due to a contraction in the economy.

Tools in the Deferral Negotiations

When that time arrives, when the loan is faltering due to decreasing borrower revenue and the borrower needs an extension, but the lender requires added assurances, there are proverbial arrows in the lender's quiver. In the current market, where softening has occurred in the hospitality and restaurant spaces, for example, the borrowers remain the most effective value-enhancing operators of the collateral when the country reopens, in return for loan deferrals, lenders have the option of requesting additional collateral. One often-utilized tool for lenders is to have the borrower add increased operating funds, in an amount calculated to assist the borrower in weathering the downturn, to a deposit account in the control of the lender, thereby using the advantages of UCC Article 9 that provide the lender a priority secured interest in the deposit account.

Harkening back to the clear communication advice, the key is to be transparent with the borrower in what is being requested and what is being offered. In a 2006 Colorado Court of Appeals case that led to protracted litigation to rectify matters for the creditor, the day after the lender conducted a field audit that revealed the borrowers had defrauded the lender for years on the extent and value of collateral, the lender's representative presented the borrowers deeds of trust to add collateral. The borrowers alleged that the lender's representative's verbal statements at the meeting caused the borrowers to believe the lending relationship would continue, and the lender would forbear from calling the loan due. This was not the case, and the lender filed suit on the loan within a month. Clarity, and a follow-up email or letter, may have thwarted the borrowers' subsequent litigious plans much sooner. Despite that, the lender requesting in good faith additional collateral, in and of itself and consisting of a secured interest in land, in this case, was a tactful strategy.

Conclusion

The difficulty in discussing negative topics while maintaining the relationship, the chaos of a multi-party deal closing, the strain of renegotiating the lending relationship can all contribute to understandable oversight. That said, the above cyclical reminders on improving communication, reviewing and repairing the loan file, and using effective tools to maintain the loan relationship distill to two concepts — diligence and forethought — that, when appropriately applied, redirect the situation to a more positive outcome. The present economic stall is an opportunity to revisit these concepts for the much-needed refresher that lenders and their counsel periodically require. ■

STINSON

Establishing and Maintaining Pay Equity

BY JOSH WHITTAKER, KEVIN KUSCHEL AND SIDNEY DIEC

In a previous article written by L&A in 2018, the growing concern of gender pay gaps and how they impact attraction and retention issues in corporate America was addressed. Through this process, it was discovered that the pay equity gap was not as serious as previously thought — at least to the extent as portrayed in political circles and media outlets. The incorrect messaging generates doubt and forces the questioning of historical practice and future application of compensation programs. As compensation professionals, should we not concern ourselves with ensuring equitable pay programs across our organizations? Is there a need to continually monitor pay programs to ensure a gap is not unknowingly created? The answer is yes, but how do we ensure pay equity is properly established?

While studies have shown that most companies have done a good job of properly aligning pay, independent of race, age or gender, there remains a need to establish and maintain equitable programs based on these factors. Of course, organizations must also be careful not to take this approach too far, disallowing adjustments for more "justifiable discrepancies," such as tenure, experience, education level and performance. These are the true drivers of competitive programs, and if improperly managed to ensure personal bias is excluded from the process, the effectiveness of compensation programs is compromised.

Strict adherence to pay equity without considering distinctions across employees with similar duties can be detrimental to your employees' morale and commitment and the integrity of compensation-setting best practices. Compensation programs should take into consideration pay equity of similar positions but should not dictate how those plans reward the employees who distinguish themselves. Knowing when pay discrimination is justifiable and how to mitigate potential litigation in the future is critical to your organization's success. Below are some methods to consider for establishing the foundation for justification:

- Developing comprehensive job descriptions that clearly define the differences in responsibility between jobs and each job's levels.

- Establishing guidelines for flexible compensation offers, such as starting salary, raises, and promotions when planning incoming prospective employees' recruitment. This also includes pay negotiations that either an incoming prospective employee, current employee or even the organization may initiate.

- Keeping detailed records of the reasons for each compensation decision made for each employee.

Consistency in applying these methods for all employees and not deviating without good reason is an absolute necessity. If not, these methods can no longer be considered defensible or justifiable. Additionally, employers can limit liability for potential risk. In particular, by promoting transparency, employers proactively diligently evaluate their compensation practices (i.e., inconsistent or outdated pay policies), which could later be used in audits if cited as a pay equity claim.

The goal then should be to conduct regular pay audits to mitigate the risks. Planning for this endeavor is critical. The initial action of a successful pay audit is to identify the goals and objectives of the audit. It could be that your company is attempting to mitigate legal risk and take advantage of regulatory safe harbors. In other instances, an audit's purpose is in response to shareholder demands for proof that a pay gap does not exist. It might be that your company desires assurances that employees are equitably compensated. The audit's purpose ultimately dictates the process and methodology.

The process and methodology approach should be robust and all-inclusive, following these general steps:

1) **Establish the team.** This should typically include HR, internal legal, outside counsel and compensation consultants.

2) **Conclude which employees are performing similar or comparable work.** This should not be confused with equal work, as comparable is a more broad definition. This stage is where the importance of proper job titling and job descriptions is realized.

3) **Analyzing data based on the job groups identified in step 2.** The focus of most companies over the past few years has been on gender inequality. While this is certainly an area of focus, ensuring all protected employee classes are similarly assessed is important. This is a simplified analysis, reviewing one person's salaries versus the next based on gender, race and age alone.

4) **The next step is applying unique individual factors that impact compensation levels, e.g., experience, tenure, education and performance.** This process is more complicated and requires specialized scoring methodologies to rank employees within each job group.

5) **Identifying and assessing pay discrepancies relative to federal and state laws to ensure they are justifiable.** Although other reasons exist, most cases justify pay differential if it can be demonstrated that the variance is attributed to i) a seniority-based system, ii) a merit-based system or iii) a method that quantifies earnings or quantity or quality of production. These allowances also apply to Colorado's new Equal Pay for Equal Work Act, which went into effect in January of this year. By now, Colorado employers should be familiar with the provisions under the act and be aware of the unique requirements not found in any other state law. Specifically — companies must make efforts to make known all opportunities for promotion to all their current employees on the same calendar day. They must disclose the salary or hourly pay rate or range of every job opening and describe all other benefits offered. The law intends to enforce equitable pay practices and transparency, new notice and record-keeping requirements, and encourage employers to periodically self-audit their compensation practices.

6) The last step is documentation and taking corrective action where necessary. Discrepancies will probably be identified. These will likely be minimal and the impact marginal, but adjustments will likely need to occur.

By promoting transparency, employers proactively diligently evaluate their compensation practices (i.e., inconsistent or outdated pay policies), which could later be used in audits if cited as a pay equity claim.

There is a need to establish and maintain pay equity across all industries, but specifically, in the Banking sector, research shows the gender pay gap is wider. There is much work to be done; however, the industry is starting to take action to close the gap with key approaches centered around recruitment, retention and career advancement. Additionally, as diversity issues continue to take center stage, companies should consider implementing gender diversity policies to attract, retain and advance female talent.

Although not the systemic problem portrayed by radical media and politicians looking to sway the vote, pay equity is an issue that needs constant monitoring. Given the regulatory and business ethics issues surrounding pay equity, compensation professionals would be remiss to ignore the issue and hope for the best. ■

Why Your Bank Should Consider Selling Their Charged Off Debt Files

BY CRAIG GEISLER, CEO CHERRYWOOD ENTERPRISES

Like many banks nationwide, you probably have a considerable amount of charged-off loans from the last four years. Like many banks, you might not know that your charged-off loans have value to a debt-buying company.

Charged-off loans are the dirty words in modern banking. You have lent funds to a bank customer, and it went bad. It is most likely due to a loss of job, divorce, injury, or in modern times: COVID. When this happens on a large scale, you are left with considerable loss. Now, we are sharing a great secret in the charged-off world that you might not know exists. Selling your charged-off loan portfolios.

Cherrywood Enterprises is a debt buying entity that has been in that space for over nine years, with their CEO Craig Geisler having spent over 14 years in the debt buying arena. Cherrywood Enterprises has worked with banks, credit unions, auto lenders, and commercial lenders nationwide, helping these entities understand their charged-off portfolios' value and infusing capital back in these financial sectors.

What are the benefits of selling your charged-off loan portfolios?

- Create much-needed liquidity through a cash infusion from the sale of the distressed debt

- Bolster the bottom line now versus waiting months or years for collection efforts to take effect

- Reduce ongoing costs associated with internal collections as well as management of third-party agencies

- Lessen or eliminate reliance on third-party collection agencies

- Eliminate months or years of waiting without a guarantee of a return — a major benefit when factoring in the time value of money

- Protect your brand — this is typically the effect of a debt buyer owning the purchased accounts outright, having a longer time horizon, and, therefore, a strong incentive to work professionally with debtors and obtain repeat business from you

The process of selling your charged-off debt portfolios is simple: we first send you a Mutual NDA to protect both parties' proprietary information. We also send you a blank Excel Spreadsheet with the headers of information we would need to review your portfolio, and we would need the sample docs for one account. It takes us approximately 3-5 business days to review these docs, and we will come back with an offer for your portfolio. Once we agree on a price, we send you a Purchase and Sale Agreement for both parties to sign, and within 24 hours of receiving that signed agreement, funds are wired directly into your account. Once you have the funds, we would need the backup docs for all of the accounts sold, and we are on our way.

It's that simple!

No further action is required on those accounts that your bank has sold! Plus, this is a program that you can do on a monthly, bi-monthly, quarterly, or annual basis! It's just a matter of changing dates and numbers!

To get started, feel free to call us at (561) 508-7650 or email our CEO directly at cgeisler@cherrywoodenterprises.com

Come and see how easy and beneficial selling your charged-off loan portfolios can be! ■

WASHINGTON UPDATE

A Robust Recovery Requires Consistent "Rules of the Road"

BY ROB NICHOLS, PRESIDENT AND CEO, AMERICAN BANKERS ASSOCIATION

Throughout the pandemic, the U.S. economy has been tested like never before and has more than proven its resilience. That's thanks in no small part to our large and diverse financial system: a network of financial institutions of all sizes, charters and business models dedicated to providing the products and services that consumers and businesses need to thrive.

The diversity of our financial system is something that is uniquely American. We must preserve that diversity — but we must do so in a manner that protects all consumers equally and ensures a level playing field between providers of financial services.

In ABA's recently released Blueprint for Growth, a banker-driven document that will serve as our advocacy north star in the year ahead, we identified the need to promote innovation and ensure consistent regulation as one of the industry's top priorities in 2021.

This plan is not new, but it remains important as we confront modern life challenges — from emerging technologies to a changing climate to recovering from a global pandemic.

Banks have always embraced innovation. Indeed, innovation has a vital role in increasing economic competitiveness, promoting financial inclusion and expanding access to banking services. But financial innovation only provides these benefits when undertaken in a safe, responsible manner.

A consistent set of regulatory standards must be applied to financial services providers, including credit unions, banks or fintech firms. Unfortunately, we've seen several instances

in recent months of firms attempting to circumvent these regulatory standards by seeking charters that would allow them to access the banking system without being subject to the same rigorous regulatory standards applicable to the nation's banks.

A prime example of this is Figure Bank, which recently applied for a national banking charter through the OCC that, among other things, would allow it to operate without deposit insurance. If approved, this charter would enable Figure Bank to apply for membership in the Federal Reserve system while avoiding compliance with regulations like the Community Reinvestment Act.

We'll continue to oppose the approval of charters like these, and we'll continue to push back against any efforts that would enable new entrants into the financial services marketplace to cherry-pick which rules of the road apply to them.

We'll also continue our efforts to advocate against further tilting the field for tax-advantaged entities like credit unions and the Farm Credit System. For example, we are pushing strongly against a recent National Credit Union Administration effort to further loosen the field of membership restrictions. Even the agency's former chair blasted the move as "abandon[ing] rigorous and introspective analysis and its congressional mandate to stay clearly within the four corners of the Federal Credit Union Act."

Should policymakers accelerate attempts to push the Federal Reserve or the U.S. Postal Service into retail banking, we'll continue making the case that this kind of involvement is unnecessary because consumers are already well-served by a broad and diverse financial services sector. According to the FDIC, the share of unbanked U.S. households in 2019 reached a record low of 5.4%. Banks are working to close that gap further through the Bank On movement, and a fast-growing number of banks have signed on. Bank On certified accounts are now offered in 28,000 branches nationwide, in 99 out of the 100 largest metropolitan markets and in all 50 states.

For us to convey this message, however, we must ensure that community banks have the capacity and ability to keep innovating. That's why we've been working diligently through ABA's Core Platforms Committee to smooth over some of the bumps in the road that have historically held banks back from rolling out new digital products and services that their customers want and that they need to remain competitive.

By supporting the digital transition — an effort that was well underway before the pandemic but is now accelerating at an even faster pace — America's banks can continue their work to support an economic recovery that is robust and inclusive. ■

PEOs and Financial Wellness

BY CHANDLER PETTY, NEXTEP

Ensuring your business has a stable foundation is critical to successfully navigating unforeseen circumstances and keeping a solid footing through hard times.

The evolution from entrepreneur to employer is never an easy one, and it's very rarely the reason anyone sets out to start a business. Managing daily HR tasks can cost business owners a tremendous amount of time and money if not done properly.

Partnering with a Professional Employer Organization (PEO) can help businesses gain access to Fortune-500-style benefits, dedicated HR experts, and a robust suite of technology. PEOs are a one-stop shop and can lead to major cost savings for your business. According to the National Association of Professional Employer Organizations (NAPEO), average PEO clients can expect a return on their investment of partnering with a PEO based on cost savings alone — the cost savings from using a PEO is an average of $1,775 per year per employee!

PEO and Financial Stability

Take a look at these stats from NAPEO. Businesses that work with a PEO:

- Are 50% less likely to go out of business
- Have 10-14% less turnover
- Grow 7-9% faster
- Were 119% more likely to receive COVID-19-related PPP loans
- Were 60% less likely to permanently close during the COVID-19 pandemic

Source: napeo.org

Rather than paying the big bucks to set up your own company medical plans, most PEOs have a large group master medical plan that provides top-tier benefits to help your company attract and retain talented employees. Instead of managing administrative tasks across multiple websites and vendor accounts, PEOs offer technology solutions to streamline your HR experience.

Guidance Through Hard Times

There are few better examples of how working with a trusted PEO can provide guidance when you need it most, than the COVID-19 pandemic. As a flurry of legislative initiatives passed, PEO HR and legal experts were hard at work providing resources and sending out information on legislative updates that impacted clients. Most PEOs have a team of Society for Human Resource Management (SHRM)-certified HR professionals to keep you informed and help make the best decisions for your business across constantly evolving HR topics.

TIME SAVED = MONEY SAVED

Often, entrepreneurs wear multiple hats, from the owner and human resources to payroll experts and more — PEOs help take care of the administrative HR tasks so you can focus more time on moving your business forward. As your company grows, so do the demands on your time. A trusted PEO partner can take the administrative burden off your shoulders, like running your payroll, managing your benefit plans, bulking up your recruiting efforts, researching new HR legislation, and compiling W-2 info for you and your people. Partnering with a PEO is a great way to empower your business with a team of HR experts, technology and long-term financial stability.

Financial Transparency

Transparency is one of our guiding principles at Nextep. We hang our hat on our promise of no-fee functionality and transparent billing — meaning our clients won't be sneakily charged for services. We take this so seriously, we've even racked up some industry certifications! Nextep is an IRS Certified PEO* with a SOC 1 Type 2 designation and an ESAC accreditation, backing up our commitment to conduct business safely and honestly.

As an ideal PEO for the banking industry, Nextep works specifically with Colorado Bankers Association to empower its members with our robust suite of technology, friendly HR experts, and next-level customer service. Nextep is here to help you navigate the challenges of running a business. From easily accessing in-depth company analytics, accessible HR business partners, and risk and compliance services, we give you the tools you need to make quick and informed decisions as a trusted partner by your side.

We've built our reputation on elevating the employment experience and enriching the lives of those we serve. We couldn't be more excited for the opportunity to serve the esteemed members of the Colorado Bankers Association. In short, Nextep is ready to help you get back to doing what you do best: running your business.

*The IRS does not endorse any particular certified professional employer organization. For more information on certified professional employer organizations, please visit www.IRS.gov. ■

COLORADO Banker
140 East 19th Avenue
Suite 400
Denver, Colorado 80203

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

This magazine is designed and published by The newsLINK Group, LLC | 1.855.747.4003