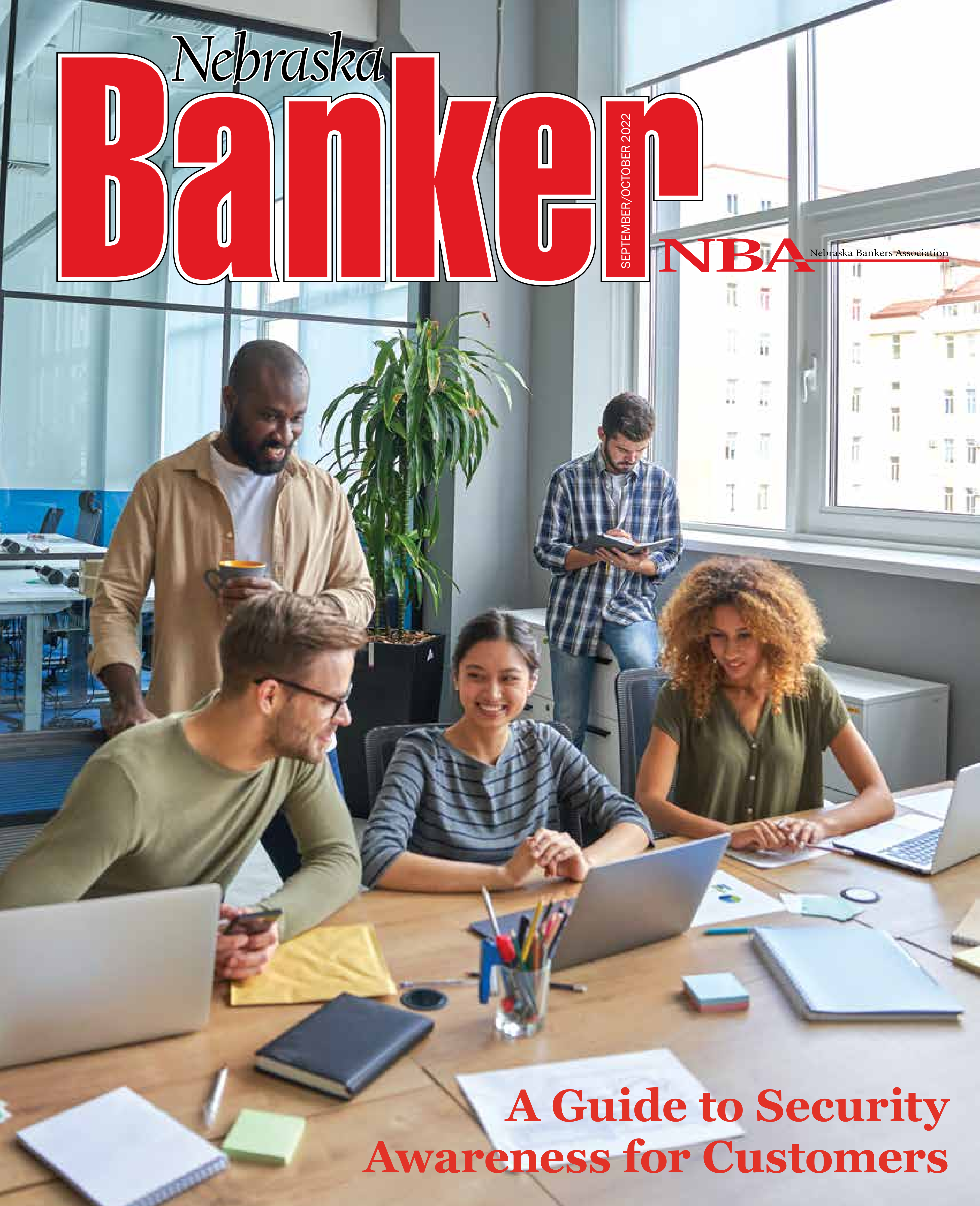
Nebraska Banker

SEPTEMBER/OCTOBER 2022

NBA Nebraska Bankers Association



A Guide to Security Awareness for Customers

OFFICIAL PUBLICATION OF THE NEBRASKA BANKERS ASSOCIATION

CONTENTS

Nebraska Banker
SEPTEMBER/OCTOBER 2022

EDITORIAL: Nebraska Banker seeks to provide news and information relevant to Nebraska and other news and information of direct interest to members of the Nebraska Bankers Association. Statement of fact and opinion are made on the responsibility of the authors alone and do not represent the opinion or endorsement of the NBA. Articles may be reproduced with written permission only.

ADVERTISEMENTS: The publication of advertisements does not necessarily represent endorsement of those products or services by the NBA. The editor reserves the right to refuse any advertisement.

SUBSCRIPTION: Subscription to the magazine, which began bimonthly publication in May 2006, is included in membership fees to the NBA.

Interest Rate Risk and Investment Strategies Seminar

October 19-21, 2022 | Oklahoma City, OK

The Skirvin Hotel

The Skirvin Hotel
One Park Avenue
Oklahoma City, OK 73102
405.272.3040

WHO SHOULD ATTEND

Financial institutions' CEOs, CFOs, investment officers, board members, and those who are directly or indirectly responsible for financial management functions will benefit from this seminar. ***There is no cost for this seminar.***

ACCOMMODATIONS

A block of rooms is available at The Skirvin Hotel. Identify yourself as a Baker Seminar attendee (or group code TBG3) when calling **+1 (800) HILTONS**. The special room rate will be available until the room block is sold out.

AGENDA

Wednesday, 19th
Twin Hills
Golf 1:00 pm

Thursday, 20th
Breakfast 7:30 am
Seminar 8:30 am
Lunch 12:00 pm
Adjourn 4:00 pm
Dinner 7:00 pm

Friday, 21st
Breakfast 7:30 am
Seminar 8:30 am
Conclusion 12:00 pm

For your convenience, register for the seminar online at **GoBaker.com/oklahoma**. Call Skoshi Heron at 888.990.0010 for more information.

OCT

FEATURED SPEAKER

David Rosenberg — *President/Chief Economist & Strategist*
Rosenberg Research & Associates Inc.

Two years after the pandemic left financial institutions drowning in excess liquidity at historically low interest rates, the industry faces a new challenge... rising interest rates. The Fed has quickly pivoted from supporting the economy to fighting inflation and institutions are now facing the first rising rate environment in years. Regulators have watched with concern as loan and investment durations extended to record highs in a search for yield and will have a renewed focus on the Investment Portfolio and Interest Rate Risk Management. Portfolio managers can no longer be reactive, but must be proactive in managing their investment portfolio and balance sheet in the face of rising rates and a flattening yield curve. This seminar will examine all of these concerns and present actionable strategies to better prepare your institution for the uncertainty ahead.

Join us for an in-depth discussion of the following topics:

- **Economic and Market Update —** Review of current economic conditions and the outlook for growth, inflation, and interest rates
- **The Powell Pivot —** Update on rate hikes, tapering, and the outlook for Federal Reserve monetary policy
- **Interest Rate Risk —** How to ensure you are prepared for the heightened regulatory focus coming in the years ahead
- **Liquidity Risk Management —** Best practices for managing liquidity risk as rates rise
- **Investment Portfolio Strategies —** Adapting your strategy and finding the best relative value for rising rates and a flattening yield curve
- **MBS/CMO Market —** Balancing prepayment and extension risk in an uncertain mortgage rate environment
- **Municipal Market Update —** The latest on managing municipal credit risk and finding the best relative value

NATIONAL REGISTRY OF CPE SPONSORS

11 hours of Economics and Finance CPE credits will be earned for your attendance.

The BakerGroup

Member: FINRA and SIPC
www.GoBaker.com | 800.937.2257
Oklahoma City, OK | Austin, TX | Dallas, TX | Houston, TX
Indianapolis, IN | Long Island, NY | Salt Lake City, UT | Springfield, IL

NBA BOARD OF DIRECTORS

STEPHEN STULL
NBA Chair
(402) 792-2500
Nebraska Bank
Dodge

LYDELL WOODBURY
NBA Chair-Elect
(402) 359-2281
First Nebraska Bank
Valley

KATHRYN BARKER
(402) 333-9100
Core Bank
Omaha

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

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

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

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

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

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

ZACHARY HOLOCH
(402) 363-7411
Cornerstone Bank
York

DONALD JIVIDEN
(402) 759-8113
Heartland Bank
Geneva

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

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

MARK LINVILLE
(402) 337-0323
First State Bank
Randolph

KRISTEN MARSHALL-MASER
(308) 384-5681
Five Points Bank
Grand Island

BRANDON MASON
(402) 918-2332
Bank of the West
Omaha

JEREMY MCHUGH
(402) 867-2141
Corn Growers State Bank
Murdock

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

JAY PRESTIPINO
(402) 392-2616
First Interstate Bank
Omaha

LUKE RICKERTSEN
(308) 537-7181
Flatwater Bank
Gothenburg

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

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

TRAVIS SEARS
(402) 323-1828
Union Bank & Trust Co.
Lincoln

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

KELLY TRAMBLY
(402) 756-8601
South Central State Bank
Campbell

NBA EDITORIAL STAFF

RICHARD BAIER
NBA President and CEO
richard.baier@nebankers.org

KARA HEIDEMAN
Director of Communications and Marketing
kara.heideman@nebankers.org

NBA Nebraska Bankers Association

233 South 13th Street, Suite 700
Lincoln, NE 68508
Phone: (402) 474-1555 • Fax: (402) 474-2946
nebankers.org

Enhancing Economic Opportunities for All Nebraskans

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

Nebraska has historically been blessed with a very stable and resilient economy. Unemployment rates are well below the national average, per capita incomes are growing, the economy is highly diversified and exports are robust. Despite this extraordinary economic success, there are several counties and census tracts across the state that have not experienced the same level of economic prosperity. Significant efforts are underway at both the state and community levels to plan for and implement transformative changes aimed at improving the economic foundation of these economically disadvantaged areas. As community and statewide leaders, bankers will play a key role in these efforts.

The U.S. Department of Housing and Urban Development identifies 68 census tracts in 11 Nebraska counties where at least half of the households have incomes below 60% of the Area Median Gross Income or a poverty rate of more than 25%. Instinctively, we also know that every city and county in our state has both visible and invisible pockets of poverty that need increased attention.

In addition, several of Nebraska's low-income areas are home to large concentrations of Nebraska's Black and Brown citizens. Data recently released by the Federal Home Loan Bank of Chicago indicates that Nebraska has 46 census tracts defined as 2022 Low-Income Minority Areas. These census tracts are in eight Nebraska counties.

While the history and characteristics of these low-income regions are varied, they often share similar characteristics:

- Lower educational attainment rates
- Lack of financial understanding (financial literacy)
- Higher-than-average incarceration rates
- Below-average home ownership levels
- Limited career opportunities
- Inadequate small business and entrepreneurial opportunities
- Inexperience in navigating economic and political systems
- Language and cultural barriers (i.e., distrust of banks)
- An estimated higher percentage of unbanked and underbanked residents

Unfortunately, public policy and economic development strategies designed to improve these high-poverty areas often become political footballs. During the most recent session of the Nebraska Legislature, state senators approved American Rescue Plan Act federal expenditures of over $330 million to support generational and transformative change in low-income regions across the state, with a focus on Black and Brown communities. The legislative steering committee in charge of shepherding these community investments has engaged a consulting firm to offer guidance and has hosted numerous town halls and focus groups to discuss possible investments and priorities.

Nebraska banks are at the forefront of efforts to combat poverty in their communities. In any given year, Nebraska banks make millions of dollars in community investments and support important economic development programs focused on small businesses, including micro-lending and entrepreneurial technical assistance. Our industry is also directly involved in facilitating access to affordable housing through a myriad of public housing initiatives, including the low-income housing tax credit program. Nebraska banks also actively promote financial literacy and first-time homebuyer training. Many individuals from low-income backgrounds have also taken advantage of career opportunities in banking to improve their economic situation.

Moving forward, your NBA government relations team will remain active in discussions surrounding the ARPA fund distributions, with a focus on strategies and investments with the greatest long-term economic impact. We will also work closely on public policy to ensure poverty reduction strategies are implemented statewide. Finally, we will continue to seek member input and focus on additional efforts the banking industry can make to decrease the poverty level and increase incomes among our fellow Nebraskans. We all share the same goal of enhancing economic opportunities for all Nebraskans. Your feedback and insights around this prominent issue are especially valuable. Please feel free to reach out to any of our team members to share your thoughts and ideas.

Will the Federal Reserve Sell MBS?

Andrea F. Pringle, The Baker Group

This question is likely to garner different responses, depending on whom you ask, and a plethora of caveats. It is a tough call for the Fed because stifling housing-related inflation without punishing everyday homeowners is a tricky task. For investors, this question matters a lot because the Fed's cessation from active Mortgage-Backed Securities (MBS) purchases eliminated demand from the largest buyer in the market and had a punitive impact on MBS valuations. If the Fed starts actively selling into the market, that could exacerbate things even further.

Why Sell?

There is a solid case to be made for selling MBS because the Fed has repeatedly conveyed its desire to hold a portfolio of predominantly Treasury securities. It has already stopped active MBS purchases as part of Quantitative Easing (QE) and is allowing the amount of MBS that naturally runs off its portfolio through principal pay downs to increase over time. Unfortunately, this may not be enough to get to a Treasury-only portfolio.

With mortgage rates nearly double the historic lows set over the past couple of years, virtually all existing mortgages have lower rates than those available today. As a result, refinance – and even purchase activity – has slowed dramatically. As high mortgage rates disincentivize people from refinancing and moving, mortgage balances are being paid down more slowly, and the resulting runoff of the Fed's MBS balance sheet is happening more slowly as well. In fact, the maximum runoff caps set by the Fed to facilitate a gradual removal of its footprint likely will not even be reached through natural paydowns.

The Fed announced plans to gradually and predictably reduce its securities holdings by setting caps on the amount of MBS and Treasury paydowns reinvested in those securities. This process began in mid-June with an initial monthly cap of $17.5bn MBS

Whatever course the Fed will take regarding MBS sales is anybody's guess. It seems prudent to err on the side of caution and refrain from outright sales in the near term to give its previous actions some time to work.

for the first three months, which shifts to $35bn/month in September. However, with prepayments slowing in response to higher primary mortgage rates, the Fed's playdowns are already running below the planned maximum $35bn cap. In other words, organic MBS portfolio reduction will be much slower than the Fed wants.

To make matters worse, the Fed's Treasury holdings do not have this problem. The cap for Treasury securities was initially set at $30bn/month and shifted to $60bn/month in September. Because Treasury securities are not plagued by slowing prepayment activity like MBS, principal pay downs of Treasuries will be able to hit the full $60bn/month cap much more efficiently. This dynamic will cause the share of MBS in the Fed's portfolio to increase relative to Treasuries rather than decrease.

Additionally, a large part of the Fed's targeted Consumer Price Index (CPI) measure considers rental and housing costs. In order to rein in inflation, shelter prices as a component of CPI need to come down. Over the long term, shelter prices in CPI tend to follow trends in home prices, which have yet to slow materially despite higher mortgage rates. This suggests shelter prices could remain strong until at least mid-2023. Thus far, the Fed has only attempted to control this by raising interest rates, but pervasively high shelter costs could put pressure on the Fed to take further action to bring down CPI.

Why Not?

While the case for MBS sales may seem strong on the surface, the Fed has a delicate tightrope to walk to avoid overly burdening homebuyers/homeowners and significantly distressing the broader housing market. It takes time for rate hikes to actually cool inflation, so selling MBS may not do much to directly impact housing inflation in the near term. We are also starting to see the beginnings of a slowdown in housing activity, so taking further action now may be an unnecessary step.

Fed action has already worked to nearly double borrowers' mortgage rates at a time when home prices are also extraordinarily high. The combined effect of both dynamics has made it almost twice as expensive to buy the same house today as it was just two years ago. Consequently, some would-be homebuyers simply give up the search and are forced to rent instead. This serves to increase demand for rental housing and further raise the price of rentals. It follows that increasing mortgage rates when rental supply is already limited might actually have the effect of temporarily increasing housing inflation rather than decreasing it. Potentially worsening an already difficult housing affordability dynamic may give the Fed pause about pursuing MBS sales too soon.

Additionally, the MBS purchased by the Fed during the last round of QE was made up of mortgages with much lower rates than today. As a result, if the Fed were to start selling its holdings now, it would impact the supply of very low-coupon MBS. There would be relatively little effect on the price of higher-coupon MBS, which sets the secondary market for mortgages originated today. In other words, Fed sales of MBS would likely have a rather minor impact on thirty-year mortgage rates today.

Whatever course the Fed will take regarding MBS sales is anybody's guess. It seems prudent to err on the side of caution and refrain from outright sales in the near term to give its previous actions some time to work. If the slowdown in housing activity that appears to be underway now sticks, further action may be unnecessary. But if housing-related inflation becomes incessant, the Fed may have to resort to any means necessary to temper it.

Andrea F. Pringle is a Financial Strategist and MBS Analyst at The Baker Group. She began her career in Washington, DC, earning her MBA from George Washington University. Andrea worked on the Capital Markets Sales and Trading Desk at Fannie Mae for five years before returning to Oklahoma to work in corporate finance. Andrea joined The Baker Group in 2020, and her work focuses on mortgage products. Contact: 800-937-2257; apringle@GoBaker.com.

HEALTH BOOST

brought to you by Wellness Partners

Call us today at

877.345.7775

to take advantage of this service

a unique team approach to lowering your blood sugar

Quarterly Check-Ins with a Registered Dietitian

Unlimited Access to a Team of Specialists

Free A1C Testing

Reduced Diabetic Medicattions
(if certain conditions apply)

To learn more, email
msiebrandt@wilcoxcompanies.com

Wellness Partners
Your Preventive Care Specialists®

Questions, Issues and Strategies Involved In Opening Accounts Online

Sharvelle Washington, CAMS BSA/Compliance Officer Bankers' Bank of the West

The new era of opening accounts online is here. Over time, more people have opted to open accounts online instead of in person at a branch, as some of us might be used to. And with online account opening come uncertainties in staying compliant with Bank Secrecy Act requirements.

Even though the process of account openings has evolved, the requirements for opening accounts remain the same. This raises a question: How can one verify someone's identity without that person being present?

Of course, third-party vendors with solutions can be integrated into the financial institution's interface to collect all the data needed to open an account. But before the decision to integrate online account openings, it's important to do some research and resolve some crucial questions.

Start by determining your financial institution's risk tolerance for online account openings. This will hinge, in part, on the products an online applicant could enroll in. Risk tolerance varies from bank to bank and also depends on the products offered by each institution.

Start by determining your financial institution's risk tolerance for online account openings.

Next, conduct comprehensive due diligence on the third-party vendors you're considering. Compare what several companies offer with respect to the data collection process and their methods of verifying the customer. Determine whether the vendor can collect scanned or captured photo IDs and a live photo at the time of enrollment, and find out what you'll be able to provide when an auditor asks for verifying information. Make sure you'll have easy access to this information.

Never ignore red flags or evasiveness on the part of a vendor. If a potential service provider is unable or unwilling to give you satisfactory answers, it's not the right vendor for your institution.

Don't forget to create a marketing strategy for engaging new customers to open accounts online. Visual appeal is important today: Showing what the process entails could entice more people to sign up. Referrals from current customers may also draw in more new customers.

Finally, stay positive throughout the entire process. Opening accounts online is still a fairly new advancement in the financial services industry. Everyone is still learning and adjusting to changing times.

Sharvelle Washington had spent her entire career working for Fortune 500 companies, Promontory Risk Review and Western Union among them. 2021 became ACAMS certified, Colorado Native, Bachelors from University of Phoenix in Business Administration and project management certification.

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

BANKING - FINANCE - CREDITORS' RIGHTS
LEGAL SOLUTIONS FOR FINANCIAL INSTITUTIONS
KOLEY JESSEN
ATTORNEYS
KOLEYJESSEN.COM
402.390.9500
LOANS – TIF/BOND FINANCING
DIP FINANCING – BANKRUPTCY/CREDITORS' RIGHTS
BANK ACQUISITIONS/DIVESTITURES
REGULATORY COMPLIANCE – GENERAL CORPORATE

The Current State of Russian and Ukrainian Sanctions:

Where is the line of contact? Where is your line of risk?

Robert (Bob) Kardell, Baird Holm, LLP

Although the war in Ukraine is half a world away, the fighting creates a number of issues for local banks. United States sanctions policies have implications for banks not only for transactions such as SWIFT money transfers but also for the types of business and trade in which bank customers engage with Ukrainian businesses. Bank customers conducting wire transfers to Ukraine risk sending money to a region controlled by Russia; bank customers engaged in the import/export business with Ukrainian businesses risk violating import/export restrictions. Banks, in turn, risk violating U.S. sanctions policies in each of these scenarios.

Common Financial Transfers to and from Ukraine

The banks, individuals, addresses, and regions in which monetary transfers are terminated are important, but it is also important to bear in mind the types of businesses that may be restricted from trading with Ukraine. While a particular financial transaction may terminate in an uncontested area in Ukraine, the underlying items may be subject to additional regulation or prohibition.

In fact, the Bureau of Industry and Security (BIS) and the Financial Crimes Enforcement Network (FinCEN) recently

The regions of the prohibition will be determined by the Secretary of the Treasurer and Secretary of State on an ongoing basis.

issued a joint alert on increased vigilance for potential Russian and Belarusian export evasion attempts.[1] The agencies warn that companies may attempt to transfer money for regulated items such as aircraft equipment, antennas, breathing systems, cameras, integrated circuits and oil field equipment, to name a few, which require additional regulatory compliance considerations.

The alert specifically states:

> *Financial institutions with customers in maritime or export/import industries should rely on the financial institutions' internal risk assessments to employ appropriate risk mitigation measures consistent with their underlying BSA obligations.*[2]

In 2019, the U.S. and Ukraine engaged in $3.5 billion in trade.[3] Of this amount, approximately $2.3 billion was in U.S. exports to Ukraine, and $1.2 billion was in U.S. imports from Ukraine. The most commonly traded items were agricultural products, minerals, base metals, machinery, and transportation. These market items seem fairly innocuous, but many smaller market items may be heavily regulated and may require an export license. Among others, some regulated export items were optical sighting systems, integrated circuits for information security, cameras, shotguns and shotgun shells, and lasers. Banks should be alert for businesses engaged in the trade of such regulated products.

Office of Foreign Asset Control and Crimea

The Office of Foreign Asset Control (OFAC) is responsible for the Specially Designated Nationals and Blocked Persons List (SDN). This list is periodically updated to reflect the current sanctions issued by the U.S. President. Prior to the most recent invasion of Ukraine, former President Obama issued sanctions Dec. 24, 2014, to block monetary transfers to the Crimea Oblast or Region of Ukraine.

Given the geographic scope of these sanctions, it is important to provide a brief note on the geography of Ukraine. Ukraine is comprised of several "oblasts," administrative divisions or regions in Russia and some of its former republics, such as Ukraine. An oblast is similar to a province or region and comprises smaller regions and cities. Crimea was an oblast of Ukraine, and OFAC sanctions often refer to oblasts or regions.

The sanctions issued by President Obama were in response to Russia's occupation and eventual annexation of the region. Executive Order (EO) 13685 specifically prohibited "new investment in the Crimea region of Ukraine by a U.S. person, wherever located."[4]

This EO was straightforward and easy enough to follow – if the person or entity resides in the Crimea region, any new business transfer is prohibited. The Crimea Oblast is now (almost) universally considered to be part of Russia. Any transfers to the Crimea Oblast are strictly prohibited due to this EO, but also due to sanctions against Russia in general.

The Oblasts of Donetsk and Luhansk and the Current Conflict

Russia's most recent invasion of Ukraine has included the recognition of the independence of these regions and/or occupation of parts of the Donetsk and Luhansk Oblasts by Russia.[5] The occupation of these oblasts led to the issuance of EO 14065 by President Biden. The EO states in part restrictions on *"new investment in the so-called DNR or LNR regions of Ukraine or such other regions of Ukraine as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State (collectively, the "Covered Regions"), by a U.S. person, wherever located."*[6]

So while EO 13685 prohibiting investment in Crimea was fairly straightforward, the EO 14065 regarding the DNR and LNR is much less clear regarding the locations of transfers that may be restricted. The regions of the prohibition will be determined by the Secretary of the Treasurer and Secretary of State on an ongoing basis. This determination of the "Covered Regions" depends on the advancement of Russian forces to determine the so-called "line of contact." The line of contact is the stretch of land that separates conflict-affected people in Ukraine from the Russian-controlled areas of eastern Ukraine. This line of contact changes rapidly, even daily or weekly, and this change may be reflected in the determination of the Secretaries of Treasury and State.

This changing landscape created a regulatory nightmare for banks attempting to follow U.S. sanctions policy.

Practical Implementation of the Order and Risk Management

Transfers to and from the former oblasts of Ukraine, now referred to as the DNR and LNR, are prohibited, as are transfers to and from Crimea, but transfers to other regions may also be prohibited. Determining the legality of transfers

Counselor's Corner — Continued on page 20

Counselor's Corner — Continued from page 19

to regions other than these enumerated areas depends on the current line of contact. But as this line changes, so will the legality of such a transfer; a transfer approved today may be headed for a city occupied by Russia tomorrow.

To avoid engaging in a prohibited transaction, banks must determine their risk tolerance levels in one of three ways: 1) avoid transactions to the covered regions only; 2) avoid transactions to the covered regions and possibly compromised adjacent regions; or 3) avoid transfers to all areas of Ukraine.

The first option of avoiding transfers only to the covered regions of DNR, LHR, and other identified regions carries the most risk. While the covered regions are certainly off-limits, the line of contact will constantly change while the war continues, and adjacent regions may also become subject to sanctions. These persistent changes may result in a transfer that crosses the line of contact, thus violating the EO.

The second option of avoiding transfers to named regions and the oblasts surrounding the conflict area carries less risk, but is administratively difficult to implement. Such a plan avoids any possible prohibited transactions but requires a thorough working knowledge of the oblasts of Ukraine and the conflict regions. Bank transfers to safe regions will not be affected so long as the conflict and line of contact remain in adjacent territories. Such a plan also requires a regular review of the line of contact, affected oblasts and regions, and regular updates to a list of affected postal codes, addresses, and cities to compare scheduled wire transfers. The adjacent and possibly affected territories would include the oblasts of Dnipropetrovsk, Kharkiv, Kherson, and Zaporizhzhia.

Finally, the least risky of all policies is avoiding all transfers to Ukraine and businesses trading with Ukrainian businesses. Such a policy would avoid any inadvertent transfers to areas within or near the conflict area and avoid running afoul of trade licenses and restrictions.

Conclusion

The war in Ukraine has created many complications for U.S.-based banks. The constantly changing line of contact creates risks for banks that transfer money to the region. There are many possible pitfalls in allowing wire transfers to Ukraine or engaging with businesses that trade in regulated goods and supplies shipped to Ukraine. To be sure, banks are in a position to have a unique insight into the war. These business trades and money transfers provide banks with insight such as letters of credit to their customers, the types of banking operations and procedures in the war regions, and the insight gained from locations of termination for wire transfer payments as part of a correspondent banking transaction.

Finally, banks must be mindful and alert to the challenging issues in financing businesses in Ukraine or near the line of contact by implementing a comprehensive policy commensurate with their risk tolerance to mitigate such challenges.

---

[1] *https://www.fincen.gov/sites/default/files/2022-06/FinCEN%20and%20Bis%20Joint%20Alert%20FINAL.pdf*
[2] *ID at page 4*
[3] *https://www.bis.doc.gov/index.php/country-papers/2618-2019-statistical-analysis-of-u-s-trade-with-ukraine/file#:~:text=The%20U.S.%20trade%20balance%20with%20Ukraine%20is%20positive.&text=In%202019%2C%20of%20the%20%242.4,and%20Mechanical%20Appliances%20(9.8%25)*
[4] *Federal Register Vol. 79, No. 247, Wednesday, December 24, 2014, p. 77357*
[5] *The Donetsk Oblast is recognized by Russia as the Donetsk People's Republic (DPR and also referred by the Russian acronym of DNR); the Luhansk Oblast is also known in Russia as Luhansk People's Republic (LPR or by the Russian acronym of LNR).*
[6] *Federal Register Vol. 87, No. 36 Wednesday, February 23, 2022, p. 10293*

6 Low-Cost Ways
to Improve Your Cybersecurity

Your business is exposed to a variety of risks every day. Improving your cybersecurity can feel like a daunting task, but there are a few ways you can get started quickly. If you are unsure where to start, our security experts offer six low-cost, easy solutions that you and your team can implement to boost your security right now.

1. Data Backup and Recovery
Backing up your data is crucial but not all backups are the same. It is critical that you have an offsite data backup solution, keeping your data protected and stored outside your network.

2. Endpoint Detection Response (EDR)
Traditional antivirus software is not sufficient protection for your financial institution. Antivirus requires regular database updates of the current virus signatures to be effective. The protection afforded by AV software is only as good as the vendor's updates. Often, threats are discovered only after the damage is done. EDR uses artificial intelligence to detect threats without having to rely on virus signatures.

3. Multi-Factor Authentication (MFA)
Two of the best methods for establishing extra lines of defense for your online accounts are using strong passwords and setting up 2-factor or multi-factor authentication (also known as 2FA or MFA). Using different passwords for each of your accounts is another best practice to hinder an attacker and keep your data, accounts and network safe.

4. Third Party Patching
Keeping your devices, browsers and other tech up to date is one of the best, first lines of defense against cyberattacks. Security patches and updates fix any technical bugs and essentially "lock" your software and devices before bad actors can make a copy of the "key."

5. Avoid Suspicious Emails
With phishing, hackers attempt to gain access to your information or credentials through your email inbox. Phishing scams may seem like a relic of the past but have become one of the main culprits behind countless cyberattacks. Here are a few quick tips.

If the email address, link or contents look suspicious:

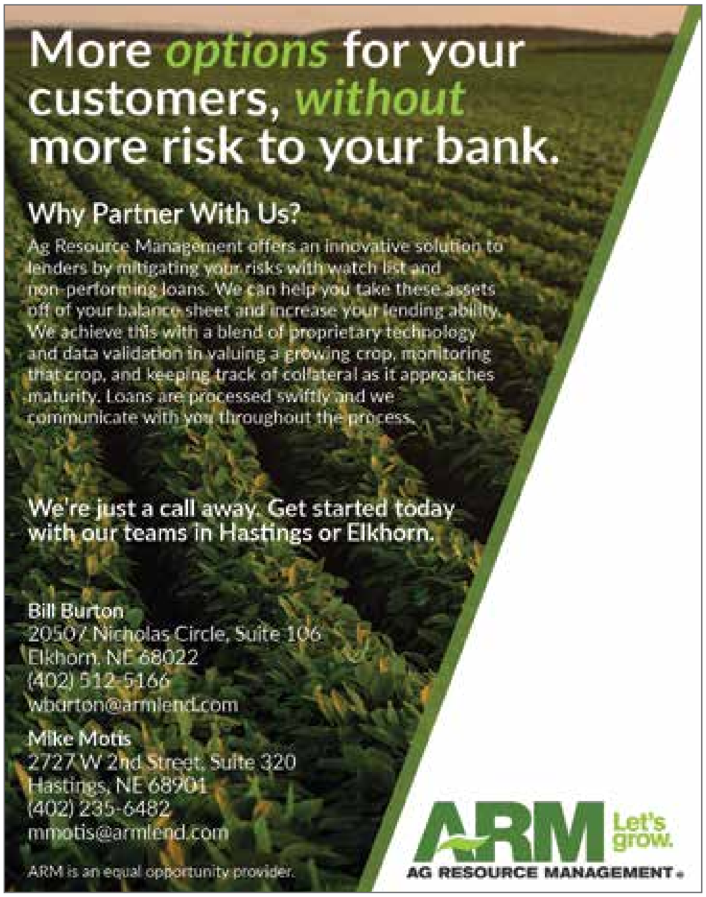
- Do not engage with the message or sender.
- Do not open the email, click on links or provide information.
- Contact your IT support immediately.

6. Book a Free Consultation
Hamilton is here to help mitigate and eliminate cybersecurity threats to your financial institution. We offer services from training, to network penetration tests and vulnerability assessments. **Contact us today to book a free consultation and learn how our cybersecurity solutions can help minimize vulnerabilities and protect your business data.**

For more information:

Scan to contact us today OR:
Call: 308.381.1000
Email: hisinfo@hamiltonisbusiness.com
Visit: HamiltonIsBusiness.com

HAMILTON®


More options for your customers, without more risk to your bank.
Why Partner With Us?
Ag Resource Management offers an innovative solution to lenders by mitigating your risks with watch list and non-performing loans. We can help you take these assets off of your balance sheet and increase your lending ability. We achieve this with a blend of proprietary technology and data validation in valuing a growing crop, monitoring that crop, and keeping track of collateral as it approaches maturity. Loans are processed swiftly and we communicate with you throughout the process.
We're just a call away. Get started today with our teams in Hastings or Elkhorn.
Bill Burton
20507 Nicholas Circle, Suite 106
Elkhorn, NE 68022
(402) 512-5166
wburton@armlend.com
Mike Motis
2727 W 2nd Street, Suite 320
Hastings, NE 68901
(402) 235-6482
mmotis@armlend.com
ARM is an equal opportunity provider.
ARM Let's grow.
AG RESOURCE MANAGEMENT


WALENTINE O'TOOLE, LLP
When time is of the essence, experience counts.
Walentine O'Toole blends confidence, experience and knowledge with the personal attention you can expect from a regional law firm.
www.walentineotoole.com
WALENTINE O'TOOLE, LLP
Attorneys at Law
402.330.6300
11240 Davenport St. • Omaha, NE 68154-0125


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

EDUCATION CALENDAR

For more information about these live and online education events and training tools, contact the NBA Education Center at (402) 474-1555 or nbaeducation@nebankers.org. You also may visit the NBA website at https://www.nebankers.org/education.html.

OCTOBER 2022

Regulation B Workshop
October 5-6
Virtual

Women in Banking Conference
October 19-20
Omaha, NE

Commercial Lending School
October 24-28
Manhattan, KS

Summit on Regulatory Issues
October 28
Lincoln, NE

NOVEMBER 2022

Bank Investment, Funding and Economic Outlook Conference
November 3-4
Lincoln, NE

Principles of Commercial/Ag Loan Documentation Workshop
November 8
Virtual

CyberSecurity Workshop
November 10
Virtual

Bank Directors Training Workshop
November 15
Kearney, NE

Bank Directors Training Workshop
November 16
Lincoln, NE

DECEMBER 2022

Agriculture & Beyond Workshop
December 6
Lexington, NE

Agriculture & Beyond Workshop
December 7
Norfolk, NE

NBA Nebraska Bankers Association

A Guide to Security Awareness for Customers

Eric Chase, Information Security Consultant, Client Services – SBS CyberSecurity

National Cybersecurity Awareness Month is back in October to promote educating the nation about cybersecurity and how everyone can be safer online. The initiative provides an excellent opportunity to evaluate the cybersecurity culture of your company and how you can share your knowledge and resources with your customers and community throughout the year.

Education and security awareness training are powerful tools when it comes to creating a strong information security program. It helps establish trust that your organization takes cybersecurity seriously and that you're committed to doing what's best for your employees and customers.

An organization with a strong security culture goes beyond internal employees and talks about cybersecurity threats with its customers as well. Educating customers about the dangers of cyber threats helps build a stronger relationship. Cyber savvy customers also benefit your business. A more secure customer will reduce the risk of their information becoming compromised or used maliciously against your business.

Cover the Basics

Your customers can benefit from the same security awareness topics shared internally, including, but not limited to:

- Recognize and report phishing
- Type of social engineering attacks and what controls can mitigate the risk
- Physical security threats and best practices
- Password best practices and password management tools
- Enable multi-factor authentication (MFA) whenever possible
- Updating software and patch management
- Remote access security
- Use of encryption
- Mobile device security
- Defending against malicious software
- Importance of anti-virus and firewalls
- Incident response plans

Tips to Share Your Knowledge

Most companies do not employ a staff of cybersecurity experts or only offer services to customers with a security background, so it is important to provide basic cybersecurity knowledge, best practices, and tips on a regular basis. A strong culture of cybersecurity at your organization has benefits beyond mitigating cyber risks; it builds confidence amongst your employees and customers that you have made it a priority.

Using multiple delivery channels to support training and education can help ensure your customers see it throughout the year. Delivery channels can include:

- Place or link to relevant cybersecurity tips, news stories, alerts, and cyber policies on your business website.
- Include a monthly tip in your newsletter or social media accounts to keep cybersecurity top-of-mind for your customers.
- Encourage your customers and employees to follow your organization or other cybersecurity organizations on social media for cyber tips and news.
- Incorporate cybersecurity tips into your on-hold message when customers call your business.
- Include cybersecurity resources with physical statements or invoices.
- Provide cybersecurity resources, control suggestions, or self-audits at the time of account opening.
- Place posters, articles, or other educational materials in the entryway, break room, bathroom, or other meeting areas.
- Invite your business customers and employees to attend an educational webinar, such as the free monthly Hacker Hour webinar hosted by SBS.

Host an event

One of the most popular and effective training methods is to invite your employees and customers to a virtual or in-person event. Getting out in front of your customers and talking about the importance of cybersecurity is a win/win:

1. You are helping to create cyber strong customers that are more resistant to attacks, benefiting both you and your customer.
2. You show your customers they are more than just a number. You're strengthening relationships and demonstrating care about their well-being.
3. You have an opportunity to show off new products/services or new features, as well as potentially increase the adoption of existing products or services.

For business customers: Plan a lunch and learn event focusing on the latest cybersecurity trends and tips for securing their business.

> An organization with a strong security culture goes beyond internal employees and talks about cybersecurity threats with its customers as well.

For the community: Host a cybersecurity awareness day for community members to shred sensitive documents, listen to short presentations, and play cyber-themed games or trivia.

For employees: Have an external presenter conduct training to help increase engagement. Many speakers will also make it fun by incorporating games or prizes for participants.

For your board: Have an expert discuss the trends they are witnessing, and the risks associated to generate increased buy-in.

Here are some additional considerations to keep in mind:

- Invite the community.
- Host several sessions to cover the most people possible. Consider recording the session for those unable to attend and/or to use for content later.
- Choose a platform (if virtual) that is easily accessible by your customers, user-friendly, and secure.
- Pair up with your chamber of commerce, a civic organization, or an academic institution.
- If you're not confident talking about cybersecurity, bring in a cybersecurity expert to speak on your behalf.

Talking about cybersecurity also offers a chance for your customers to see how your organization is protecting their information. In today's market, where cybersecurity is becoming a deciding factor for consumers with many options, being open and transparent about cybersecurity can instill customer confidence and draw in new customers.

Visit www.sbscyber.com > Education > Free Download for more security awareness materials you are free to share, including a Security Awareness Toolkit with security tip graphics, sample social media posts, and more. For more information, contact Robb Nielsen at 605-251-7375 or robb.nielsen@sbscyber.com. SBS helps business leaders identify and understand cybersecurity risks to make more informed and proactive business decisions. Learn more at www.sbscyber.com.

Cryptocurrency:
Safe or "Sus"?

Carol Ann Warren, Bankers Alliance

In today's financial regulatory environment, two of the hottest topics are (1) cryptocurrency and (2) cybersecurity. Within the past year, multiple agencies have released various regulations and guidance regarding cryptocurrency, banking, and cybersecurity, both individually and collectively.

As my teachers would say, if something is said more than once, it is probably important, and you will likely see the material again. Similarly, cryptocurrency and cybersecurity threats are likely here to stay, and regulators are preparing for those implications. Banks are now put on the spot to adapt to the market shift and the regulations that will surely follow.

What is cryptocurrency?

The Merriam-Webster's dictionary defines cryptocurrency as "any form of currency that only exists digitally, that usually has no central issuing or regulating authority but instead uses a decentralized system to record transactions and manage the issuance of new units, and that relies on cryptography to prevent counterfeiting and fraudulent transactions."

How does cryptocurrency relate to banking?

For bankers, the question of how cryptocurrency relates to banking is pressing and hard to answer. Crypto-currency usage is typically stereo-typed between two different groups: underground-market transactions (i.e., drug market or selling a kidney online) and GameStop/Reddit kids that almost crashed the stock market in 2021. Volatility and illicit activity are two of the biggest regulatory fears for bankers, so how do banking and cryptocurrency relate?

According to a November 2021 article from Pew Research, 16% of Americans have used or are invested in cryptocurrency. Of that 16% of Americans, 52% of those individuals are between the ages of 18-49. The individuals in this age group are not typical "in-person" banking customers.

First, who are the individuals actually investing or using cryptocurrency?

According to a November 2021 article from Pew Research, 16% of Americans have used or are invested in cryptocurrency. Of that 16% of Americans, 52% of those individuals are between the ages of 18-49. The individuals in this age group are not typical "in-person" banking customers. As the market is shifting and these individuals have more market power, banks scramble to advertise to this group. Cryptocurrency may be a way to do that successfully.

The guidance from regulators is that banking, one of the most highly regulated industries in the country, is supposed to mix with cryptocurrency, one of the most unregulated commodities in the world. The two seem like oil and water, but the Office of the Comptroller of the Currency (OCC) argues in Interpretive Letter #1170 that it is more like M&Ms and popcorn, an unlikely yet satisfying combination.

The OCC didn't actually say that, but they did argue that for banks, providing custodial services related to cryptocurrency would be in line with a bank's intended purpose – "safe keeping" of assets.

The banking world has been shifting from physical currency and safekeeping to virtual safekeeping for many years now. Therefore, the argument is that providing services for cryptocurrency is not a far-fetched idea, but a natural progression.

How does cryptocurrency relate to cybersecurity?

Because cryptocurrency is "so hot" right now and because of its anonymity, it is a prime target for hackers and bad actors around the world. From what the banking industry is seeing with P2P activity in relation to Regulation E and the new Interagency Guidance on cybersecurity, the question many bankers are asking is, "Do we want to add cryptocurrency to this dumpster fire?"

The answer: Maybe.

The Interagency Guidance defines a "cybersecurity incident" as one that rises to the level of a "notification incident." A cybersecurity incident is an occurrence that:

(i) Results in actual or potential harm to the confidentiality, integrity, or availability of an information system or the information that the system processes, stores, or transmits; or

(ii) Constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Cryptocurrency: Safe or "Sus"? — Continued on page 28

This new guidance is giving rise to new policies, procedures, and safeguards for banks to have to implement. Ultimately, this is giving time to prepare for the inevitable cybersecurity attack, but this is not without cost to the bank.

Cryptocurrency: Safe or "Sus"?

—Continued from page 27

This new guidance is giving rise to new policies, procedures, and safeguards for banks to have to implement. Ultimately, this is giving time to prepare for the inevitable cybersecurity attack, but this is not without cost to the bank.

The next question is: If a bank takes on servicing cryptocurrency customers, does this increase the risk of a cybersecurity incident?

The answer: Probably.

Ultimately, this will be more of a cost-benefit analysis for the bank. According to a recent CNN article, there were over $1.9 billon worth of cryptocurrency stolen in 2022, so far. According to FinCEN, ransomware attacks are at an all-time high and only continue to increase.

There is an argument that combining the banking with cryptocurrency will only lead to an increase in cyberattacks on banks, which is likely true.

Is it worth it?

The answer: Maybe.

Banks need to have safeguards in place to protect current assets, private information, and to comply with the myriad of new guidance. There is an argument that the infrastructure is already there.

Lastly, several agencies acknowledge the risk associated with servicing cryptocurrency and still push for banks to consider servicing this group.

At the end of the day, a bank is one of the safest places to keep assets, virtually or physically. Therefore, banks may want to consider servicing this group, because banks have specialized in safekeeping throughout their existence.

If they choose not to service this group, they may miss out on a lucrative market opportunity. ◗

Carol Ann Warren, Bankers Alliance

CHIPPEWA VALLEY BANK

IS YOUR BANK SUFFERING UNREALIZED SECURITY PORTFOLIO LOSSES?

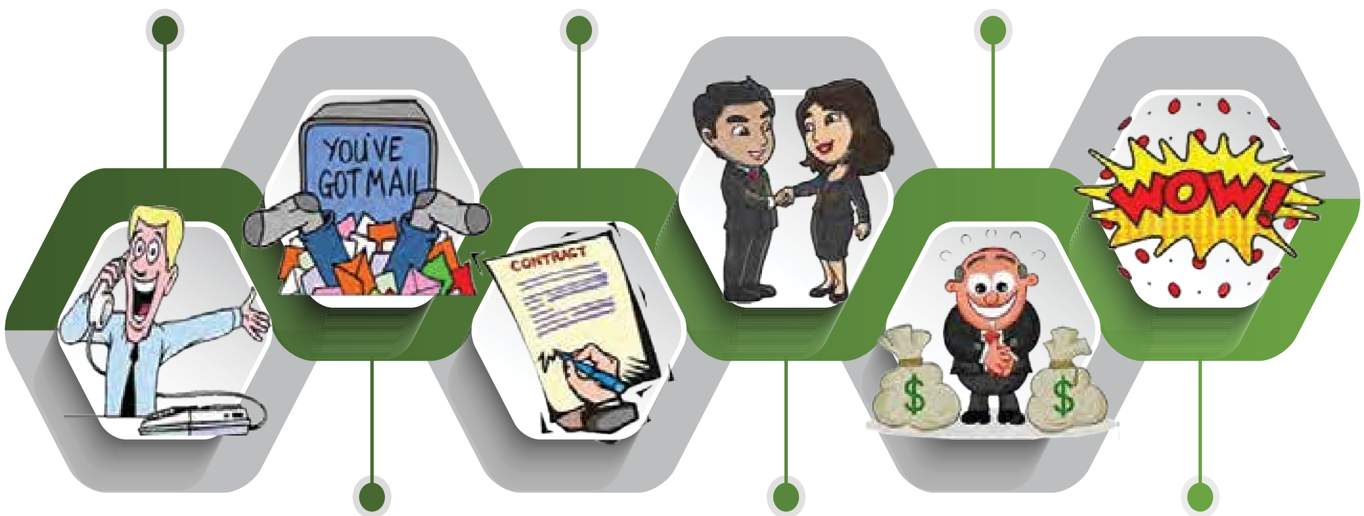
ARE YOU IN NEED OF A CAPITAL INJECTION?

Bank Stock and Bank Holding Company Stock Loans up to $50 Million Done the Simple Way

1.
Calling us is the first step.

3.
CVB preparing the loan documents generally within 5 to 10 days.

5.
CVB wires the funds.



2.
You email us the appropriate documents of information.

4.
Meeting the customer. We will come to you to sign loan documents.

6.
Wow that was easy.

» Call Rick Gerber or Ryan Gerber at 1-866-282-3501 or email

rickg@chippewavalleybank.com
ryang@chippewavalleybank.com

FDIC

EQUAL HOUSING LENDER

JFC ADVISOR NETWORK

EXPERTS AT SUPPORTING FINANCIAL INSTITUTIONS

Incorporate A Successful Investment Program In Your Bank

A Successful Investment Program Can:

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

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

www.jfcadvisor.com

9060 Andermatt Drive, Suite 101
Lincoln, NE 68526

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

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

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

NBA Nebraska Bankers Association

233 South 13th Street, Suite 700
Lincoln, NE 68508

This magazine is designed and published by The newsLINK Group, LLC | 855.747.4003