Nebraska Banker

JANUARY/FEBRUARY 2022

NBA Nebraska Bankers Association

Financial Literacy:
Nebraska's in-school savings banks

OFFICIAL PUBLICATION OF THE NEBRASKA BANKERS ASSOCIATION

CONTENTS

Nebraska Banker
JANUARY/FEBRUARY 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.

Funding Solutions That Meet Changing Times

PMA Funding (PMA) is a leader in providing institutional funding options.
One call gains access to:

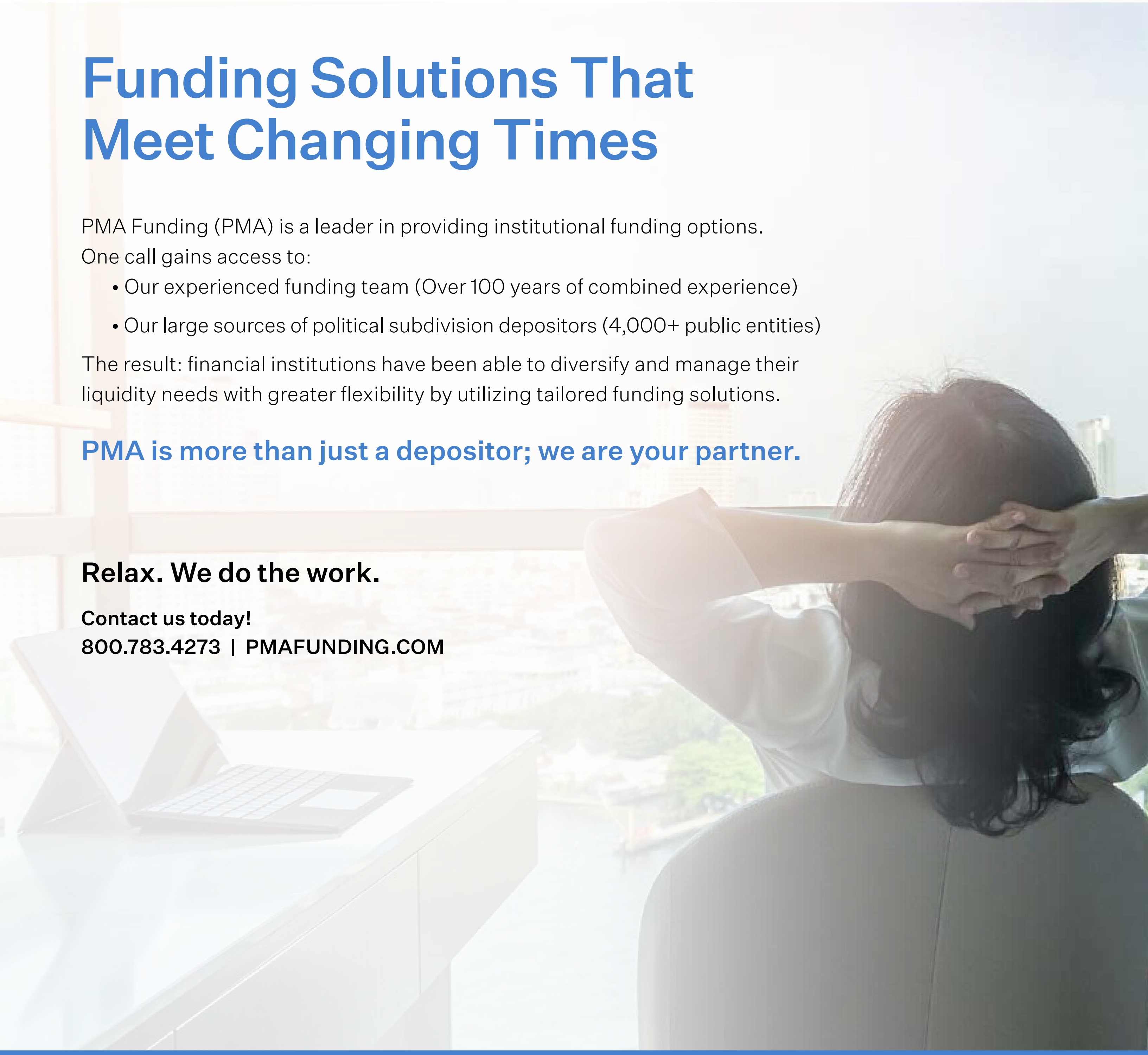
- Our experienced funding team (Over 100 years of combined experience)
- Our large sources of political subdivision depositors (4,000+ public entities)

The result: financial institutions have been able to diversify and manage their liquidity needs with greater flexibility by utilizing tailored funding solutions.

PMA is more than just a depositor; we are your partner.

Relax. We do the work.

Contact us today!
800.783.4273 | PMAFUNDING.COM



NBA BOARD OF DIRECTORS

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

STEPHEN STULL
NBA Chairman-Elect
(402) 792-2500
Farmers State Bank
Dodge

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 BOTHOF
(402) 334-0300
Northwest Bank
Omaha

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

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

KARL GRAMANN
(402) 988-2255
Adams State Bank
Adams

KIM HAMMES
(402) 918-2332
Bank of the West
Omaha

REX HASKELL
(402) 687-2640
First Northeast Bank of Nebraska
Lyons

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

STEVE KUNZMAN
(308) 382-4000
Home Federal Bank
Grand Island

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

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

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

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

SCOTT ZIMBELMAN
(308) 784-2000
Homestead Bank
Cozad

CHRIS HOVE
NBA Past Chairman
(402) 423-2111
Nebraska Bank of Commerce
Lincoln

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

CHIPPEWA VALLEY BANK

IS BORROWING MONEY MORE COMPLICATED AND DIFFICULT THAN IT NEEDS TO BE?

Bank Stock and Bank Holding Company Stock Loans Done the Simple Way

Bank mergers, acquisition loans and refinances up to $50 million

✓ Approval typically within 2 to 3 days and sometimes immediately
✓ In many cases the loan can be started, closed and funded in less than 2 weeks
✓ No Correspondent Bank Account relationship required
✓ If the Federal Reserve approves it we can likely get the deal done for you
✓ Standard Commercial Loan Documentation used in most cases
✓ We won't restrict you to unnecessary covenants
✓ Limited or no reporting requirements
✓ Limited or no origination costs
✓ Low interest rates
✓ Principal payments often determined with the borrower's input on a year by year basis
✓ In many circumstances we accept bank capital growth instead of loan principal reduction
✓ We will come to you! Most loans initiated and closed at the borrower's home or office.

Deal directly with lender/owner who is a CPA and understands the banking industry. We have 35 years of industry experience and can make your job far less stressful and time consuming. We understand transactions.

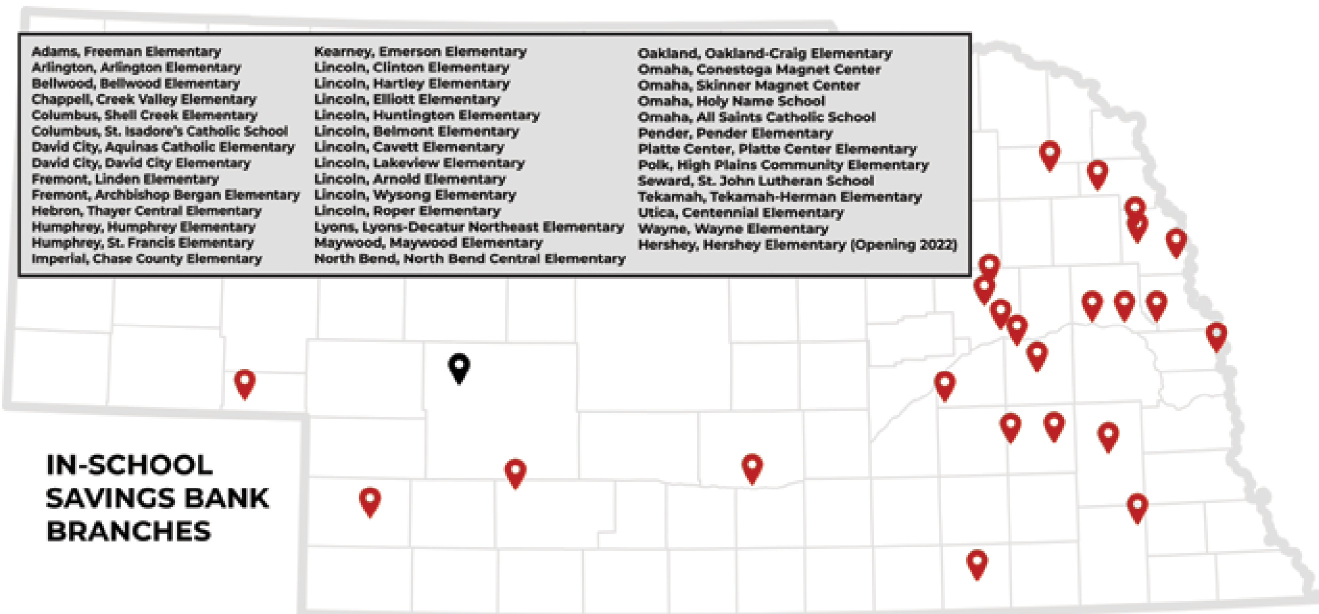
Our belief is to make the loan and stay out of the banker's way and let you do your job.

Call Ryan Gerber or Rick Gerber at 1.866.282.3501 or email ryang@chippewavalleybank.com or rickg@chippewavalleybank.com

Financial Literacy:

Nebraska's in-school savings banks

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



SINCE ARRIVING AT THE NBA IN 2014, I HAVE WORKED CLOSELY with the NBA Board of Directors and member banks to encourage and promote financial literacy. One fun, proven financial education strategy embraced by a growing number of NBA members is the creation and operation of in-school savings banks.

Nebraska's first in-school savings bank opened in 2002 at the Conestoga Magnet School in Omaha. Today, 19 NBA member banks operate 34 in-school bank branches. At the beginning of this year, Nebraska banks and credit unions operated 36 in-school savings banks. The NBA's internal goal is for members to commit to 22 new in-school bank branches in 2022.

In-school savings banks are deposit-only bank branches located inside elementary schools. They offer a fun, real-world experience and help students establish and reinforce a savings habit. Banks, local schools, the Nebraska Council on Economic Education and the Nebraska Department of Banking and Finance are partners in creating the in-school savings banks.

The branch is open one day a week to accept student deposits. Student tellers, trained by the partnering financial institution, staff the branch alongside a representative from the bank. In lieu of earning interest on their deposits, students receive incentive prizes. Free shirts, pencils and other promotional materials branded with the school bank and school logo, for instance, are greatly coveted. The school has a non-interest-bearing custodial account with the partner financial institution to serve as the main account for all student deposits. Students receive their savings balance, in the form of a check, when they move or graduate from the school.

The in-school bank branches not only educate students and increase their savings rates but also build positive relationships with their local bank. They also help to increase parental understanding and involvement in the financial system. The in-school branches have proven especially invaluable in higher-poverty schools.

As a result of the COVID-19 pandemic, the importance of financial education has become increasingly clear. Currently, more than one-half of Americans cannot afford a $400 emergency expense. Similarly, one-third of Americans report having little to no savings for retirement. In addition, a growing student loan debt crisis is financially suffocating the next generation, resulting in less purchasing, investment and savings power for Millennials and Generation Z.

Research conducted by Jennifer Davidson, president of the Nebraska Council on Economic Education and an assistant professor at the University of Nebraska-Lincoln, found that students who participate in an in-school savings bank are much more likely to be banked as adults. In addition, student participants are also much more likely to be employed after high school. These students also make smarter choices about debt and student loans.

Davidson's research also found that financial institutions partners' primary motivation for participation was to provide an opportunity for students to improve their financial literacy and support the community they serve. The research also indicated that financial institution partners believed the program is well worth the cost.

An informal survey of NBA members who sponsor in-school savings banks also found high levels of satisfaction with the program. One NBA member described their in-school branches as one of the bank's most cost-effective marketing, promotion, workforce recruitment and community reinvestment activity!

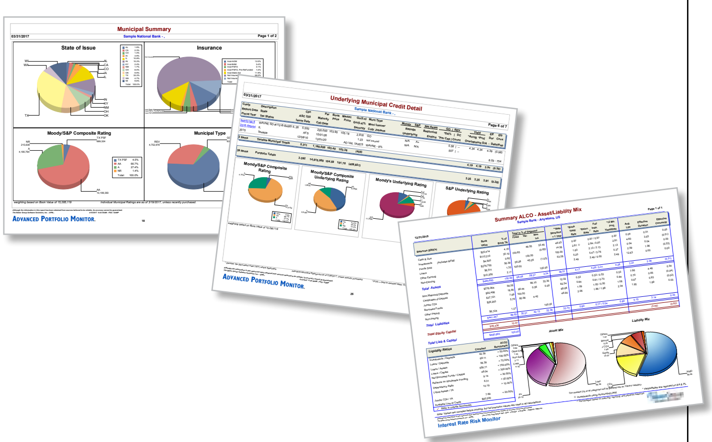
If you are interested in learning more about how your bank may benefit from an in-school savings bank, reach out to Kara Heideman (kara.heideman@nebankers.org) at the NBA or Dr. Jennifer Davidson at the Nebraska Council on Economic Education (jdavidson2@unl.edu).

Today, 19 NBA member banks operate 34 in-school bank branches. At the beginning of this year, Nebraska banks and credit unions operated 36 in-school savings banks. The NBA's internal goal is for members to commit to 22 new in-school bank branches in 2022.

Six-Month Free Trial

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

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



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

Baker's Software Solutions Service Package Includes:

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

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

Bond Accounting – Baker Bond Accounting® (BBA)

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

Investment Analysis – Advanced Portfolio Monitor (APM®)

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

The BakerGroup

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

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

WASHINGTON UPDATE

Cryptocurrencies:

Unlocking Banking's "New Frontier"

Rob Nichols, President and CEO, American Bankers Association

IN CASE YOU HAVEN'T NOTICED, CRYPTOCURRENCIES ARE AN increasingly hot topic of conversation in this country.

According to a Pew Research Center survey fielded in November, 86% of Americans said they have heard about cryptocurrencies, and 16% said they have invested in, traded or used them. Cryptocurrency use is growing particularly rapidly among younger Americans, with 31% between 18 and 29 telling Pew they have participated in crypto transactions.

More often than not, these trades are happening through financial intermediaries — and consumers are increasingly turning to banks to hold these digital assets. In fact, I've heard from a growing number of bank leaders that their customers want to buy, hold and use crypto — and they want to do it through their banks.

Banks have already begun making inroads into the crypto services business — offering a responsible pathway for consumers to adopt these novel financial products. For example, Vast Bank, a community institution based in Oklahoma, recently launched a crypto custody account that bank customers can manage in their app alongside their FDIC-insured dollar account. Or Quontic Bank, which offers a checking product that provides rewards in bitcoin, offering consumers an opportunity to wade into the crypto space without buying it themselves. Large custody banks — such as the Bank of New York Mellon and Northern Trust — are also developing custody services for crypto.

Bank customers know they can rely on their banks to steward their finances and keep their financial data safe. A recent Morning Consult poll highlighted that banks are the most trusted among all financial services providers. Given that, it's no surprise that consumers want to receive cryptocurrency services from their bank. But don't just take my word for it: a survey from NYDIG, a bitcoin services firm, confirmed that a whopping 81% of bitcoin holders would shift

Bank customers know they can rely on their banks to steward their finances and keep their financial data safe. A recent Morning Consult poll highlighted that banks are the most trusted among all financial services providers. Given that, it's no surprise that consumers want to receive cryptocurrency services from their bank.

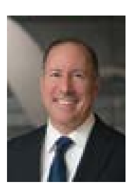
their bitcoin to a bank if it offered secure bitcoin storage. Undoubtedly, this "new frontier" of cryptocurrency represents a huge opportunity for banks.

But for banks to successfully navigate this new frontier, the bank regulatory architecture needs to catch up – quickly. More clarity is needed from the banking agencies about how banks can offer these services in a safe and sound manner. Without this clarity, the unlevel playing field between banks and the rapidly growing cadre of firms seeking to operate as banks while evading the full scope of bank regulations will continue.

There have been some positive developments, with the OCC issuing an interpretive letter clarifying its approach for approving crypto-related activities for national banks. Additionally, a report by the President's Working Group on Financial Markets highlighted the risks of stablecoins, recommending they be issued by insured depository institutions subject to consolidated supervision. Any providers of custodial wallets should also be subject to appropriate federal oversight.

For our part, ABA is taking a deep dive into what we can do to support banks' participation in crypto and other digital assets through both our advocacy and technology partnerships. Additionally, in December, we invested in NYDIG, a leading provider of bitcoin services for banks. This investment will support banks' ability to meet customer demand in this rapidly evolving market so that as we unlock this "new frontier" of cryptocurrencies and digital assets, consumers can continue to place their trust in America's banks to meet their financial needs.

We understand that expanding into cryptocurrency products and solutions won't be for every bank, and that's okay. We firmly stand with banks in their right to decide what products they will offer according to their own judgment and market strategy. However, even with mixed opinions on the value of cryptocurrency as an asset class or as a basis for a product set, ABA strongly believes banks should have access to the tools, partners and regulatory frameworks that allow them to meet their customers' needs.



Email Rob Nichols at rnichols@aba.com.

Employee Data Theft in the Age of FDIC Compliant Investigations

Robert Kardell, Baird Holm, LLP

EMPLOYEE THEFT OF CUSTOMER DATA IS ALWAYS A CONCERN and has become even more so as information can be condensed to digital assets, which are easily moved, copied, or downloaded. The issue can be especially troublesome for banks because of confidential customer data. The information is often easily identifiable to the customer and can include common data such as addresses, email addresses, and telephone numbers, but also often includes sensitive information such as social security numbers, bank account information, dates of birth, and credit card information.

Banks often provide commissions to loan officers to compensate for the closings of mortgage, business, or agricultural loans. Because of the compensation structure, commissioned sales officers may believe the customers and their sensitive information belong to them rather than the bank for which they work. Sales officers may even attempt to take customer information with them when they leave one bank and seek employment elsewhere.

Taking such information may lead to violations of non-compete or non-disclosure agreements. But the taking of such sensitive information may also cause violations of the Gramm-Leach-Bliley Act and even state data breach notification statutes that protect such personal information and may require customer notification. [1]

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act ("GLBA") protects information that a customer gives to a bank, or an employee of a bank, to obtain a product or service. The act defines sensitive information as follows:

> Nonpublic personal information: "Nonpublic personal information" generally is any information that is not publicly available and that:
>
> - A consumer provides to a financial institution to obtain a financial product or service from the institution;
> - Results from a transaction between the consumer and the institution involving a financial product or service; or
> - A financial institution otherwise obtains about a consumer in connection with providing a financial product or service. [2]

However, this language is very broad and could apply to almost any information provided by a customer to a bank for a product or service.

The regulations, thankfully, are more specific:

> [S]ensitive customer information means a customer's name, address, or telephone number, in conjunction with

the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name or password or password and account number.[3]

In combination with account numbers, social security numbers, a driver's license number, and other information commonly collected by banks, the demographic information is "sensitive customer information" under GLBA. This sensitive information is not uncommon on internal sales or customer lists.

Once that information is in possession of the bank, the bank has an affirmative obligation to:

1. Ensure the security and confidentiality of customer information;
2. Protect against any anticipated threats or hazards to the security or integrity of such information;
3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer; and
4. Ensure the proper disposal of customer information and consumer information.[4]

And when the security or confidentiality of customer information is not protected:

When an incident of unauthorized access to sensitive customer information involves customer information systems maintained by an institution's service provider, it is the Financial Institution's responsibility to notify its customers and regulator.[5]

And the regulations state:

Where an incident of unauthorized access to customer information involves customer information systems maintained by an institution's service providers, it is the financial institution's responsibility to notify the institution's customers and regulator.[6]

When an incident of unauthorized access to customer information is discovered — such as when an employee may download, save, print, email, or otherwise copy customer data to take with them to a new financial institution or to start a new business — the bank may have a duty to report this data breach to its regulator, law enforcement, and its customers. While no bank wishes to notify its customers of a breach, there may be options, such as using the threat of providing notification to regulators or law enforcement to elicit the former employee's cooperation in an investigation to determine the risk of harm.

The regulations require an investigation to occur:

When a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused.[7]

The question then becomes, "What is a 'reasonable investigation' for the bank to determine the likelihood of harm?"

Reasonable Investigation

First, the bank must have a "Response Program" "appropriate to the size and complexity of the institution and the nature and scope of its activities, designed to address incidents of unauthorized access to customer information."[8] At a minimum, a response program should include:

1. Assessing the nature and scope of an incident and identifying what customer information systems and types of customer information have been accessed or misused;
2. Notifying its primary federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined later in the final guidance;
3. Immediately notifying law enforcement in situations involving federal criminal violations requiring immediate attention;
4. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, such as by monitoring, freezing, or closing affected accounts while preserving records and other evidence; and
5. Notifying customers when warranted.[9]

The provisions concerning the response program appear to leave little room for ambivalence as to whether notification needs to be made to federal regulators or law enforcement but do allow a measure of judgment when deciding as to whether to notify customers "when warranted."

The reading of the comments in the Federal Register can provide some further guidance regarding the notification

Counselor's Corner — continued on page 16

Notification to federal regulators should occur when the institution initiates its investigation[10] involving unauthorized access or use.

standard for federal regulators or law enforcement. Notification to federal regulators should occur when the institution initiates its investigation[10] involving unauthorized access or use.

But is the "unauthorized access or use" defined by law or an employment contract?

"Unauthorized access or use" is discussed extensively under the customer notice requirements. The guidance states:

> Under the Security Guidelines, the proposed Guidance explained that an institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to a customer. Substantial harm or inconvenience is most likely to result from improper access to sensitive customer information. This type of information is most likely to be misused, as in the commission of identity theft.[11]

> The guidance then suggests that the definition of "unauthorized access or use" is related to the commission of crimes such as identity theft. Unauthorized access or use then is not defined by the employment contract. Furthermore, a properly conducted, well-planned investigation may allow the bank to determine whether there was an intent for an illegal purpose or if taking the data is a contractual issue that does not warrant notification to the federal regulators, law enforcement, or customers.

Conducting the Investigation

Conducting a well-planned investigation while leveraging the notification requirements under GLBA or state statutes to regulators, law enforcement, or customers may yield the answers as to the purpose for "unauthorized access or use." Leveraging the threat of notification can be used to force cooperation from an ex-employee and cooperation from their new employer to investigate the incident fully. Suggested steps for the investigation with full cooperation from the ex-employee and the new employer may look something like this:

Former employee:

- Interviewing the former employee to determine where the data was downloaded, emailed, saved, printed, etc., to determine what possible accesses others may have had to the data or whether there is a threat to the data.
  - If the ex-employee admits to downloading the data:
    - Ask the employee for access to the devices;
    - Hire a computer forensics expert to review any devices of the former employee on which the data had resided to determine the security of the data; and
    - Hire a computer forensics expert to ensure the data is securely wiped from the devices on which the information had been located.
- Ask the former employee to sign an affidavit attesting to the fact that the information was downloaded, the locations of the download, anyone who had access download location (e.g., if downloaded to a phone, who else has access to the phone), and that all other copies of the data have been destroyed.

New Employer:

- Consider interviewing representatives of the new employer to determine whether the data was transferred to or saved on the new employer's network.
- If the data is not on the network, consider asking for an affidavit or a letter from the organization stating so.
- If the new employer has the data on their network,

- Consider asking for a computer forensics expert to wipe the data; or
- Consider asking for an affidavit that the data has been securely wiped from the network device.

The above steps, if well documented, may allow a bank to reasonably conclude that the information has been secured and was not accessed or used for any illegal purpose, such as for opening credit cards or obtaining a new line of credit and meet the requirements of an investigation under the FDIC guidance.

Conclusion

Financial institutions are in a unique position to possess sensitive and personal information of customers. That information must be protected from hackers and employees seeking to email, download, copy, or otherwise remove the information from the bank's possession.

The regulations and notification requirements allow a bank to investigate whether the access and use will require notification. The threat of notification of regulators and law enforcement may provide leverage for the cooperation and interview of former employees. The interviews, the investigation, and the resulting affidavits and reports may provide the evidence necessary for a bank to conclude the actions of the employee; while a violation of an employee agreement is not grounds for data breach notification required under GLBA.

For more information, please contact Robert (Bob) Kardell, at 402.636.8313, bkardell@bairdholm.com, or visit bairdholm.com.

[1] Although state data breach notification laws may apply, this article will limit the discussion to the applicability of GLBA, the definition of sensitive data under GLBA, and the investigation standards under GLBA. This article will also not address the notification requirements under GLBA or applicable state statute.
[2] 15 USC § 6809(4)
[3] 2 CFR Appendix B to Part 364
[4] 12 CFR Appendix B to Part 364 - Interagency Guidelines Establishing Information Security Standards
[5] Financial Institution Letter, FIL-27-2005, April 1, 2005, https://www.fdic.gov/news/financial-institution-letters/2005/fil2705.html
[6] Supplement A to Appendix B to Part 364 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
[7] Supplement A to Appendix B to Part 364 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice.
[8] Federal Register, Vol. 70, No. 59, Tuesday, March 29, 2005, Rules and Regulations, page 15739.
[9] Federal Register, Vol. 70, No. 59, Tuesday, March 29, 2005, Rules and Regulations, page 15741.
[10] Federal Register, Vol. 70, No. 59, Tuesday, March 29, 2005, Rules and Regulations, page 15741.
[11] Federal Register, Vol. 70, No. 59, Tuesday, March 29, 2005, Rules and Regulations, page 15744 (emphasis added).

Ransomware Guides and How to Use Them

Lynda Hartup, Senior Information Security Consultant, SBS CyberSecurity, LLC

RANSOMWARE cyberattacks are one of the fastest-growing attack methods globally, causing many organizations to ask themselves a critical question. Have we done enough to secure our institution against a ransomware attack?

Ransomware readiness is crucial in today's cyber climate, but evaluating the processes and controls you have in place to prevent, recover from, and mitigate the effects of a ransomware attack can seem like a daunting task. Pair that with the abundance of ransomware readiness guidance available, and formulating a plan to assess your institution can make most of us want to turn around and go home.

If you want to assess your institution's ransomware readiness and aren't sure where to start, or maybe you've reviewed some of these sources already and are confused about which one to put your time into, don't panic! We will review several references to help get you started.

In October 2020, the Conference of State Bank Supervisors released their Ransomware Self-Assessment Tool (R-SAT). The R-SAT was developed to help financial institutions assess their risk for ransomware and identify any gaps in their ransomware protection program. It was also designed to give executive management and the board of directors an overview of an institution's preparedness in the event of a ransomware attack.

Then, in December 2020, SBS CyberSecurity released Top Six Controls to Mitigate a Ransomware Attack. This resource lists specific controls that can be put in place to protect your institution's network and data from a ransomware attack.

Fast forward a year later, in August 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released a fact sheet titled, "Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches." This fact sheet provides information on preventing and responding to ransomware-caused data breaches.

Let's dig into each of these resources to see how using them together can help you build a strong ransomware protection program.

Who is the audience for each guide?

Right off the bat, the R-SAT lets you know its audience. From executives to directors, the R-SAT promotes valuable insight into an institution's preparedness. For example, it can be used by an information security officer (ISO) to:

- Assess readiness
- Report on programs
- Identify gaps

Tech Talk– continued on page 20

Tech Talk— continued from page 19

Though the R-SAT can be used as a guide for mitigating gaps within protection programs, it's also important to look elsewhere for additional guidance on best practices.

The CISA fact sheet provides information on preventing and responding to ransomware-caused data breaches. It is not an assessment or reporting tool but a general guide for building baseline best practices. ISOs and IT Managers, or anyone responsible for implementing and developing policies, would benefit from reviewing this.

The SBS CyberSecurity document is another fundamental guidebook, as it proves to be the most technical and granular of the three tools. It lists specific controls you can implement, along with an Incident Response Playbook on how to handle ransomware if you are attacked. Your in-house or outsourced network administrator would be responsible for implementing the controls in this guide.

What is in each guide?

The R-SAT addresses areas of ransomware risk utilizing the functions of the National Institute of Standards and Technology (NIST) Cybersecurity Framework; identify, protect, detect, respond, and recover. To assist in the reporting and reviewing process, it has a series of mostly yes or no questions and checklists for various controls.

The CISA fact sheet is a high-level guide for preventing, detecting, and responding to ransomware attacks. It lists general controls for prevention and detection, best practices for responding, and many links for more detailed guidance.

The SBS CyberSecurity guidance lists specific, granular controls. Rather than providing an overview of the types of controls that should be in place, it gives you detailed items to improve the security of your program and implement your policies.

That's all great, but which one do I use?

All of them!

To assess and report on your ransomware readiness, start with the R-SAT. It will help you determine:

- Which controls your institution has implemented;
- What policies and procedures you have in place; and
- Any gaps that should be addressed.

Once you have identified the gaps, working through the CISA fact sheet is the next step. As the fact sheet only lists general controls and best practices, while skipping over more detailed controls, it is a great guide to assist in developing policies for your program. It also has many links to more in-depth information for building a robust prevention program, which leads us to step three.

Building a solid prevention program requires more insight than each guidance can give us individually. When used in conjunction, however, the three guides discussed can help you build a robust Ransomware Prevention Program.

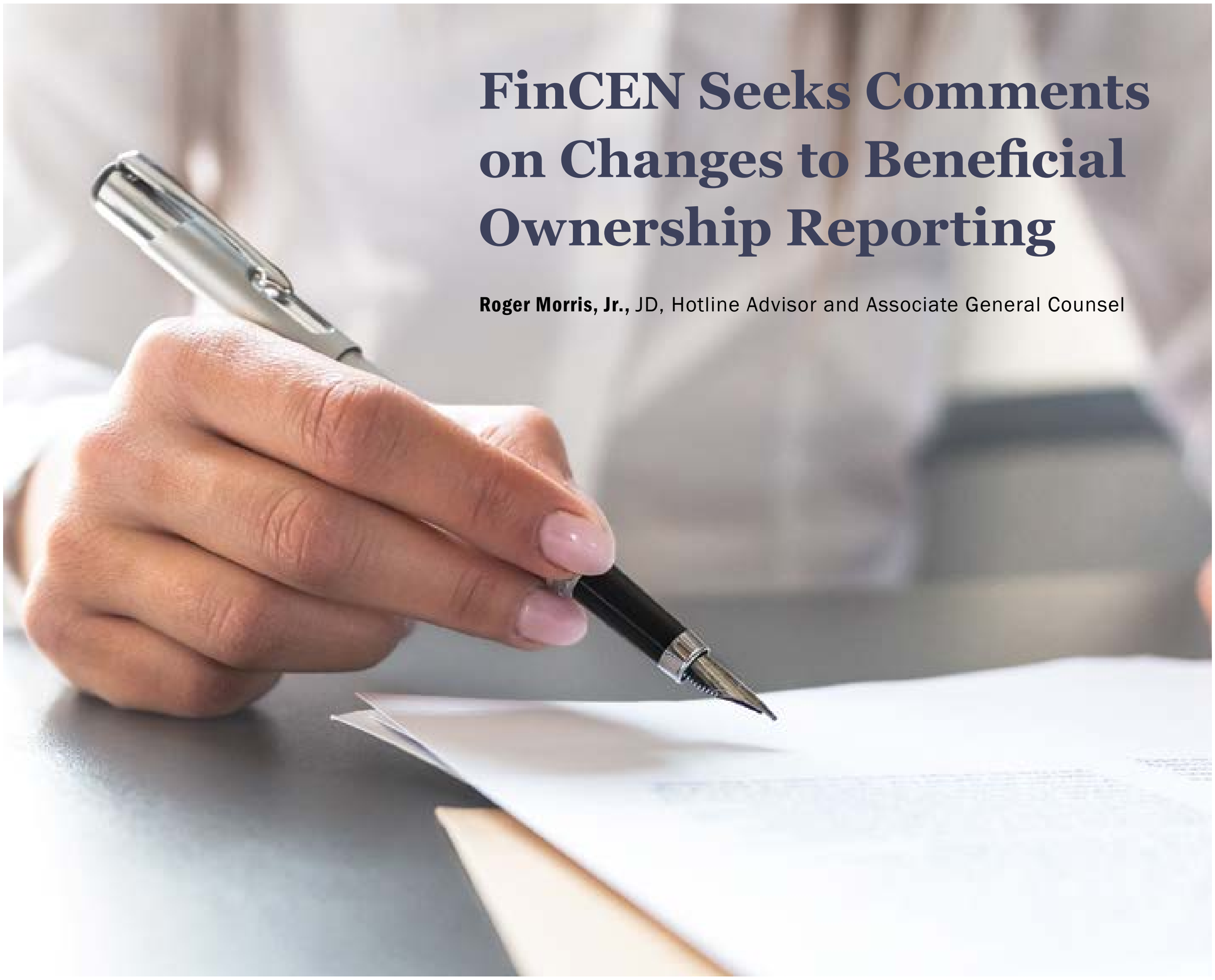
After that, take a look at the SBS CyberSecurity guide, which lists specific practices and controls you can implement. These are not general guidelines but real-world practices to help secure your network and protect your institution. This guide will help you implement the policies you developed from the CISA fact sheet.

Building a solid prevention program requires more insight than each guidance can give us individually. When used in conjunction, however, the three guides discussed can help you build a robust Ransomware Prevention Program. Utilize the three as a step-by-step process:

- **R-SAT** — used to assess the program and identify gaps
- **CISA fact sheet** — assists in building policies and procedures with additional technical guidance provided by embedded links
- **SBS CyberSecurity guide** — provides specific, real-world controls to implement, as well as an Incident Response Playbook

Go forth and protect, my friends! It's dangerous to go alone, so take this guide to help you along your way.

SBS delivers unique, turnkey cybersecurity solutions tailored to each client's needs, including risk management, consulting, auditing, network security, and education. Learn more at sbscyber.com.



FinCEN Seeks Comments on Changes to Beneficial Ownership Reporting

Roger Morris, Jr., JD, Hotline Advisor and Associate General Counsel

IN EARLY DECEMBER, THE U.S. FINANCIAL CRIMES Enforcement Network (FinCEN) issued a Notice of Proposed Rulemaking implementing Section 6403 of the Corporate Transparency Act (CTA), which allowed the public until Feb. 7, 2022, to review and comment on the proposed rules. According to the proposed rulemaking, the ability to operate through legal entities without requiring the identification of beneficial owners is a key risk for the U.S. financial system. Therefore, the CTA seeks to set a clear federal standard for incorporation practices, protect vital U.S. national security interests, protect interstate and foreign commerce, better enable various law enforcement agencies to counter illicit activities and bring the U.S. into compliance with international standards. If enacted, these rules would add a number of government reporting requirements to certain entities, and financial institutions could have access to this information which could possibly ease the burden of customer due diligence.

The purpose of the CTA is to curtail illicit use of the U.S. financial system by forming a centralized government database of beneficial ownership information that certain institutions and the government could access. To create this database, the proposed rules would require certain entities to report specific information about their "beneficial owners," as FinCEN looks to eventually create a beneficial ownership registry. Banks with customer due diligence requirements are very familiar with "beneficial owners" as they are currently required to collect such information at account opening.

FinCEN defines a "beneficial owner" as every individual who, directly or indirectly, through contract, arrangement, understanding, relationship or otherwise, exercises substantial control over the reporting company or owns or controls at least 25% of the ownership interest of the reporting company. The proposed rules set forth three indicators of "substantial control:" (1) service as a senior officer; (2) authority over the appointment or removal of any senior officer or dominant majority of the board of directors (or similar body); and (3) direction, determination, or decision of, or substantial influence over, important matters of a reporting company. The proposed rules also include a catch-all provision clarifying that substantial control can take additional forms not specifically listed.

In addition to the beneficial owner information, the proposed rules require reporting companies to report identifying information about each "company applicant." A "company applicant" is a person who files a document that creates a domestic reporting company or who first registers a foreign reporting company with a secretary of state or similar office in the U.S. Additionally, the proposed definition of a company applicant includes any person who directs or controls such filing by another person.

Any company newly formed or registered on or after the effective date of the regulations must file a report within 14 calendar days from its date of formation or registration. Companies that have been formed or registered prior to the effective date of the regulations are required to file a report within one year from the effective date (the proposed rules shorten this filing deadline from two years in the CTA). Further, companies have an affirmative obligation to update the information they provide to FinCEN within 30 days of any changes in the information. This includes changes with respect to the identity of a beneficial owner, as well as changes to the information reported for any beneficial owner or company applicant.

Collecting this information is intended to help prevent and combat money laundering, terrorist financing, tax fraud and other illicit activity, FinCEN said in its notice of proposed rulemaking. But how will these proposed reporting requirements affect community banks? Under FinCEN's existing regulations, covered financial institutions have the requirement to collect and verify beneficial ownership information from their customers and maintain records of such information. But until now, their customers – including individuals and companies of varying sizes – did not have to report such information to the government. The CTA makes companies subject to such beneficial ownership reporting requirements, and financial institutions will have access to this information. The availability of beneficial owner information to financial institutions with customer due diligence obligations would be practical and useful. For instance, financial institutions could use beneficial owner information for other customer identifications purposes, and reporting companies could pre-approve specific financial institutions that should have access to their information.

Comments on the proposal were due February 7. FinCEN is planning additional rulemakings to implement the CTA, including establishing rules for who may access beneficial ownership information through the database and what safeguards will be put in place to secure and protect the data, and revising the customer due diligence rule to reflect the new beneficial ownership reporting requirements. FinCEN is also in the process of developing the database infrastructure that will house beneficial ownership information. ◗

Roger Morris serves C/A as a Associate General Counsel Roger brings a combination of unique experiences to C/A that he uses to provide guidance on a wide variety of regulatory and compliance issues. Prior to C/A, he worked for one of the largest law firms in the south-central United States based in its Lexington, KY office where he was a member of the firm's Real Estate and Lending Team. In that role he concentrated his practice on commercial lending transactions and the sale, acquisition, leasing, and development of commercial property. Roger also counseled clients on banking law, estate planning, estate and trust administration, and general business matters.

Roger graduated from the University of Kentucky College of Law where he served as Managing Articles Editor of the Kentucky Law Journal, the state's premier law publication. During law school he worked for the Kentucky Personnel Cabinet where he worked on a variety of compliance and policy issues. He also graduated summa cum laude from the University of Kentucky with a Bachelor of Arts in Economics.

The Fed's Balancing Act for 2022

Jeffrey F. Caughron, The Baker Group

ON THE FIRST TRADING DAY OF 2022, THE U.S. 10-YEAR Treasury Note yield jumped above 1.60%, then traded up another 10bps in the two subsequent sessions. That was a 35bps increase in two weeks and aligned with a similar move higher for market measures of inflation expectations. The bond market hadn't seen a worse start to a year since 2009. It seems the market is entering the new year with the same concerns and uncertainty that plagued it for most of 2021, but with greater urgency. We've seen this movie before, though, and it's clear that policymakers and investors alike need to carefully assess the strength and staying power of an inflation environment that's unusual but not so transitory.

Typically, an inflationary impulse arises late in an economic cycle and is driven by an overheated economy where everything is maxed out and hitting on all cylinders, and strong demand is pulling up the general price level. That is not really what is happening now. Instead, we're dealing with "supply shock" inflation, where COVID-induced shutdowns produce bottlenecks and sclerotic trade flows. Dockworkers, truck drivers, processing personnel and other key points in the supply chain are working with reduced staffing and capacity, causing ripple effects throughout the system. So, are rate hikes and a tighter monetary policy the right medicine for "supply shock" inflation as is normally the case with "demand-pull" inflation? Or might a higher cost of borrowing just exacerbate the supply chain disruptions?

Former Treasury Secretary Lawrence Summers recently warned of a trying period for the U.S. economy in coming years with a risk of recession followed by "stagnation." He fears that "we are already reaching a point where it will be challenging to reduce inflation without giving rise to recession." Fed decision-makers are all too aware that if they move too aggressively and inflation really is just a matter of temporary supply chain problems, they run the risk of creating recession to little purpose. The Fed needs to go slow if the inflation trend is truly benign. But if it has deeper, more fundamental roots, too gradual a policy would allow inflationary psychology to become embedded in the economy, risking a wage-price spiral, pushing households and firms to get ahead of assumed cost increases and resort to stockpiling. That's the Summers worst-case scenario: a return to 1979.

There can be no question that the Fed is right to accelerate the "tapering" and stop pumping liquidity into an over-liquified banking system. In their zest to prop up the economy to when COVID was new, they characteristically overdid the job, creating way too much cheap money, distorting financial markets, and fueling asset price bubbles in speculative assets that pose serious risks going forward. The quantitative ease needs to stop. That's the easy part of the Fed's task. The hard part is subsequently determining when and how fast to raise rates.

The flattening yield curve reflects the dangerous waters the Fed must navigate. Short-term yields have risen commensurate with the expectation of multiple rate hikes. All members of the Federal Open Market Committee (FOMC) now see at least one, and some see as many as four hikes in 2022. Longer-term yields, though, have behaved differently. Despite the new year's jump, the 10-year yield remains below its March 2021 high of 1.75%. That may change, of course, but the fact that yields in the long end have moved so slowly up to this point has allowed the yield curve to flatten and belies genuine concern about growth going forward. The Fed is indeed walking a tightrope. Let's hope they're able to keep their balance.

Jeffrey F. Caughron is Chairman of the Board with The Baker Group. He has worked in financial markets and the securities industry since 1985, always with an emphasis on banking, investments and interest rate risk management. You can contact him at 800-937-2257 or jcaughron@GoBaker.com.

EDUCATION CALENDAR

Due to COVID-19, event schedules are subject to change. Please visit nebankers.org/education.html or call the NBA Education Center at 402-474-1555 for the most current event schedule.

MARCH 2022

Supervisor Bootcamp Conference
March 15-16
Lincoln, NE

Tri-State Human Resources Conference
March 29-30
Overland Park, KS

APRIL 2022

Spring Agri-business Conference
April 5-6
Kearney, NE

Cybersecurity Virtual Workshop
April 12
Virtual

Demystifying Cryptocurrency Webinar
April 18
Virtual

MAY 2022

NBA Annual Convention
May 4-6
LaVista, NE

Small Business Lending Virtual Workshop
May 24-25
Virtual

NBA Nebraska Bankers Association

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

Overdraft Overhaul

Katie Harrison, J.D., CRCM Director

OVERDRAFT SERVICES ARE A STANDARD BANKING PRODUCT. Life happens, and thankfully, most banks offer an overdraft product to come to the rescue when you are on vacation and forgot to do a savings transfer, or transpose numbers when balancing your checkbook. The end of 2021 came with a cautionary tale for financial institutions from regulators: Overhaul your overdraft services or potentially face enhanced scrutiny.

History

This is not the first time the Consumer Financial Protection Bureau (CFPB) has conducted research related to overdraft programs. Shortly after its creation in 2011, the CFPB published a semiannual report in 2012 that highlighted the pitfalls and consumer woes related to account maintenance and overdraft programs. The report revealed general consumer challenges with financial services but specifically discussed consumer confusion concerning overdraft programs, alluding to complex parameters.

In recent years, there would be an enforcement action here or there related to overdraft fees. Many of these actions stemmed not from the products themselves but how consumers were sold or enrolled for participation in them. More recently, in 2020, TD Bank was found to be in violation of Regulation E as it related to overdraft fees for ATM and one-time debit card transactions and ordered to pay $112 million in fees.[i] In 2018, Minnesota-based TCF National Bank was in hot water for the same practices and was assessed $28 million in fees.[ii]

Regulator Research

The CFPB conducted research using call report data to determine overdraft and insufficient fees on bank revenue. It primarily looked at two data points:

1. Overdraft/NSF fee reliance since 2015
2. Checking account overdraft at financial institutions served by core processors

The first data point showed institutions with more than $1 billion in assets totaled $11.97 billion collectively in fees in 2019. Overall market revenue for these fees was $15.47 billion in 2019. The apparent problematic statistic for advocacy groups and regulators is that overdraft and nonsufficient funds fees account for about two-thirds of fee revenue for institutions, making banks heavily reliant on this revenue. The second data point looked at core processors and their data for smaller institutions, primarily data for 2014. This research found 92.9% of smaller banks and 60.9% of credit unions had an overdraft program with 13 to 19% lower fees than large banks.[iii]

Research Reactions

On Dec. 1, 2021, CFPB Director Rohit Chopra published prepared comments in conjunction with the published CFPB research. One comment emphasized that instead of being paid (in interest) for banks holding consumers' money, consumers now pay large banks for this privilege, primarily through account service charges like overdraft fees. Chopra went on to liken an overdraft fee to interest paid on a short-term loan, using the example of a consumer being charged a $34 daily fee for a day or two for the bank covering the small negative balance in their deposit account, and how that would equate to an annual percentage rate (APR) of more than 10,000% on a loan.

Chopra also said CFPB bank examiners will prioritize examinations of banks heavily reliant on overdraft fees, likely focusing again on call report data for this determination. “Financial institutions that have a higher share of frequent overdrafters or a higher average fee burden for overdrafting should expect us to be paying them close supervisory attention. Ultimately, we plan to inform institutions on where they stand relative to their peers with overdraft. We believe sharing that information will increase transparency and help against the race to the bottom we have seen in this market.”[iv]

> Ultimately, we plan to inform institutions on where they stand relative to their peers with overdraft.

Industry Response

In response to the CFPB’s claim to enhanced scrutiny into overdraft-related products, multiple large banks have begun slashing overdraft and insufficient fees or have drastically overhauled their overdraft products with more consumer-beneficial features. Here is a quick snapshot of some recent changes at large institutions:

Ally	No more overdraft fees
Bank of America	Overdraft fee reduced from $35 to $10 on debit card purchases with insufficient balances
Capital One	Complete elimination of all overdraft and NSF fees
JP Morgan Chase	No overdraft fee until account overdrawn at least $50; No fees assessed until after a full day to restore overdrawn balances
	Allow access to direct deposit up to two business days early
	No NSF Fees

Cutting fees in these programs may be more of a challenge for smaller institutions that do not have the diversified revenue streams that larger banks have. As your institution reviews its programs and procedures regarding overdraft protection and handling of insufficient funds, bear in mind the consumer protection regulations that may be applicable:

- Regulation B — Equal Credit Opportunity Act
- Regulation E — Electronic Fund Transfer Act
- Regulation V — Fair Credit Reporting Act
- Regulation Z — Truth in Lending Act
- Regulation DD — Truth in Savings Act
- Third-Party Oversight
- Unfair, Deceptive, or Abusive Acts or Practices (UDAAP) .

This article is for general information purposes only and is not to be considered as legal advice. This information was written by qualified, experienced BKD professionals, but applying this information to your particular situation requires careful consideration of your specific facts and circumstances. Consult your BKD advisor or legal counsel before acting on any matter covered in this update.

[i] Consumer Financial Protection Bureau Announces Settlements with TD Bank for Illegal Overdraft Practices, August 20, 2020, https://www.consumerfinance.gov/about-us/newsroom/cfpb-announces-settlement-td-bank-illegal-overdraft-practices/.

[ii] Bureau of Consumer Financial Protection Settles With TCF National Bank, July 20, 2018, https://www.consumerfinance.gov/about-us/newsroom/bureau-consumer-financial-protection-settles-tcf-national-bank/.

[iii] CFPB Research Shows Banks’ Deep Dependence on Overdraft Fees, December 1, 2021, https://www.consumerfinance.gov/about-us/newsroom/cfpb-research-shows-banks-deep-dependence-on-overdraft-fees/.

[iv] Prepared Remarks of CFPB Director Rohit Chopra on the Overdraft Press Call, December 1, 2021, https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-rohit-chopra-overdraft-press-call/

Katie Harrison, J.D., CRCM Director

ONE LAST THING ...

Did you know that you can enjoy your association news anytime, anywhere?

The new online article build-outs allow you to:

- Stay up to date with the latest association news
- Share your favorite articles to social channels
- Email articles to friends or colleagues

There is still a flipping book for those of you who prefer swiping and a downloadable PDF.

Check it out!

Scan the QR code or visit:
nebraska-banker.thenewslinkgroup.org

JFC ADVISOR NETWORK

EXPERTS AT SUPPORTING FINANCIAL INSTITUTIONS

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

Grow A Successful Investment Program In Your Bank

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

PRESORTED
FIRST CLASS MAIL
US POSTAGE
PAID
SALT LAKE CITY, UT
PERMIT NO 508

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