



# Colorado Banker

September/October 2021

Chairman's Message:  
Financial Literacy and Banks:  
**A Job or a Duty?**

Page 4



OVER A CENTURY: BUILDING BETTER BANKS — *Helping Coloradans Realize Dreams*



# Move off manual processes and network shares.

Meet SPARK: A transformational digital solution  
for business lending in your community.

Learn more at [lendwithspark.com](https://lendwithspark.com) →



# Contents

- 2 A Word From CBA: Compliance and Consumer Privacy Nightmare
- 4 Chairman’s Message: Financial Literacy and Banks: A Job or a Duty?
- 6 Feature: Digital Personalization: 33% Say It’s Not Worth the Risk.
- 8 Washington Update: Congressman Blaine Luetkemeyer House Financial Services Committee Update
- 10 What a Small Town Taught Me About Artificial Intelligence
- 12 ATM Technology Growth
- 13 It’s Not Hip To Be Square
- 14 Be in the Know – SBA 504 Refinance
- 16 Strengthening Your Bank’s Defenses Against Ransomware
- 18 The Path to Service Quality and Managing Costs for the Future
- 20 Fed’s Durbin Proposal Creates More Confusion Than Clarity
- 22 The OCC Reconsiders Going It Alone on CRA
- 24 Transfers Are Nonreportable; No Such Thing as Prior-Year Conversion; 12-Month Limit Only for IRA-to-IRA Rollovers
- 26 Colorado Banks and Financial Institutions – State Privacy Law Compliance Obligations
- 29 Automated Clearing House Debit Entry Fraud



# Over a Century

## BUILDING BETTER BANKS—

*Helping Coloradans Realize Dreams*

*Don Childears*  
CEO

*Jenifer Waller*  
President

*Brandon Knudtson*  
Director of Membership

*Lindsay Muniz*  
Director of Education

*Alison Morgan*  
Director of State Government Relations

*Rita Fish*  
Executive Assistant

*Margie Mellenbruch*  
Bookkeeper\*

*Craig A. Umbaugh*  
Counsel\*

*Jim Cole*  
Lobbyist\*

*Melanie Layton*  
Lobbyist\*

*Garin Vorthmann*  
Lobbyist\*

*Andrew Wood*  
Lobbyist\*

\* Outsourced

140 East 19th Avenue, Suite 400  
Denver, Colorado 80203  
voice: 303.825.1575 — fax: 303.825.1585

### Websites:

[coloradobankers.org](http://coloradobankers.org)  
[smallbizlending.org](http://smallbizlending.org)  
[financialinfo.org](http://financialinfo.org)

[colorado-banker.thenewslinkgroup.org](http://colorado-banker.thenewslinkgroup.org)

©2021 The Colorado Bankers Association is proud to present Colorado Banker as a benefit of membership in the association. No member dues were used in the publishing of this news magazine. All publishing costs were borne by advertising sales. Purchase of any products or services from paid advertisements within this magazine are the sole responsibility of the consumer. The statements and opinions expressed herein are those of the individual authors and do not necessarily represent the views of Colorado Banker or its publisher, The newsLINK Group, LLC. Any legal advice should be regarded as general information. It is strongly recommended that one contact an attorney for counsel regarding specific circumstances. Likewise, the appearance of advertisers does not constitute an endorsement of the products or services featured by The newsLINK Group, LLC.

# Compliance and Consumer Privacy Nightmare

By Jenifer Waller, President  
Colorado Bankers Association





“

*The industry has been working on expanding financial services to unbanked individuals.*

*Many of these individuals have a lack of trust in the government.*

**T**he Biden administration’s proposal to use bank account data to combat tax evasion would undoubtedly raise banks’ compliance burden and, even more concerning, would threaten the privacy of bank customers.

The proposal would require financial institutions and other financial services providers to track and submit to the IRS information on the inflows and outflows of every account above a threshold of \$600 during the year, including breakdowns for cash. While the stated goal of this data collection is to uncover tax evasion by wealthy citizens, this proposal misses that mark by targeting everyone.

In addition to the significant privacy concerns, it would create tremendous liability by requiring the collection of financial information for nearly every bank customer without proper explanation of how the IRS will store, protect, and use this enormous trove of personal financial information.

One must question the impact on the unbanked and underbanked. The industry has been working on expanding financial services to unbanked individuals. Many of these individuals have a lack of trust in the government. I must assume the reporting required by the proposal would discourage them from opening a banking account.

Further, the federal government’s history of keeping this type of data secure is dubious at best. The IRS is one of several government systems that has recently experienced a data breach. The concern is the government’s ability to keep financial data secure.

The program would be costly, not fit for the stated purpose, and loaded with unintended and seriously negative consequences. The cost to taxpayers is an estimated \$87 billion over the next 10 years.

The proposal fundamentally changes the nature of the information your bank is required to report on and forces banks to provide the government with information that does not reflect taxable activity. The Treasury Department and IRS have both stated this is a method for them to raise revenue.

We have been successful at blocking the proposal so far, but the Biden administration is being very vocal in their support for the provision, and they will have numerous opportunities to include this provision in the bill.

Bankers, thank you for making your opposition known by contacting members of Congress and alerting your customers to the potential privacy risks. Keep up the good work. 🌐

## Chairman's Message

# Financial Literacy and Banks: A Job or a Duty?

By Mike Brown  
Regional President, Alpine Bank  
2021-2022 CBA Chairman



*What forms has this taken across the banking spectrum? For starters, many banks — big and small — have created their own “classes” for customers and non-customers alike.*

Let me tell you an ugly secret that not even my closest colleagues know about me: before my long career in banking, I was absolutely clueless when it came to my personal finances.

I did not lack for intelligence or drive; during my college years, I maintained pretty solid grades. But when it came to my checking account, unopened bank statements would pile up, along with more than a few overdraft fees.

My budget (and my access to ramen dinners) consisted of whatever a nearby ATM machine told me on a given day. And when it came to borrowing for my last year of college, I didn't know about my interest rate or how my inevitable loan payments would be calculated. I was only concerned about where to sign and when the money would show up.

Now, fast forward more than three decades later. By virtue of lifelong experience — not to mention choosing banking as a career — I came to cure my own lack of financial awareness. But across our country, our state, and our communities, there are many intelligent, hardworking individuals who struggle with financial literacy, including concepts like budgeting, money management, investing and borrowing.

Globally, the United States ranks behind more than a dozen countries when it comes to financial literacy among adults. Nationally, surveys conducted over the past 10 years have consistently shown that well over half of American adults do not understand basic financial terms. The negative effects of this issue may be seen in nationwide problems, such as student loan defaults as well as the lack of retirement planning by the majority of working American adults.

The simple fact is that our society does not formally equip students and adults with everyday financial knowledge. This issue is not confined to a single age, gender, racial or economic group. But many — if not most — of these good folks have one thing in common: They're customers of our banks.

Our industry has come to realize that serving our customers and our communities goes far beyond daily deposit and lending transactions. Financial education has increasingly

come to be recognized as one of our jobs. And many of us have come to view this as an obligation.

What forms has this taken across the banking spectrum? For starters, many banks — big and small — have created their own “classes” for customers and non-customers alike. Common topics range from business financial management to walking first-time homebuyers through the basics of applying for a mortgage loan.

And for many years, banks have worked with their local schools to provide education to students ranging from middle schools to community colleges. To do this, banks have partnered with national and local nonprofits such as Junior Achievement. And as technology advances, our industry has more recently worked with online providers such as EverFi.com, which provides financial education that can be

accessed by students in both classrooms and homes.


In Colorado, the need for financial literacy has been clearly recognized by our industry and our elected leaders. Earlier this year, the Colorado legislature — with vocal support from the Colorado Bankers Association and its members — passed a bill requiring our public high schools to provide financial education to students ranging from freshmen to seniors. Required topics include:

- The costs associated with obtaining a college degree, including how to manage student debt
- Credit cards and credit card debt
- The home buying process, including mortgage debt
- Saving and investing for retirement.

This is a long-overdue means of formally educating our Colorado students as they embark on financial decisions that will impact the rest of

their lives. And the CBA and its many members are proud to have influenced and supported this critical legislation.

But our job is not done. Our industry has a continuing role to play in financial literacy. If you're a banker looking to provide financial education, the CBA can help point your bank to tried-and-true resources that already exist. Don't look at it as one more job ... it's an investment in the success of our customers and our communities.

CBA is a long-term supporter of financial literacy. In 2005, we ran a bill to include financial literacy in education standards. In the most recent legislative session, we worked with a broad coalition to expand financial literacy standards to include the topics of saving for retirement, managing credit cards, student loans, and first-time home buying information. 

## up to 4% down payment assistance



Liz and Miguel, CHFA homeownership customer, Denver

### chfa home finance

Help your homebuying clients reduce upfront costs with one of CHFA's down payment assistance programs. These can even be used to supplement their own down payment contribution. The homebuyers must be using one of the CHFA's first mortgage loan programs to be eligible.

- **Down Payment Assistance Grant:** Up to 3 percent of the first mortgage; no repayment required
- **Second Mortgage Loan:** Up to 4 percent of the first mortgage; repayment required upon the payoff of first mortgage or sale or refinance of the home.

Learn more at [chfainfo.com](http://chfainfo.com).

303.297.chfa (2432)  
[www.chfainfo.com](http://www.chfainfo.com)

With respect to its programs, services, activities, and employment practices, Colorado Housing and Finance Authority does not discriminate on the basis of race, color, religion, sex, age, national origin, disability, or any other protected classification under federal, state, or local law.



financing the places where  
people live and work

# Digital Personalization: 33% Say It's Not Worth the Risk.

By Neal Reynolds, President,  
BankMarketingCenter.com



**T**he pressure on banks to really step up their digital experience game is, as we all know, greater than ever. Branch banking, according to pundits, is probably going away. “Probably” because, honestly, no one really knows, right? It sure looks like it, however.

That being the case, where does that leave banks? With a huge incentive to ramp up their digital experience through personalization.

Also, according to pundits, most banks are offering only the basics in this channel. And why is that? There is no doubt that personalization is a big deal in customer engagement. Having that deep understanding of each customer’s unique needs, driven by data and analytics and aided by machine learning, is every marketer’s dream. That understanding of exactly what a customer is thinking, feeling and needing forms the very bedrock of any solid, strategic marketing effort.

According to the Boston Consulting Group (BCG), “a majority of people who are either open to or actively mulling changing banks would consider banking with a tech company — such as Amazon, Facebook, or Google — if they could. This is not surprising because such companies have spurred a desire for more customized interactions and fostered a willingness to trade data for a better experience.” BCG goes on to say: “Several consumer brands have shown the way forward. Netflix uses personalization techniques to make movie and series recommendations. Yet while many financial institutions are conceptually on board and heavily investing, the Netflix of banking has yet to emerge. The main reason is that true end-to-end personalization requires developing new muscles — such as strong cross-channel offerings, cross-enterprise collaboration,



a single view of the customer, and a new technology ecosystem — all of which are difficult to build.”

Agreed, for the most part. Is receiving a purchase recommendation from Amazon or Netflix the same as getting one from your bank? I'm not convinced. When Netflix tells me that I might be interested in a certain program because it somehow aligns with one I'd watched previously, I have no concerns about data sharing and privacy. The kind of personal data that a bank needs to personalize one's digital experience is far different from the data that Netflix uses to recommend their latest docuseries.

I think it might have been one of those satirical commercials done by Saturday Night Live a while back; I'm not sure. But what I do remember was their lampooning of banks using personal data for marketing purposes. At one point in the faux commercial, which featured a young couple, the man receives a series of SMS messages from their bank. The messages are fairly innocuous at the start but become progressively more disconcerting. The first text seems ordinary enough: “We hope you're enjoying the new truck you purchased with one of our auto loans.” When it's followed shortly afterward by, “We've noticed that you made a large purchase at the grocery store just the other day ... having a party?” The couple gets a bit concerned. By the last message, they're totally creeped out: “We have the loan you need when you're ready to decorate that baby room. Congratulations.” The gag, of course, is that the couple doesn't know they're pregnant, yet their bank somehow does.

Granted, this is a bit of hyperbole, but it does point to the fact that monetizing consumer data can pretty quickly run afoul of the consumer's desire for privacy. Consumers want the convenience of products and services being brought to their attention based on their “buyer journey” and purchasing habits. Still, they're definitely conflicted about how much of their personal information is needed to make that happen.

A Cognizant (<https://www.cognizant.com/whitepapers/putting-the-experience-in-digital-customer-experience-codex1180.pdf>) white paper on the subject states when it comes to digital experiences, “critical customer interfaces should be reexamined in an era when Starwood Hotels allows you to check in and open the door to your room with your SmartPhone. Without making sound decisions over the coming months, many may be left struggling to catch up to digital winners.”

Again, can a bank's digital experience be equated with the ability to open a hotel room door without “hassling” with a key? What if you received a text or email from your bank saying: “Your oldest daughter is nearly 28 years old. Shouldn't she be getting married soon? Maybe you should consider one of our HELOCs for that reception.” Or, better still, “Is everything okay at home? Over the past two weeks, you've spent \$187.50 at the liquor store.”

So, are banks “way behind” companies like Netflix and Amazon in offering a personalized experience? I'm not sure that we're comparing apples to apples here. Yes, banks do need to do a better job of anticipating customer needs and engaging them across all channels with “the right message at the right time,” but it does make sense that they tread lightly here. Research from Epsilon indicates that a substantial percentage of consumers want and expect personalization:

- 90% of consumers feel that personalization is “very/somewhat” appealing.
- 80% of consumers are more likely to do business with a company that offers personalized experiences.

However, the research indicates this as well: “Despite consumers' growing comfort with (and demand for) personalized interactions, a significant percentage of consumers are still protective of their personal information.” Twenty-five percent of consumers see getting personalized offers as “creepy,” and 32% say that getting personalized experiences is not worth giving up their privacy. More than one-third (36%) feel that companies don't do enough to protect their private information.

BCG estimates that for every \$100 billion in assets that a bank has, it can achieve as much as \$300 million in revenue growth by personalizing its customer interactions. Moving forward, the lion's share of that interaction will be digital. Banks will certainly appreciate the \$300 million in revenue growth, but they're smart to take a thoughtful approach to try to be the next “Netflix bank.” After all, isn't personalization about listening to, understanding, and responding to the wants and needs of customers? Those who are listening are, in my opinion, being justifiably cautious. 🍷

*About Bank Marketing Center*

*Here at BankMarketingCenter.com, our goal is to help you with vital, topical, and compelling communication with customers and messaging to help you build trust, relationships, and revenue. Visit [bankmarketingcenter.com](http://bankmarketingcenter.com), or by phone at 678-528-6688, or email [nreynolds@bankmarketingcenter.com](mailto:nreynolds@bankmarketingcenter.com).*



## Congressman Blaine Luetkemeyer House Financial Services Committee Update

**R**ecently, the House Financial Services Committee held a hearing entitled “A Biased, Broken System: Examining Proposals to Overhaul Credit Reporting to Achieve Equity.” Committee Chairwoman Maxine Waters called for this creatively named hearing to gain support for legislation to create a government-run credit bureau within the Consumer Financial Protection Bureau.

Bankers in Colorado understand the value of accurate credit reporting. It is how risk is assessed and interest rates are determined. Incomplete or inaccurate credit reports force banks to either deny loans or raise the cost of credit. As one of the few members of Congress with a banking background — I started my career as a bank examiner then spent over 30 years in the banking and insurance industries — I often find myself explaining these very basic facts to some of my colleagues on the Financial Services Committee, particularly those who believe government control over credit reporting is a good idea.

The bills discussed at the hearing would quite literally give the CFPB the power to determine who is creditworthy in the U.S. by giving the Bureau the authority to decide which portions and how much of a person’s credit history

is made available to banks when considering a loan application. Proponents of these bills believe this new, centralized credit bureau would benefit disadvantaged communities that struggle with access to credit. They believe the current system unfairly punishes certain people based on factors out of their control. While we all likely have ideas on how to improve the current credit reporting system, this solution would only exacerbate the problem. Misreporting credit history or limiting available information raises the cost of credit across the board, but particularly for low-income communities — the people reading this know-how to assess and price risk. It takes information, and when that information is limited or altered, you have no choice but to assume additional risk. Not only will that raise costs for low-income borrowers, but it will also eliminate access for some altogether, which is bad for consumers, the banks, and the surrounding communities.

Eighteen months ago, the American economy was ground to a halt. Businesses were shuttered, people were forced to stay at home, and everyone was left to wonder what’s next. When the American People looked to the government for a solution, the government turned to the banks. Through PPP and other rescue programs, banks

facilitated the movement of trillions of dollars and were the key factor in their survival for many businesses. Despite the fact that we continue to grapple with loan forgiveness and workforce participation remains low (also thanks to the government), the economy is improving. That wouldn't be possible without the banks.

While there are plenty of bad ideas floating around in Congress — looking no further than the proposed CFPB credit bureau — there are also efforts to work with the private sector to keep the momentum going. As the Ranking Member of the House Small Business Committee, I'm pushing on the Small Business Administration to improve the forgiveness process and get their other programs in order. I also just recently introduced a bill to replace the single director position at the CFPB with a five-person bipartisan commission. The Bureau is constantly being used as a political football, and its director wields so much power that the Supreme Court grappled with whether the position was even constitutional. Allowing one person to hold such unchecked power over our economy is irresponsible and verges on negligence. My bill would provide increased accountability and transparency so

the American people can trust the CFPB to do its job without political motivation.

If you take one thing away from this column, I hope it is this: banks' participation in our economy and our government is critical. As you can likely tell, my beliefs differ wildly from some of my colleagues, which illustrates the need for private sector input. Banks are often the first to see economic winds changing. You likely know what programs work and don't work before lawmakers. So, whether it's to elected representatives or even your regulator, please speak up. You know your business better than anyone else and will be your customers' and community's best advocate. Our economy and our government depend on a strong financial system. 🌐



*Republican Blaine Luetkemeyer represents Missouri's 3rd District in the U.S. House of Representatives. He serves on the House Financial Services Committee as Ranking Member of the Subcommittee on Consumer Protection and Financial Institutions as well as the Ranking Member of the House Small Business Committee.*

# SBA 504

WE MAKE IT EASY

LET OUR TEAM HELP  
YOU SECURE THE  
DEAL AND LOWER  
YOUR RISK

- UP TO 90% OVERALL FINANCING
- UP TO 25 YEAR TERM
- FIXED-RATE

Leveraged financing and refinancing of owner occupied real estate and long-term equipment. Most for-profit small businesses eligible.



SBA defines businesses with net profit after tax <\$5.0 Million and tangible net worth <\$15.0 Million as small.

[PREFERREDLENDINGPARTNERS.COM](https://www.pREFERREDLENDINGPARTNERS.COM) | 303.861.4100

# What a Small Town Taught Me About Artificial Intelligence

By Neal Reynolds, President,  
BankMarketingCenter.com



**A**s a community bank, nothing is more important to your success than understanding your customers and delivering value. What's different today? There was a time when understanding your customer's needs and overall financial behavior was, well, easy. Unfortunately, that's simply not the case anymore.

For a long time, community bankers achieved this customer insight by interaction. If you're old enough to be reading this and grew up in a small town, I'm sure you remember. I do because that's how I grew up.

You've seen "It's a Wonderful Life," right? Remember when Potter questions the loan that George has approved for Ernie, the cab driver? "I can vouch for his character," George tells Potter. Having grown up in a small town, not terribly unlike Bedford Falls, I had a very similar experience myself, many of them, in fact. When I was ready for my first car loan at age 18, Mr. Jepson, the kind gentleman who ran our local community bank, didn't need me to fill out a loan application, survive a host of credit checks, or have a bunch of agencies confirm that I wasn't a criminal. He knew my parents, my grandparents, and all

my family. He knew I had a steady job at the IGA grocery store, was headed off to college and was in church on Sundays and Wednesday nights; he knew all about me.

Those days are gone. Vouching for someone's character just isn't an option anymore. With online and mobile options, customers no longer walk into their local branch and do all their banking there. The insights that bankers need, that they used to get through interaction, are tough to get. Instead of that personal cooperation to gain those insights and act upon them, bankers now rely on Data, Artificial Intelligence (AI) and Machine Learning (ML) technologies.

This past January, Business Insider talked about the tremendous impact that AI can have on a bank's customer experience. "Banks can use AI to transform the customer experience by enabling frictionless, 24/7 customer service interactions." The Insider goes on to say that banks can, and are, "using AI to deepen customer relationships, and provide personalized insights and recommendations." Thus, artificial intelligence is now gathering and analyzing the data that a banker's "real" intelligence once gathered and analyzed in order to know the customer. Today,

without personal interaction, that customer is a “persona,” an AI/ML-generated individual who can be used to predict behavior and personalize an experience.

Creating personas is nothing new and, unfortunately, in a pre-AI/ML world, have been developed using assumptions and/or simply on past actions such as purchases. The drilled-down insights that AI/ML provides can help bankers develop a far more accurate picture of their customer’s identities and behaviors. In the article, 10 Ways AI Can Improve Digital Transformation’s Success Rate, Forbes states, “using AI to better understand customers, personas need to be the foundation of any digital transformation initiative. The most advanced uses of AI for persona development combine brand, event and product preferences, location data, content viewed, transaction histories, and, most of all, channel, and communication preferences.” In short, you not only know the “what” about your customer, but the “when, where, why, and how,” as well.

Despite its necessity, the implementation of these technologies in banking is still something that most banks are “planning for.” Why has this transformation in customer data management taken so long? The legacy data solutions so pervasive in today’s banking industry

cannot be transformed quickly, easily or inexpensively. As a result, a growing number of community banks have looked to multiple core and edge systems for gathering, analyzing and reporting. The integration of these systems, though, is time-consuming and costly. So time-consuming, in fact, that it’s quite possible the data gathered can be obsolete by the time the integration is complete.

Through these advanced consumer profiles and AI/ML’s predictive analytics, you’re far better equipped to reach the right customer in the right place at the right time with the right message. It’s almost a return to those Bedford Falls days when you knew the cab driver well enough to approve a loan application based on knowing his character, but not quite. Unfortunately, “personalization” through technology will never be the same as personalization through personal interaction. But, this is the world in which we now live. 🌐



To view campaigns, visit [bankmarketingcenter.com](http://bankmarketingcenter.com). Or, you can contact Mr. Reynolds directly by phone at 678-528-6688 or email at [nreynolds@bankmarketingcenter.com](mailto:nreynolds@bankmarketingcenter.com).

*Together, let's make it happen.*

**Tom Ashaug**

Call me at 701.451.7516

Based in Fargo, N.D., serving North Dakota, South Dakota and Minnesota

### Why choose Bell as your bank's lending partner?

Leverage our large lending capacity, up to \$20 million on correspondent loans. Our lending limits are high enough to accommodate what you need, when you need it.

- Commercial & ag participation loans
- Bank stock & ownership loans
- Bank building financing
- Business & personal loans for bankers

**We do not re-participate any loans.**

**Bell Bank**

bell.bank

Member FDIC  
EQUAL OPPORTUNITY LENDER  
32150

# ATM Technology Growth

By Joe Woods, Dolphin Debit



**D**o you remember the Commodore 64 computer? My grandparents had one when I was growing up. I remember the floppy discs you had to swap in and out when playing a game or working on a program, printing my school reports on the dot matrix printer. I remember being amazed at what it could do. Flash forward to today, and I look at the iPad and tablet-based devices with Bluetooth and Wi-Fi connectivity, touch screens, etc. — technology has advanced at an exponential rate in the past few decades.

The ATM is seeing that same technological advancement. It wasn't that long ago that envelope deposit was amazing new tech. Now we see new ATMs with features like video teller, contactless card usage, etc. As ATM experts, we help our clients plan, develop, and implement these new ATM technologies. Although these ATM advancements are critical for success, we're seeing this growth in technology outpace the ability of bank staff.


Although it's not the core competency of the bank to be the ATM expert, the bank is dependent upon ATM technology to help support and ultimately facilitate its strategy and growth.

We are seeing an increase in technology adoption at the ATM. Many of our clients and soon-to-be clients are asking us about these new technologies and making

them part of their two-to-five-year growth strategy. As an example, our deployments for new clients that include automated deposits have skyrocketed. It was only a few years back when many of our banks were choosing to eliminate deposits and stick with basic cash dispensing functionality at the ATM.

Likewise, the ITM, VTM, PTM (pick your acronym) discussions are growing in frequency. Many clients are choosing to deploy ATMs that are prepped or capable of an ITM upgrade — but they have yet to make the investment in the full upgrade or integration. This is the perfect strategy for a bank that has to replace their ATMs due to software requirements or age but are not fully certain what the future direction is for their ATM technology.

Whatever your situation, there is an ATM strategy that fits your needs. At Dolphin, we work with each client to design an ATM program that makes sense for the bank and its customers. Just like your customer base, every ATM location is unique. We understand that this uniqueness is what sets your bank apart.

ATM strategy continues to grow as an integral part of the branch transformation conversation in this “digital age” and should be top of mind for your team. Adding Dolphin as a partner gives your institution an “ATM department” that will cut costs, streamline operations, free up core staff, and ensure strategies are in place for future enhancement and technology upgrades. 



accounts using PayPal, Square and QuickBooks. This lost business equated to nearly \$27 million in initial deposits and \$60,000 worth of merchant fee income in one year!


If your commercial portfolio is declining, it's likely that your customers are going elsewhere. You need a payment partner that will help you to compete in the marketplace, protecting you against customer attrition.

## Think Outside the Square

Fintechs-turned-bank eliminate barriers to payment processing by providing rapid onboarding, but fast doesn't mean good. Square often works with higher-risk businesses and has been known to hold merchant funds, sometimes for days or weeks, without notifying the merchant. Plus, Square requires the purchase of equipment that cannot be used with other systems.

Fitech offers numerous ways to securely set up a merchant account and can have the merchant accepting payments in as few as 24 hours. Our equipment is system agnostic, so merchants don't have to worry if their equipment will work, and funds deposit the next day — no unexpected account holds.

## Pick the Right Partner

Speed and convenience are important in a tech-driven environment, but don't ignore service. Your payment partner should create a roadmap that reinforces your brand and deliver a superior customer experience 24/7. 

*Fitech, like the CBA, focuses on the interests of community banks. For help crafting an advantageous payment strategy, contact Erin Jester, Director of Sales, at 559.908.4010 or [ejester@fitech.com](mailto:ejester@fitech.com).*

# It's Not Hip To Be Square

**T**he phrase, "It's Hip to Be Square," couldn't be further from the truth when it comes to fintechs and the risk they pose to community banks. Some fintechs may seem innocent, but in reality, they are quite powerful, and they are quickly taking away both commercial customers and depository fee income from community banks.

## Know the Risk

As merchants seek convenience, providers such as QuickBooks and PayPal are offering payroll solutions, taking payments, and, eek, making

loans, thereby obscuring the lines for merchant services and jeopardizing your long-term relationship with business customers.

## Seize the Opportunity

Does your institution integrate with QuickBooks? QuickBooks partners with a competing bank and is providing competitive services such as interest-yielding accounts, ACH transfers and Visa debit cards directly to your commercial account holders.

Fitech recently helped a community bank in South Carolina identify hundreds of its commercial

# Be in the Know – SBA 504 Refinance

By Juliene Wynn, Director of Lending & Compliance,  
Preferred Lending Partners

Anyone who participates in SBA financing eagerly awaits new 504-debt refinancing rules. After much anticipation, on July 29, 2021, the U.S. Small Business Administration published the new interim final rules for 504-debt refinancing programs as authorized under Section 328 of the Economic Aid Act. The new rule was effective immediately. The updated regulations expand the usefulness of 504-debt refinancing programs to assist small business recovery and growth. Check out the updates below.

## For 504 debt refinancing **WITHOUT** expansion:

**Qualified debt** — must be at least six months old before the SBA application date to be eligible for refinance, reduced from two years old. Qualified debt for the small business is defined as at least 85% of the original debt that was allocated for financing eligible fixed assets.

New businesses are not eligible for refinance without expansion. The applicant must have been in business for at least two years. (Note: this is not a “new” rule.)

**Allows the refinance of existing government-guaranteed debt** — existing SBA policies related to refinancing existing 504 or 7(a) loans will apply (these are the same requirements that currently exist for the 504-debt refinance with expansion program), including the following:

- For an existing 504 loan, either both the third-party loan (1st mortgage) and the SBA 504 loan (2nd mortgage) must be refinanced, or the third-party loan must be paid in full.
- For an existing 7(a) loan, the CDC must verify in writing that the present lender is either unwilling or unable to modify the current payment schedule. In the case of same institution debt, if the third-party lender or the CDC affiliate is the 7(a) lender, the loan will be eligible for 504 refinancing only if the lender is unable to modify the terms of the existing loan because a secondary market investor will not agree to modified terms.
- The refinancing of any federally-guaranteed debt will provide a “substantial benefit” to the borrower — minimum 10% savings on the new installment amount attributable to the debt being refinanced (same definition as currently used in the 504-debt refinance with expansion program); this is now required for all 504-debt refinance without expansion projects. Prepayment



penalties, financing fees, and other financing costs must be added to the amount being refinanced in calculating the percentage reduction in the new installment payment. The portion of the new installment amount attributable to “Eligible Business Expenses” will not need to be included in this calculation. “Eligible business expenses” are defined as operating expenses of the business that were incurred but not paid prior to the date of application or that will become due for payment within 18 months after the date of application. This includes accrued expenses such as salaries, rent, utilities, inventory, and other expenses of the business that are not capital expenditures.

**Current on all payments** — eliminates the requirement that the borrower must be current on all payments due for not less than one year before the SBA application date. Because the qualified debt now must be incurred not less than six months before the date of the 504 Loan application, the SBA no longer requires that the applicant be current on all payments due on the Qualified Debt for not less than one year before the date of application. In accordance with prudent lending standards, the SBA expects the CDC to consider whether the applicant is


current on all payments due and the applicant’s history of delinquency in its credit analysis.

**Reinstates an alternate job retention standard** — all existing jobs measured on a full-time equivalent (FTE) basis can be counted as jobs retained by the refinancing project.

**For 504 debt refinancing WITH expansion:**

The amount of the existing indebtedness that may be refinanced as part of a 504 project is increased from not more than 50% to not more than 100% of the project costs of the expansion.

All other existing policies and procedures for 504-debt refinancing with and without expansion continue to apply unless specifically modified by the interim final rule.

Specifically, in the 504-debt refinancing without expansion program, the 20% cap on eligible business expenses and the maximum loan to value for projects involving eligible business expenses continue to apply. 

*Contact one of the local Colorado CDC’s for more information.*



**> GREAT JUST GOT GREATER.**

Fitech, a trusted payment partner for financial institutions, has a hard-earned reputation for delivering solutions that expand payment options, improve non-interest revenue and streamline business efficiencies. And our solutions keep getting better and better.

As the newest member of the Deluxe family of companies, we are transforming payment technology for FI’s and their merchants, from start up to maturity.

**See what we have to offer!**

Erin Jester, Director of Sales  
559-908-4010 | [ejester@fitech.com](mailto:ejester@fitech.com)

**FITECH**  
by deluxe

# Strengthening Your Bank's Defenses Against Ransomware

By Sean Martin, CSI

## Cyberattacks Continue Making Headlines

In May 2021, a ransomware attack targeted one of the nation's largest pipeline companies, resulting in a nearly \$5 million ransom payment, disruption of fuel supply, and even panic purchasing among consumers in certain regions of the country. Shortly thereafter, JBS — which is among the largest meat processing companies in the world — was also hit with a ransomware attack, paying \$11 million to keep its data safe.

Another example: Kaseya — an IT solutions developer for managed services providers (MSPs) and enterprise clients — announced it was the victim of a cyberattack in July 2021. Hackers carried out a supply chain ransomware attack by exploiting a vulnerability in Kaseya's software against multiple MSPs and their customers. It's estimated that up to 1,500 businesses — including financial institutions — were affected by the attack and experienced ransomware compromise.

The recent increase in the frequency of ransomware attacks is an enormous concern for all organizations, but especially for financial institutions, whose data is particularly sensitive to these attacks. Ransomware is a growing threat, and banks must be vigilant against this type of attack.

CSI's 2021 Banking Priorities Executive Report revealed the overwhelming majority (81%) of bankers view social engineering as the greatest cybersecurity threat in 2021. Phishing aimed at internal targets that let attackers into internal systems (32%) was another top cybersecurity threat identified by bankers in that report. There is plenty of evidence to support this concern, as employees working from home continue to be targets for cybercriminals.

## Is Your Bank Prepared for a Cyber-attack?

As cybercriminals continue to evolve their tactics and cast a wider net for victims, ensure your bank is prepared to confront this heightened risk. Reference these seven steps as a guide to enhance your bank's preparedness for attacks and defend against future threats, including ransomware.

### 1. Have a Plan in Place

The automated nature of modern ransomware and the immense scale used in attacks are warning signs to all financial institutions. Ransomware attacks will likely increase in scale, frequency, and sophistication as more cybercriminals seek an easy payout. As ransomware attacks surge, institutions must consider the operational, financial, and reputational implications of being held hostage by ransomware.

Does your institution have an actionable plan in writing? If not, developing one should be your priority. Communicating a plan of action to your entire organization in your Incident Response Plan (IRP) — which highlights prevention, detection and protocol during an attack — allows for a quicker response and possible isolation of any infected devices.

### 2. Conduct Regular Data Backups

Ransomware thrives on holding your data captive, making regular data backups essential. If your data has been duplicated and stored elsewhere, ransomware becomes far less threatening. To minimize the damage from an attack, the best recommendation is to implement a risk-based backup program with the frequency and retention period of backups defined according to the criticality of the data. After determining your backup schedule, test your data backups to ensure they work properly.

### 3. Prioritize Employee Education

A core component of most cyberattacks remains consistent: at some point, the attack encounters a human who allows the cybercriminal access to your system. Therefore, training your staff — especially at the highly targeted customer service level — should be paramount. Educating employees and providing them with social engineering training reduces the likelihood of those employees inadvertently aiding an attack.

Ensure your employees are familiar with the signs of ransomware and know how to react when they encounter suspicious activity. With proper training, your bank's staff will become a powerful line of defense in protecting against malicious attacks.

### 4. Leverage Industry Best Practices

Cybercriminals often use confusion and fear as their weapons of choice. Their methods are constantly evolving, designed to circumnavigate any new roadblock they encounter. Because of this, one of the best ways of fighting cybercrime is creating a unified community dedicated to a constant and open flow of information and articulation of best practices. Organizations such as FS-ISAC allow institutions and businesses across all industries to share best practices and insight in the hopes of achieving a unified front against cybercrime.

### 5. Assess Privilege Control

Allowing all your employees unlimited access to your customers' secure data is an enormous liability. Ensure that only employees who need deep access into valuable customer files have it and only give administrative privileges to an appropriate few. Limiting these privileges to a smaller, more acutely trained pool of employees will decrease your bank's overall risk.

Additionally, consider requiring multi-factor authentication (MFA) to enhance protection. Using MFA requires multiple factors to verify a user's identity, preventing a hacker from accessing accounts by obtaining or cracking a password. Authenticating a user's identity and protecting credentials using two or more pieces of evidence will further strengthen the resilience of your network.

### 6. Secure Your Entire Perimeter ... Including the Cloud

Without tight perimeter security, your bank is basically leaving the front door wide-open. It's no longer optional to simply deploy firewalls and intrusion prevention systems. Financial institutions must go above and beyond typical security measures to keep their

systems safe and should consider taking advantage of enterprise-grade security solutions.

It's important to understand that your perimeter extends beyond your physical perimeter. As more institutions prioritize cloud migration, ensure you approach cloud adoption with security considerations in mind. Having the proper security configurations and deploying the latest enhancements for your environment will maximize the benefits of the cloud. Further, monitoring your entire perimeter — including your cloud-based IT infrastructure — is critical.

### 7. Monitor Your Network

One of the biggest challenges community financial institutions face is monitoring for suspicious activity. Security systems and tools are critical, but neither take the place of eyes on glass. One of the wisest investments you can make is partnering with a managed services provider (MSP) that offers around-the-clock assistance in monitoring suspicious activity. These same providers can assist with administrative functions — including system and software updates — and offer practical, actionable advice to make sure your bank is doing everything possible to prevent attacks.

## Mitigate Your Bank's Cybersecurity Risk

Cybersecurity is more than a technology issue; it is a business issue. Don't leave your bank vulnerable to ransomware or other cyberattacks. By keeping a pulse on current and evolving threats, you can mitigate your cyber risk to keep your networks, data, and users safe.

Gain additional insight on strategies to detect, prevent and manage cybersecurity threats by watching CSI's on-demand webinar. [https://www.csiweb.com/what-to-know/content-hub/odwebinars/cybersecurity-insight-keys-to-mitigating-cybersecurity-threats/?utm\\_source=association&utm\\_medium=article&utm\\_campaign=odw\\_fy22\\_07\\_cybersecurityinsight](https://www.csiweb.com/what-to-know/content-hub/odwebinars/cybersecurity-insight-keys-to-mitigating-cybersecurity-threats/?utm_source=association&utm_medium=article&utm_campaign=odw_fy22_07_cybersecurityinsight). 



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



# The Path to Service Quality and Managing Costs for the Future

By Bryan T. Di Lella, Senior Vice President  
ICI Consulting

**T**hroughout the course of the pandemic, households have accumulated significant savings. Banks, awash in deposits and with interest rates still at low levels, have increased lending while working through the many challenges of the past year, including maintaining services to existing customers. Despite the operational obstacles brought on by the pandemic, most financial institutions have managed to attract new customers, which has further aided the growth in asset size for institutions nationwide. The Paycheck Protection Program (PPP) has also contributed substantially to this growth.

While the economy gradually adjusts from heavy government stimulus and returns to growth levels seen before the pandemic, banks are adapting to new ways of serving their customers. Beyond the logistical challenges of in-person meetings and modifications to branch operations to maintain service quality to customers, banks have mostly resorted to bolstering the use of Digital Channels to continue to operate and thrive throughout the pandemic.

The rapid adoption of Digital Banking has exacerbated the need for banks to have responsive and innovative digital and mobile offerings. Indeed, the pandemic accelerated the use of such channels among a rising set of customers who may not have interacted with their financial institution in this manner before. For banks that are really tuned into their customer base, it is obvious that effective digital channels must be a part of current and future strategy. This is the contemporary path to service quality for those banks, and they are prepared to invest in it.

Notably, service quality is mostly the result of the management and philosophy of the bank. As with most

any business, customers want to see that their bank cares — that it values the relationship and understands the customers' needs regardless of where and when the interaction takes place. If banks embrace this intense customer focus, they will forge new paths to service quality. One ICI Consulting client that kept its branches open and operational boldly stated, "We never had to ask our customers to make an appointment to visit a branch."

In part, service will only be as good as the software tools banks use to implement Digital Banking. Therefore, a comprehensive survey of the institution's requirements, and a rigorous evaluation of current offerings, are demanding the attention of bank executives to be competitive in the market, responsive to existing customers, and in a position to attract new ones. Banks must look ahead to a time when the economy stabilizes, employment returns to normal levels, and people embrace their everyday routines. To secure a long-term and stable customer base, banks will need to grow by catering to a younger demographic while still providing superior service to their clients. Attracting and servicing future generations will require innovative new products and services delivered through Digital Channels. Banks must also anticipate the likely challenges ahead and be prepared for a time when growth levels out. When this occurs, one of the most dependable actions is to control costs.

With few exceptions, Data Processing expenses are among the top three expenditures, along with Salary & Benefits and Premises & Fixed Assets that a financial institution incurs on an ongoing basis. Data Processing expenses, which include an institution's spending on Core Processing & Ancillary Systems, are easily addressable cost reduction targets.

The Ancillary Systems are key applications that surround and interact with the Core System. They include important services like ATM/EFT, Credit Card, Online Banking, Mobile Banking, Loan Origination & Servicing, Payments, Wire Transfer, Cash Management, Document Management, BSA/AML, IT Security, Check Processing, among others. These Ancillary Systems are as important as the Core System because they not only support the key business functions of the institution, but also serve as touchpoints for customers.




We also see banks aggressively pursuing new strategies to expand and emphasize Digital Channels — many that shrewdly started such projects prior to the onset of the pandemic. In modernizing their Digital Channels, banks are not only reaching more customers, but they are also doing so with more innovative and integrated applications while potentially reducing data processing spend. Furthermore, they are making a sound investment in what will become a vital channel through which customers will be served in the future.

Banks are also making changes to the Digital Channel to address a shifting mix of commercial or consumer business, integration to the Core System, and even because of variable vendor product and support plans. When reviewing Data Processing systems contracts, ancillary grouping products that serve the Digital Channel with other important applications and especially the Core System will naturally increase the purchasing power and thus negotiation leverage for the bank. We commonly recommend this holistic approach to our clients as it tends to yield the best results.



The rapid adoption of Digital Banking has exacerbated the need for banks to have responsive and innovative digital and mobile offerings.

Banks will do a great service to their customers and shareholders by closely examining and monitoring Data Processing costs. There is a wide range of pricing models in the industry. The best way to gain insight into comparable market prices is to conduct a competitive evaluation of alternatives. The banks that take the time to do so and start the process 24 to 30 months prior to contract expiration will see the best outcome. In terms of finding solutions that effectively serve customers and addressing the institution's business requirements at the best price and terms.

This goal can be mainly achieved by either negotiating new technology contracts or renegotiating existing technology contracts. While some executives deem the technology review process painful, it nevertheless remains an important part of appropriate due diligence by the institution in a key area that is the foundation of efficient and cost-effective operations. Unless the bank enjoys annual contracts, most banks maintain multi-year contracts with the vendors of Core Processing and Ancillary Systems. With the opportunity to review alternative solutions and/or address costs only every five, seven or 10 years, it is wise to take advantage of the typical contract cycle to carefully review these business-critical applications. If not then, when? 

*Since 1994, ICI Consulting has been a leading bank and credit union advisor nationwide. ICI is a consulting firm that supports financial institutions by providing core processing assessments, gap analyses, vendor evaluations, contract negotiation and conversion services. ICI Consulting is well known for saving clients time and money during core processing & ancillary systems evaluations and negotiations with the providers of these business-critical solutions. Learn more at [ici-consulting.com](http://ici-consulting.com).*

# Fed's Durbin Proposal Creates More Confusion Than Clarity

By Myron Schwarcz and Keith Ash  
SRM (Strategic Resource Management)



**B**anks that issue debit cards should brace for challenges if the Federal Reserve moves ahead with a plan to amend certain regulations for card-not-present transactions.

The Fed has proposed clarifications to the Durbin Amendment's Regulation II, including a requirement that card-not-present transactions must be capable of being processed across at least two competing networks.

While the agency has suggested that the change would be “non-

substantive” in terms of new obligations and compliance, there are concerns that, with no further clarifications, the implications for issuers could be very substantive from contractual, financial and compliance perspectives.

When Reg II was created, the Fed believed the market for card-not-present transactions was not mature enough to have solutions to back two unaffiliated networks for online transactions. While some domestic debit networks now support card-not-present transactions, the business case for enablement is murky, and certain

issuers have elected not to opt-in. The Fed has said it feels such practices are inconsistent with Reg II and must be addressed with this clarification.

## What are the concerns for issuers?

Practicality is a big consideration. Depending on how the Fed interprets the two-network requirement, the proposal has raised questions around the compliance obligations that issuers will need to monitor. How can issuers ensure that every merchant accepts both of their card payment networks? Does an issuer need to support all merchants even if one is considered high risk? How will innovation be handled if only one network supports an emerging capability?

The proposal could prove to bedevil community banks. If card-not-present volume shifts from national card networks to regional networks, smaller issuers could run the risk of failing to meet certain contractual obligations and commitments with their networks. That could eventually contribute to more consolidation among smaller banks.

While the current conversation is limited to Durbin's requirement that issuers make at least two network options available for all debit transactions, industry advocates used the comment window to revisit broader interchange grievances. Retail associations and merchants want the Fed to step in and mandate



When Reg II was created, the Fed believed the market for card-not-present transactions was not mature enough to have solutions to back two unaffiliated networks for online transactions. While some domestic debit networks now support card-not-present transactions, the business case for enablement is murky, and certain issuers have elected not to opt-in.

that two networks be enabled as early as the holiday season. They also want the Fed to reexamine the regulated interchange rate, arguing that issuer costs have declined by almost 50% since the ceiling was set in 2011, with no adjustments having been made.

Issuers and associations like the American Bankers Association and the National Association of Federally-Insured Credit Unions caution that the proposal could have unintended consequences for safety and security and a financial impact like the original Reg II rollout. They have strongly suggested that the Fed take more time to analyze the potential implications for issuers and consumers.


Though debit interchange rates are not part of the proposal, the Fed left the door open, stating it will continue to review the regulation and may propose more revisions. And Sen. Durbin brought up the topic of credit interchange in the Judiciary Committee earlier this year as he seeks bipartisan support for further refinements to Reg II, including a potential expansion to credit transactions.

### How should bankers respond?

The comment period ended August 11, so the most proactive thing bankers can do now is prepare for any worst-case scenarios.

Issuers should watch and plan for the proposed changes by taking inventory of their existing relationships and evaluating the implications of change occurring as early as next year.

New contractual relationships should be carefully considered, including commercial terms, given the uncertainty. Issuers should actively engage their government relations

areas and make this issue a priority at the local and national levels while working with their associations. 

#### About the Authors

*Co-author Keith Ash, Senior Vice President at SRM, has 25 years of payments expertise across issuer, network, and process roles. Before joining SRM, Keith spent 14 years at MasterCard leading new business and account management initiatives. Keith can be reached via email at [kash@srmcorp.com](mailto:kash@srmcorp.com).*

*Co-author Myron Schwarcz, EVP at SRM, has two decades of experience in the banking industry, advising leading financial institutions on their strategic initiatives. Further inquiries of Myron may be made via email at [mschwarcz@srmcorp.com](mailto:mschwarcz@srmcorp.com).*



# The OCC Reconsiders Going It Alone on CRA

By Chris W. Bell, JD  
Sr. Hotline Advisor and Associate General Counsel  
Compliance Alliance

To modernize the agency's regulations under the Community Reinvestment Act (CRA), the Office of the Comptroller of the Currency (OCC) published a final rule (June 2020 rule) in the Federal Register June 5, 2020. Previous to this modernization, the OCC had chosen to partner with the other federal regulators to pursue a shared CRA framework for all covered financial institutions. The June 2020 rule was designed to: (i) expand and make clearer "qualifying activities" (including bank lending and investing); (ii) revise the delineation of "assessment areas"; (iii) provide more "consistent and objective" methods for assessing CRA performance; and (iv) mandate "timely and transparent" reporting. On July 20, 2021, the OCC announced it will propose to rescind the agency's May 2020 final rule overhauling the CRA, signaling the OCC's intention to collaborate with the Federal Reserve Board (Fed) and the Federal Deposit Insurance Corporation (FDIC) on a separate joint rulemaking.

The announcement follows the completion of a review undertaken by acting Comptroller Michael Hsu.

Comptroller Hsu stated that although "the OCC deserves credit for taking action to modernize the CRA," the adoption of the final rule was "a false start" in attempting to overhaul the regulation. According to Comptroller Hsu, the OCC intends to work with the Fed and the FDIC to develop a joint Notice of Proposed Rulemaking and build on an Advance Notice of Proposed Rulemaking issued by the Fed last September. The federal agencies issued an interagency statement noting that they have "broad authority and responsibility for implementing the CRA" and that "[j]oint agency action will best achieve a consistent, modernized framework across all banks to help meet the credit needs of the communities in which they do business, including low- and moderate-income neighborhoods."

The OCC explained that the additional time it will take to reconsider the June 2020 rule will (i) enable banks to more flexibly deploy their resources for COVID-19 pandemic-related purposes, (ii) allow the OCC to consider additional input from stakeholders, (iii) provide the OCC with more time to assess issues and questions that have





been raised with regard to the rule's implications, and (iv) enable the OCC to reevaluate the necessary data and take further regulatory action, as needed.

## What's Changing?

While this reconsideration is ongoing, the OCC will not object to the suspension of the development of systems for, or other implementation of, provisions with a compliance date of Jan. 1, 2023, or Jan. 1, 2024, under the 2020 rule. At this time, the OCC also does not plan to finalize the Dec. 4, 2020, proposed rule that requested comment on an approach to determine the CRA evaluation measure benchmarks, retail lending distribution test thresholds, and community development minimums under the June 2020 rule. In addition, the OCC is discontinuing the CRA information collection pursuant to the Paperwork Reduction Act (PRA) notice published in the Federal Register in December 2020. While this reconsideration is ongoing, the OCC will not implement or rely on the evaluation criteria in the June 2020 rule pertaining to: quantification of qualifying activities (12 CFR 25.07 and 25.08); assessment areas (12 CFR 25.09);


general performance standards (12 CFR 25.10 through 25.13); data collection (12 CFR 25.21); recordkeeping (12 CFR 25.25); and reporting (12 CFR 25.26).

## What's Not Changing?

Please note that the OCC has not merely voided its June 2020 rule. It is important to remember that parts of the June 2020 rule are currently in effect. The OCC will continue to implement the provisions of the June 2020 rule that had a compliance date of Oct. 1, 2020. The OCC interpreted and explained these provisions in OCC Bulletin 2020-99. These implementation efforts include

- Issuance of OCC Bulletin 2021-5 providing bank type determinations, lists of distressed and underserved areas, and the median hourly compensation value for community development service activities;
- Deployment of the CRA Qualifying Activities Confirmation Request process for banks and other stakeholders to request confirmation whether an activity meets the qualifying criteria under the June 2020 rule; and
- Provision of training on provisions of the June 2020 rule with the Oct. 1, 2020, compliance date in a series of webinars for examiners and bankers.

Compliance Alliance members can find a summary of the June 2020 rule at <https://compliancealliance.com/find-a-tool/tool/occ-cra-modernization-final-rule-summary>.

The right partner can help you navigate the ever-changing regulatory landscape. Bankers Alliance and our teams of companies are here to help with your CRA needs. Compliance Alliance will continue to bring our members up-to-date information and training regarding the CRA modernization efforts and the tools that your financial institution needs to stay in compliance and fulfill your CRA requirements. Review Alliance can audit your systems to make sure that you are gathering, tracking, and reporting the information you need. 

*Chris W. Bell serves as Associate General Counsel for Compliance Alliance. He holds a Bachelor's degree in Political Science from the University of Memphis (Memphis, TN), a Master's degree in Political Management from the George Washington University (Washington, D.C.), and a JD from the St. Mary's University School of Law (San Antonio, TX). Chris began his career working for a regional bank in Tennessee, where he developed a passion for serving customers through the banking system.*

*In law school, Chris focused his studies on the different financial aspects of the law, including the Internal Revenue Code and Uniform Commercial Code. Chris has worked in the legal department of a federal savings bank and for the Texas Department of Banking. As one of our hotline advisors, Chris helps C/A members with a wide range of regulatory and compliance questions and he is one of our featured authors.*

# Transfers Are Nonreportable; No Such Thing as Prior-Year Conversion; 12-Month Limit Only for IRA-to-IRA Rollovers

By Carrie Horn, QPA, TGPC, CISP, CHSP



**In 2020, we had a client transfer his Traditional IRA from another financial organization to an IRA with our organization. The client completed the appropriate IRA transfer paperwork, and the other organization sent the funds by check payable to our financial organization as custodian for the customer's IRA. We deposited the funds into the Traditional IRA as a transfer. Our client received a 2020 IRS Form 1099-R showing this as an IRA distribution and the other financial organization is refusing to correct it. Is there anything our client do to avoid paying taxes on the distribution?**

As you're aware, an IRA-to-IRA transfer is a nonreportable transaction. If the sending organization (the payer) reports the transaction as a distribution on IRS Form 1099-R, Distributions From Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc., the IRS will think that a distribution occurred and that it will be includible in the IRA owner's taxable income. Thus, it's important that the Form 1099-R be corrected.

The IRA owner should contact the sending organization and provide copies of the transfer paperwork to show that the transaction was requested and completed as an

IRA-to-IRA transfer, and ask the sending organization to issue a corrected Form 1099-R. He should also retain documentation of how and when he contacted the sending organization with his request. If the sending organization refuses to correct the Form 1099-R, he can then go to the IRS.


The IRS provides Form 4852, Substitute for Form W-2, Wage and Tax Statement, or Form 1099-R, Distributions From Pensions, Annuities, Retirement or Profit-Sharing Plans, IRAs, Insurance Contracts, etc., to be used by tax preparers as a substitute for Forms W-2, W-2C, and 1099-R. According to the instructions, IRA owners who do not receive corrected forms from payers by the end of February of the year the Form 1099-R is received may call the IRS at 800-829-1040 for assistance. The IRS will contact the payer to request the corrected Form 1099-R and also issue a Form 4852 to the IRA owner. If the IRA owner does not receive the corrected form in sufficient time to file his tax return timely, he may complete Form 4852 as directed in the instructions and attach it to his tax return. IRS Form 4852 requires that the IRA owner complete the questions in Line 8, Form 1099-R, as they should have been on a correct Form 1099-R (e.g., for a transfer, enter \$0 as the gross distribution). Specific details are found in the instructions.

**A client completed a conversion of her Traditional IRA to her Roth IRA on Feb. 2, 2020. We showed this as a conversion on the 2020 IRS Form 5498, but the client is now stating that this was a prior-year conversion for 2019. She is asking us to correct the Form 5498 to show it as a 2019 conversion. Can this be done?**

No. IRA owners frequently get the conversion rules confused with the IRA contribution rules. Unlike making IRA contributions, conversions can never be done after December 31 for a prior year, even if they are completed before the IRA owner's tax filing deadline. You are correct in reporting the conversion contribution on a 2020 Form 5498, IRA Contribution Information, because the conversion took place in 2020.

**An IRA owner rolled over his 401(k) plan balance to a Traditional IRA in January 2021. In February 2021, he converted his Traditional IRA to a Roth IRA. Now he's requesting to move his Roth IRA to a different financial organization as a distribution and rollover within 60 days. Is this**

**permissible or will he violate the one-per-12-month rollover limitation?**

This is a permissible transaction for the IRA owner. The 12-month limitation on rollovers only applies to rollovers between IRAs (e.g., Traditional IRA to Traditional IRA or Roth IRA to Roth IRA). An IRA owner may roll over only one IRA distribution in a 12-month period, regardless of the number of IRAs he owns. But rollovers from qualified retirement plans, including 401(k) plans, are not included in this rollover restriction. An IRA owner may perform an unlimited number of rollovers between an IRA and a retirement plan, such as a 401(k) plan. Also, there are no restrictions on the number of Roth IRA conversions that an IRA owner may perform in a 12-month period, as long as the multiple conversions do not involve the same assets. 



Carrie Horn, QPA, TGPC, CISP, CHSP

**COAN, PAYTON & PAYNE, LLC PROVIDES A FULL RANGE OF LEGAL SERVICES TO THE BANKING INDUSTRY.**

 R. Clay Bartlett	 G. Brent Coan	 Donovan P. Gibbons
 Amanda T. Huston	 Michael C. Payne	 Brett Payton
 Steven T. Mulligan	 Julie Trent	 Matthew L. Chudacoff

  **COAN, PAYTON & PAYNE, LLC**  
ATTORNEYS AT LAW

Denver | Fort Collins | Greeley  
**CP2LAW.COM**

**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:  
[colorado-banker.thenewslinkgroup.org](http://colorado-banker.thenewslinkgroup.org)

# Colorado Banks and Financial Institutions – State Privacy Law Compliance Obligations

By Elizabeth Harding, Shareholder in the Tech Transactions & Data Privacy Practice Group at Polsinelli

**E**merging privacy laws in the US are leading to increasingly complex compliance obligations for banks and other financial institutions. Colorado recently joined ranks with California (with its CCPA and upcoming CPRA privacy laws) and Virginia (with its VCDPA) by adopting its own comprehensive privacy law, the Colorado Privacy Act (CPA). The CPA comes into force on Jan. 1, 2023, and will regulate how personal information of Colorado residents is collected, used, stored, and shared.

## Which organizations are subject to the CPA?

The CPA applies to organizations that conduct business in Colorado or that target their products or services to Colorado residents or households (“consumers”) **and**:

- Control or process the personal data of at least 100,000 Colorado consumers per year; or
- Sell personal data and process or control the personal data of 25,000 or more Colorado consumers or more.

## To what extent does the CPA apply to banks and other financial institutions?

The good news for Colorado-based banks and financial institutions is that they are subject to a blanket exemption under the CPA on the basis that they are governed by the Gramm-Leach-Bliley Act (GLBA). The GLBA imposes privacy requirements on financial



institutions’ collection of nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes.

## Does this mean that Colorado-based banks and financial institutions don’t have to worry about State privacy laws at all?

No. Although Colorado (like Virginia) applies a blanket exemption to financial institutions (and their affiliates) that are subject to GLBA, other State privacy laws take a different approach. Notably, California’s CCPA (and forthcoming CPRA) contains a narrower exclusion, which applies only to personal information collected, processed,

sold, or disclosed pursuant to GLBA. In other words, the exemption applies to certain information, rather than the organization as a whole. To the extent Colorado-based banks and financial institutions are subject to the CCPA, certain personal information that they process will still be subject to the requirements of California’s privacy law.

A Colorado-based bank could be subject to CCPA in a number of ways:

- If it targets products or services to California residents or households and (a) has annual revenues in excess of \$25 million, OR (b) processes the personal information of 50,000 or more California residents, households, or devices, or (c) derives 50% or more of its revenues from the sale of California residents’ personal information

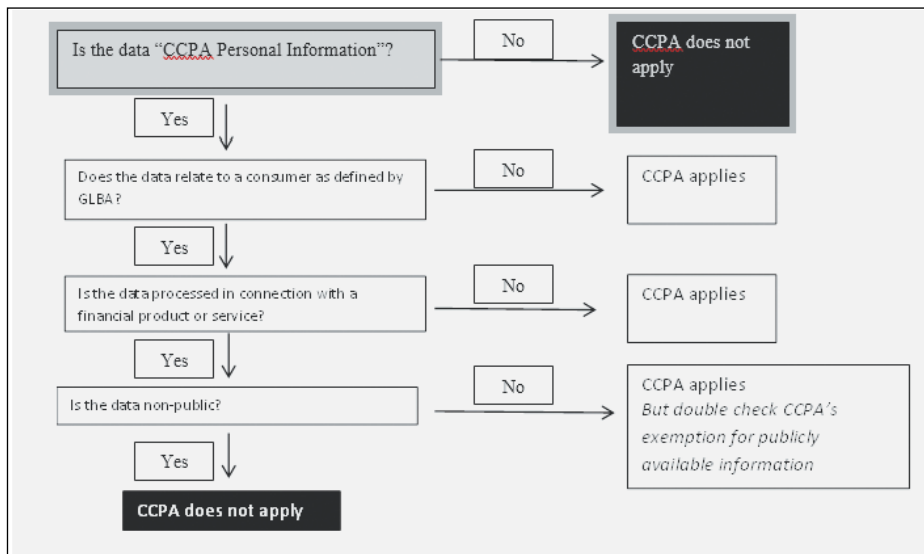
- If it controls, or is controlled by, a business which meets the threshold requirements **and** shares branding with such business

Note, however, that obligations under California’s privacy laws would apply only with respect to personal information relating to a California resident or household.

## How does the GLBA exemption work under CCPA?

The GLBA exemption under CCPA (and the forthcoming CPRA) applies with respect to personal information collected, processed, sold, or disclosed pursuant to ... GLBA. Given that most personal information collected by banks and financial institutions meets this threshold, the majority of personal information processed by such organizations will be out of scope for purposes of the CCPA. However, the exemption does not apply to all personal information. For example, personal information collected from an individual visiting a bank’s website, or applying for a job with the bank, would not be collected, processed, sold, or disclosed pursuant to GLBA, and therefore would not fall within the exemption.

The flowchart below provides a helpful graphic for understanding when the GLBA exemption may apply:



Examples of consumers whose personal information is **protected by GLBA include:**

- Bank customers;
- Individuals applying for a financial product or service (whether in person or online), regardless of whether application is accepted;
- A list of a third-party financial institution’s customers provided to the bank or financial institution (e.g., as part of a joint offering); and
- A legal representative (parent or guardian, for example) of an individual who is otherwise a GLBA consumer.

Examples of consumers whose personal information is **not protected by GLBA** (and therefore is subject to CCPA) include:

- Employees;
- An individual who opens a financial account for their sole proprietorship or on behalf of another business entity;
- Website visitors;
- Individuals on marketing lists obtained by a third-party vendor, that is not a financial institution, and sold to the bank or financial institution; and
- Individuals on general marketing lists developed or obtained by the bank or financial institution (e.g., list of attendees at a marketing event sponsored by the bank or financial institution), but who have not obtained a financial product or service from the bank or financial institution.

Examples of personal information that would not be **covered by GLBA** (and therefore **subject to CCPA**) include:

- Names and email addresses of attendees of a conference sponsored by the bank or financial institution;
- Personnel records;
- Contact information for volunteers of a charity event hosted by the bank or financial institution;
- Contact information obtained by a vendor that is not a financial institution and sold to the bank or financial institution; and
- Information obtained from an Internet cookie of an unregistered visitor who browses parts of the bank or financial institution’s website that is open to the public.

## What obligations do banks and financial institutions have under CCPA?

CCPA places broad obligations on organizations that meet its threshold requirements, including:

- Duty of transparency – businesses must provide consumers with clear

*continued on page 28*

continued from page 27

and transparent notice of the data they collect, what they use it for and who they share it with.

- Right of access, deletion, correction and portability. In addition, consumers have the right to opt out of the sale of their personal information.
- Requirement to enter into contracts with third party service providers who may process personal information on the business' behalf.
- Requirement to implement reasonable security measures to protect against unauthorized use or disclosure of personal information.

CCPA also includes a private right of action for individuals in the event certain sensitive personal information (for example, social security number, account information, password and passport number) is subject to a data breach. The GLBA exemption does not apply with respect to an individual's right to bring an action against a bank or financial institution in the event such organization fails to implement appropriate security protections. The private right of action under CCPA is one of the biggest areas of concern for organizations, as it enables impacted consumers to claim statutory damages in an amount between \$100 and \$750 per incident.

### **What should Colorado banks and financial institutions be doing now?**

In addition to their obligations under GLBA, banks and financial institutions meeting the thresholds discussed above have direct obligations under CCPA, regardless of whether they are physically located in California or not. Violation of state privacy laws could lead to regulatory investigations, fines and class action litigation. Regardless




In addition to their obligations under GLBA, banks and financial institutions meeting the thresholds discussed above have direct obligations under CCPA, regardless of whether they are physically located in California or not. Violation of state privacy laws could lead to regulatory investigations, fines and class action litigation.

of where the bank or financial institution is located, it should consider implementing the following:

- Post a clear and transparent privacy notice, explaining what personal information is collected, what it is used for, to whom it is disclosed, and for how long it is retained.
- Analyze and understand which personal information is in scope for purposes of GLBA and is thus exempted from CCPA requirements, and which is not. This is particularly important when it comes to analyzing whether or not a consumer request (for example, for access to, or deletion of, personal information) needs to be complied with under CCPA.

- Confirm that agreements with third party vendors include adequate privacy and security obligations, and other relevant protections.
- Review security and access controls.

In addition, banks and financial institutions should consider whether to adopt CCPA standards at an enterprise level, or just with respect to individuals who are resident in California. Given the variances in existing State laws, and the likely implementation of new State laws in the absence of a Federal privacy law, there is logic to applying a consistent standard to all personal information regardless of which State the individual is actually resident in. 

# Automated Clearing House Debit Entry Fraud



**B**anks and financial institutions rely on technology to operate successfully and provide customers the best products and services. With technology, though, comes the heightened risk of falling victim to wire fraud schemes that can result in significant financial losses.

One example is Automated Clearing House (ACH) debit entry fraud, when a bad actor executes ACH transfers from a victim's bank account into an account controlled by the fraudster. Because of the rising popularity in using ACH transfers and strict National Automated Clearing House Association rules, banks and financial institutions have never been more at risk. According to the most recent Federal Reserve Payments Study, the number of ACH debit transfers (16.6 billion) exceeded the number of check payments (14.8 billion) for the first time in 2018. In 2000, to provide context, there were 42.6 billion check payments

and only 2.1 billion ACH transfers. "More people and businesses are using this type of transaction, but financial institutions should be aware of the risks involving ACH and the potential for fraud," said Jerry Keup, National Underwriting Officer, Banks and Diversified Financial at Travelers. "There are steps these institutions can take to reduce the likelihood of a fraudulent incident taking place, but they should be vigilant and address any vulnerabilities seriously."

Risk mitigation steps include, but are not limited to:


**Develop methods to identify synthetic identity fraud.** The Federal Reserve bank has identified red flags to aid in recognizing synthetic identity fraud. These include paying close attention to accounts that show:

- The credit file depth is inconsistent with the customer's age or other profile information

- Multiple identities with the same Social Security number
- Multiple applications from the same phone number, mailing address or IP address
- Use of secured credit lines or piggybacking to build credit
- Social Security numbers issued after 2011
- Multiple authorized users on the same account

**Monitoring and analytics.** Using software and analytic data can often detect financial crime attempts much faster than the human eye. But even the best controls can fall short. Travelers offers a wide range of coverages for financial institutions, including an endorsement that covers two specific ACH scenarios:

- A fraudster opens a deposit account with a bank or credit union, then feeds that account with stolen funds from victims through ACH pulls.
- A fraudster establishes a loan or line of credit with a bank or credit union and causes ACH transfers from victims' accounts to repay the loan or line of credit.

Preventive measures taken or reinforced now against ACH fraud attempts can lead to positive results in the future. It's worth the time and investment. 

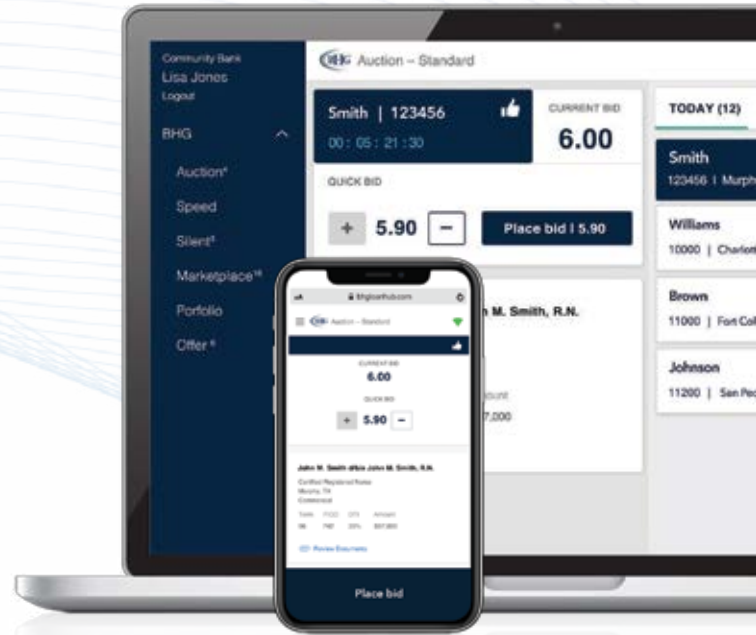
*Travelers is committed to managing and mitigating risks and exposures and does so backed by financial stability and a dedicated team – from underwriters to claim professionals – whose mission is to ensure and protect a company's assets. For more information, visit [travelers.com](https://travelers.com) or talk to your independent insurance agent about ACH coverage.*

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

# THE BHG LOAN HUB

#1 Source for Top-Performing Loans

Gain exclusive access to our secure, state-of-the-art loan delivery platform and learn how more than **1,300 community banks** have earned nearly **\$800MM** in interest income since 2001.



## HOW DOES IT WORK?



Log in to BHG's state-of-the-art loan delivery platform – The BHG Loan Hub



Review and underwrite complete loan packages to make informed decisions with ease



Bid on or purchase loans with the click of a button

Visit [BHGLoanHub.com/CO](https://BHGLoanHub.com/CO) to gain access.