Correspondent Views

BANKERS' BANK OF THE WEST newsletter for community banks

Issue 1 ▪ 2017

PRESIDENT'S MESSAGE

A challenge: reinvent what's possible for community banking

The weekly senior management team meetings we hold at BBW focus on tactical matters but sometimes lead to strategic or hypothetical discussions as well. When that happens, I've found that referring back to the bank's mission statement results in the most constructive ideas. That's because you've got to have a goal in mind before figuring out how to get there.

Our organization's mission can be captured in a single word: partnership. Internally, that word is our gold standard. It's the benchmark we use to assess our performance and, if necessary, adjust our tactics.

From a high-level perspective, we carry out the mission of partnership in three ways: by facilitating community banks' movement of money, helping community banks grow in accordance with their strategic directives, and working to ensure the long-term viability of community banking.

Bill Mitchell
BBW President and CEO

Lately we've turned our attention to how to best accomplish our mission in the future. We're always looking for ways bring more value to our relationships, and the first two months of 2017 allowed us time to reflect, anticipate, and to some extent, reinvent what's possible.

One outcome of that recent reinvention process stems from a suggestion from an experienced and very perceptive community bank president who serves on the board of directors of our holding company. Even as the number of community banks continues to drop due to mergers and acquisitions, this director knows—as we all do—that community banking remains critically important to individuals, many towns, small businesses, and the local and national economies. From this awareness, he posed a challenge: What else can BBW could do to foster the sustainability of smaller institutions?

Based on what we've witnessed at numerous peer-to-peer meetings of community bankers, we think collaboration is at least part of the answer. So in March, BBW will host a small gathering of community bank CEOs and industry allies with specialized expertise to tackle the issue of sustainability. In addition to a roundtable discussion, this initial "meeting of the minds" will have an educational component featuring Adam Fiedor and Michael Richter (GLC Advisors & Co. LLC) and Dave Nowling (Graduate School of Banking at Colorado faculty member).

Our hope is that this will be the first of several such small-scale gatherings, a forum for learning about strategic options for shareholder liquidity, and the start of a dialogue on adding value through leadership. Most importantly, it's a first step. I'd invite other community bank CEOs interested in attending future roundtable discussions to get in touch with me (contact information below).

While we're encouraged by the response to the March CEO roundtable and the way it's taking shape, BBW is working on other important 2017 projects as well. One is our information security and technology conference, to be held in Denver July 16 through 18. The goal of this education-packed program is to provide current, relevant information to the people charged with guiding, supporting and securing your bank.

It all comes down to partnership. The tactics we use to carry out our mission need to be evaluated, tweaked, and reinvented from time to time. But our mission as your partner is set in stone.

To contact Bill Mitchell, call 303-291-3700.

A journey of a thousand miles begins with a single step.
Lao Tzu, philosopher

TAKING NOTE

COMMERCIAL LENDER SEMINAR SCHEDULED

For the tenth consecutive year, BBW will bring the highly rated seminar for business loan officers known as **Loan Officer Financial Management Training** to Denver. The hands-on program will be held October 26 and 27 in the Bankers' Bank of the West board room and led by **Mike Milan** of Finagraph.

With an emphasis on relationship-building, the curriculum is geared toward experienced business loan officers with portfolio, underwriting or calling responsibilities. It focuses on cultivating effective techniques, strategies and tools lenders can deploy immediately for the benefit of the bank and its commercial customers.

Registration is open and, because class size is limited to 24 participants, early enrollment is recommended. The seminar brochure—including the program outline, logistics and registration form—is coming soon to **www.bbwest.com**.

FASTER PAYMENTS TASK FORCE ISSUES REPORT

Part one of the Faster Payments Task Force final report can be downloaded at **https://fedpaymentsimprovement.org/**. Locate it under **Faster Payments** on the main menu.

PRESSING FORWARD ON INFORMATION SECURITY

Anne Benigsen, a key member of the BBW team and head of the bank's information technology area, has received a globally recognized and governed certification in the field of information security: designation as a Certified Information Systems Security Professional (CISSP®).

The certification requires exhaustive study and commitment, professional experience in multiple areas of information security, a passing score on a comprehensive exam covering eight areas of information security, and endorsement of all of these qualifications by another certification holder. Additional continuing education requirements must be met to maintain standing.

The deep experience and knowledge signified by the certification will enhance not only BBW's information technology and security capabilities but also, by extension, the community banks we serve. Congratulations, Anne!

ABOUT

Correspondent Views is published by Bankers' Bank of the West for independent community banks in our service area. Downloadable versions are posted to our website.

If prefer to receive newsletters by email, send your request to **info@bbwest.com**.

Headquarters:
Bankers' Bank of the West
1099 18th St., Ste. 2700
Denver, Colorado 80202
303-291-3700 | 800-873-4722

BBW Bancorp, Inc. Board of Directors

BRACING FOR MORE OF THE SAME

Expect threats to become pervasive, stealthier, more numerous

Greg Miller, IT Analyst
Bankers' Bank of the West

Last year cybersecurity threats and attacks increased to mainstream levels. No relief is in sight for 2017. In fact, cybersecurity threats are all but certain to evolve and escalate.

Some things to watch for on the cyber landscape:

- IoT (Internet of Things) attacks will heat up. The intended targets could be anything from routers and digital video recorders to refrigerators—and even cars. Smart devices like these have already been hacked easily thanks to the typically weak authentication controls on such devices. Watch for more frequent and widespread IoT hacking incidents this year and beyond.
- The evolution of ransomware. Criminals have found extortion via ransomware very profitable, so experts predict it will become more sophisticated, devious and rampant.
- No letup on internal threats. Through more and more phishing and social engineering attempts, hackers will try to become the "man in the app" by obtaining local credentials to gain access to systems. The paradox of human nature means that users are both your strongest and weakest defense.
- The new battleground will emerge. As people increasingly look to the cloud for software for service (SaaS) solutions, it will become both the next big arena for hacking attacks as well as the new frontier for cybersecurity.
- Mobile devices will be at greater risk. They've become so commonplace—it seems everybody has one, or several—that mobile devices are very attractive targets for hackers today. Malware for mobile devices exists already, and attacks will continue as the devices become further integrated in our daily lives.

SPREAD AWARENESS; STAY SAFE

Tax scams committed in 2016 resurfacing in full force today

The BBW Information Technology Department

We're in the midst of tax season, which in recent years has become a magnet for scams from nation states, hacktivists and criminals looking to make a profit and cause disruption. How can you protect yourselves and your customers?

FIRST, be aware of what's out there.

- Business Email Compromise (BEC) attacks. Criminals either spoof or hack a CEO, HR office or CFO email account and, using that false identity, request W2 information from employees. Sometimes staff receive bogus follow-up emails requesting wire transfers or inquiring whether they are "still in the office."
- Banks are targeted frequently. The top scam victims in 2016 were financial institutions. Criminals favor tactics that work, so we can expect many more attempts this year.

SECOND, understand what you can do about it.

- **Educate**. Keep employees updated on the specific dangers of this season. Inform your business customers, too. If small businesses are unaware, they can become easy targets for criminals once they're finished attacking larger businesses.
- **Protect**. Requiring two-factor authentication (2FA) or multifactor authentication for email can make compromise much more difficult.
- **Verify**. If in doubt, call or otherwise confirm the source of an email. If the originator is unavailable, ask your IT team to decipher the email header and tell you where it came from.
- **Report**. U.S. governmental agencies are interested in receiving information on phishing attempts and internet crime. Some key contacts are listed below.

RESOURCES & REPORTING CHANNELS

Internal Revenue Service website: ..... www.irs.gov
To report a phishing attempt: ..... email phishing@irs.gov
To report a scam to the
Internet Crime Complaint Center: https://www.ic3.gov
In case of W2 compromise: ..... www.identitytheft.gov
or: ..... www.irs.gov/identitytheft

ON THE HORIZON FOR LENDING

Shifting consumer buying patterns—a potential risk to loan portfolios

Jim Swanson, President ▪ Bank Strategies LLC

Evidence of shifting consumer shopping patterns toward e-commerce and away from physical stores is all around us. Maybe you see changes in your own habits: How many of you made some holiday purchases last year online instead of venturing out to malls and shopping centers?

The media have run numerous stories of one retailer after another announcing plans to substantially downsize store locations, and reported on others at risk of going out of business altogether. A few of the names in the news have been venerable retailers like JC Penney, Sears/K-Mart, Macy's, and Office Depot. Even WalMart has closed stores.

E-commerce sales have climbed steadily over the past decade, increasing nationwide from approximately three percent of total retail sales to nearly eight percent.[1] As younger generations who grew up with internet shopping accumulate wealth and constitute the bulk of consumers, a reversal of the movement toward e-commerce seems unlikely.

Businesses focused on e-commerce are making significant capital investments to foster this trend and remove some of the advantages traditionally enjoyed by brick-and-mortar retailers. Amazon, for example, recently announced plans to open a million-square-foot fulfillment center in the Denver metro area that will create an estimated 1,000 jobs and radically reduce delivery times for online shopping purchases.

This move was in addition to a 452,000 square foot sortation center the company opened in the area last June. Amazon's next goal is 30-minute delivery. That's little more than an average consumer's round-trip driving time to the local shopping center—and a significant competitive advantage over the convenience offered by brick-and-mortar retailers.[2]

What do these changes mean for community banks? The immediate answer could vary depending on your customer base. But with CRE 2 loan levels up materially over the past three years across a nine-state region that Bank Strategies LLC monitors, odds are there is growing exposure in this lending sector.

It's true that most community banks are not financing WalMart pad sites or large retail shopping centers. Nevertheless, your real estate portfolios likely have some retail exposure risk. The first step in managing any risk is to understand your bank's exposure level. In this case, that involves identifying what volume of retail-focused business you have in your owner-occupied CRE sector and in the tenant base of your non-owner occupied portfolio.

In our experience, we've found the retail sector often flies off the radar when it comes to banks' CRE stress testing and risk management practices. This points up the importance of knowing your level of exposure. You might find additional steps are needed to quantify, manage and control your risk exposure—such as stratifying exposure between businesses focused on consumer goods that could be more vulnerable to e-commerce competition and those that are serviced-based. Other risk management strategies you may be familiar with include setting concentration limits and ongoing monitoring processes, clarifying policy expectations, and in some cases, tightening standards.

At the end of the day, shifting consumer buying patterns reflect the changing world we live in, and underscore the need to evaluate the impact of these changes on the external risks facing your bank.

The Denver-based Bank Strategies LLC consulting firm assists community banks by bringing decades of expertise to activities as varied as credit risk management, loan policy and procedure review and development, profitability enhancement, safety and soundness exam preparation, and regulatory compliance risk management. Contact them at **303-903-9369** *to discuss your bank's unique needs.*

[1] U.S. Department of Commerce. (2016). *Quarterly Retail E-Commerce Sales 3rd Quarter 2016 – CB16-188. U.S. Census Bureau News.*

[2] Rusch, Emilie, and Chuang, Tamara. (January 24, 2017). Amazon opening first fulfillment center in Colorado, hiring 1,000 in Aurora. *Denver Post*.

Upgrading tools, automating processes, shaving expenses, and staying smart

Debbie Wendt, SVP–Operations ▪ Bankers' Bank of the West

We're already about one-sixth of the way into 2017—who sped up the clock, anyway?—and it seems change is afoot on all fronts. Fortunately, the changes we have to report are positive.

ACH template history

From the **ACH Template Management** screen, users now have access to an audit of individual entry detail record changes. All changes to a record are audited—even those excluding an entry. To access an audit, click the **Change History** link for the template you want to research.

International wire report

Account activity and transaction reports are updated for FX interfaces that contain information about both the US Dollar amount and the FX amount in the transaction. Wires that don't contain both amounts are displayed with detail in the appropriate columns.

The **Amount** column is updated to reflect the US Dollar amount of the transaction. Approved totals at the bottom of the report equal the sum of the US Dollar amount of all the FX transactions, if such information is available, in the report. The **FX Amount** and **FX Currency** columns provide users additional transaction detail without clicking on the transaction link.

Are you aware

LendingTools.com can build a direct connection from your core system to BIDS for the purpose of receiving and sending ACH files, eliminating the need for manual uploads and downloads. Note that all files still must be approved.

To enroll in this service or find out more about the direct connection option, which is for ACH files only, contact the BBW Operations team.

Keep in mind the bottom line

Starting with the March monthly analysis statements to be sent in April, earnings credits will be applied to offset not only charges for BBW services but also Federal Reserve Bank fees. The change in calculation will benefit banks that maintain high DDA balances.

For banks that have considered raising balances but haven't, the prospect of reduced fees makes this a good time to review (and possibly adjust) peg balances and keep a tight rein on expenses.

How to fill knowledge gaps

The catalog of 2017 WesPay-led webinar classes for BBW customers was sent to BIDS administrators in early February. If you haven't gotten your copy, our Operations specialists (see contact information below) will be happy to email it to you.

All of the scheduled courses are current and applicable to anyone who works in bank operations—full-time, part-time, seasonally, or on a float basis. The banking industry changes quickly, and the task of keeping all your people up to date is never-ending. Because it's convenient, focused, and reasonably priced, web-based training can effectively fill in any knowledge gaps your bank might have.

For assistance or information, contact BBW's helpful Operations team at **ops@bbwest.com**.

Before you sign that agreement, read

Mary Ann Elliott-Supples
SVP–Bank Card ▪ Bankers' Bank of the West

Nobody wants to be the bearer of bad news. I don't. That's why I urge all community bankers to closely read and carefully consider the long-term ramifications of any agreement before they sign.

An alarming number of merchant service providers build non-compete clauses into their contracts. Those clauses often prevent the community bank from marketing or providing card services to its own merchant customers for an extended time AFTER termination of the contract.

Given the importance of a loyal business customer base, community banks have a vested interest in maintaining close merchant relationships — which is impossible when an outsider cuts the bank out of the picture.

So scrutinize any contract you're presented with for phrases like "agreement not to market." This condition should be a non-starter, and you have better options.

Need help with a review of your contract? Reach us at 1-800-601-8630 or bankcards@bbwest.com.

NEW ON THE CYBER LANDSCAPE

Complex malware threat needs to be understood, detected

Anne Benigsen, CISSP ▪ First VP – Info Security & Technology
Bankers' Bank of the West

There is always something looming on the horizon when it comes to information and cybersecurity. This could be the year of a highly advanced threat known as fileless malware, which was used recently to steal more than $1 billion through banks. Many industry experts believe two hacker groups, Carbanak and GCMAN, were responsible for those thefts.

The buzz began with the 2015 discovery by Kaspersky, the cybersecurity developer, of an infection of its network that was caused by a new type of malware derived from Stuxnet, a nation-state-sponsored worm. What made the malware remarkable was that it created no permanent files and left no traces on any hard drive. Instead, it resided solely in the memory (RAM) of the computer. So after the computer was shut off, there was no evidence.

Now hackers are starting to use variants of fileless malware to get a foothold into a system, and then use regular Windows tools for financial gain—by, among other things, installing legitimate products that can be used for nefarious purposes.

Kaspersky Lab discovered this variant recently and, after doing an international study, found it on 140 enterprise networks, including financial institutions in the United States. It's reasonable to assume many more financial institutions are compromised because most are outside of the enterprise tests performed by Kaspersky.

These protective measures are recommended for financial institutions:

- Change passwords. That is, **all** passwords—not just into user accounts, but into firewalls, routers, switches, and other appliances.
- Utilize two factor authentication (2FA) or multifactor authentication for more services and in-house programs or portals.
- Maintain a high level of proficiency within your in-house or third-party experts.
- Ensure you have detection and prevention tools that are regularly upgraded and sourced through industry leaders.
- Make sure your in-house or third-party information and cybersecurity team understands the "indicators of compromise" for this threat.♦

The threat landscape has gotten more sophisticated, and we must be able understand, detect and remediate new threats, even when we cannot prevent them.

♦ **https://securelist.com/blog/research/77403/fileless-attacks-against-enterprise-networks/**

BANKERS' BANK OF THE WEST
1099 18th Street ▪ Suite 2700
Denver, Colorado 80202

INSIDE on page 5:
Another reason to think strategically before signing that agreement