Correspondent Views

BANKERS' BANK OF THE WEST newsletter for community banks

Issue 2 ▪ 2019

PRESIDENT'S MESSAGE

Decisions, decisions: optimal outcomes depend on intelligent choices

Having many options to choose from can be exciting. Or nerve-racking. The way you feel about making a decision depends on your frame of mind and the potential downside consequences. It's easy to order onion rings instead of chili fries without giving it a second thought. On the other hand, choosing one of three core providers on the basis of several dissimilar proposals could easily keep a banker up at night.

Bill Mitchell
President & CEO

For people in the banking profession, making choices is a day-in, day-out job requirement—on the credit side as well as in operations. The process of getting to a decision is often part science and part art.

Lenders, credit analysts, members of your loan committee, and loan operations staff can look to the bank's internal policies and procedures and regulatory guidance for decision support. Add to that a firm grounding in business principles, the five (or more) Cs of credit, financial tools, and problem-solving aptitude.

The people in your operations area can refer to standardized processes, rules, industry best practices, and the bank's own policies and procedures when decisions are needed. Banks that enable employees to take job-related periodic training, earn certifications, and join professional associations are building a sturdy foundation for informed decisions.

The "art" side of decision making is harder to recognize except in hindsight. In business, the evidence doesn't always point clearly in one direction. Some combination of integrity, wisdom, intuition, empathy, and common sense can lead to the fairest, most reasonable call when the solution isn't obvious.

With so much information and sophisticated technology at our fingertips in the workplace, we need to communicate thoroughly and often across our organizations. Keeping everyone current on policies, best practices and current threats is vital to making progress on all fronts—from efficiency and profitability to staff retention and security.

"Refreshers" don't need to be long or boring. When I served as president of a community bank, we used to start each day with a brief standup meeting. More than a team-building ritual, it was a time for sharing new information, reminders, and alerts (technology-related and otherwise). The routine worked for us, but how the communication happens is less important than making it happen one way or another.

What brought this topic to mind was BBW's Payments Conference, which concludes today. I was impressed with the mix of attendees (from seven states) and their areas of responsibility—e-banking, sales support, risk, compliance, technology, operations, and finance, to name a few. Some 35 of them signed up to participate in the pre-conference roundtable discussion as well. Their appetite for knowledge and interest in discussing industry issues with peers reflects positively on them and the banks they represent. I'm confident they'll return to work with ideas, data, insights, and contacts that will aid in making future decisions.

If you sent people to the Denver conference, please ask them to share their favorite take-aways. Inside this issue is news on future educational events. Mark your calendar; learning is a life-long process, after all!

TAKING NOTE

SNEAK PREVIEW: 2019 WSDEF SYMPOSIUM

Eric Cook, self-described "recovering banker" of 15 years, will present at the 2019 **Western States Director Education Symposium** to be held **October 27-29 at the Westin Kierland Resort & Spa** in Scottsdale. Since shifting his focus in 2007 to digital marketing strategy, Eric has worked with community banks across the country, leveraging his background in the financial services industry to educate them on strategies well-suited to advancing banks' goals and compatible with their unique privacy and risk concerns. Eric is on the faculty of the Graduate School of Banking at the University of Wisconsin, among others. Event website is **wsdef.org**.

ALSO ON THE FALL CALENDAR

Once again, **Dr. David Kohl** will conduct a webinar on agriculture and ag lending ahead of the loan renewal season. The hour-long session is scheduled for the morning of **November 25**. A session summary and sign-up flyer will be posted to bbwest.com by the start of the third quarter. The presentation is meant for community bank ag lenders, credit analysts, chief credit officers, board members, and management.

To add yourself or colleagues to the notification list, email the contact information (including name, bank and email address) to **training@bbwest.com**. Please specify "Dr. Kohl" in the subject line.

ALERTS TO SHARE WITH YOUR CUSTOMERS

As scammers take up new tricks for cheating consumers, more government and public service agencies are issuing warnings and advice for avoiding such traps. For a robust list of credible posts by Federal Trade Commission staffers, visit **consumer.ftc.gov/blog/**. A 2018 post dated December 27 includes a link to an audio recording of an actual imposter scam call meant to scare Social Security recipients into disclosing personal information.

At the same site, you can sign up for email updates, browse blog posts by topic and date, and add comments of your own.

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 you 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

David A. Ochsner.....Chairman of the Board
Commercial Bank ▪ Nelson, Neb.

Gary Crum .....Director
Western States Bank ▪ Laramie, Wyo.

Mark Daigle .....Director
TBK Bank ▪ Durango, Colo.

John (JV) Evans III .....Director
D. L. Evans Bank ▪ Burley, Idaho

Copper W. France .....Director
Bank of Commerce ▪ Rawlins, Wyo.

Kristin W. Godfrey, Esq. .....Director
Jones & Keller P.C. ▪ Denver, Colo.

Bruce Hellbaum .....Director
Rawlins National Bank ▪ Rawlins, Wyo.

Zac Karpf.....Director
Platte Valley Financial Cos., Inc. ▪ Scottsbluff, Neb.

Quentin D. Leighty .....Director
First National Bank of Las Animas ▪ Monument, Colo.

Debbie L. Meyers .....Director
DunamikosGroup ▪ Denver, Colo.

William A. Mitchell Jr. .....Director
Bankers' Bank of the West ▪ Denver, Colo.

Max T. Wake .....Director
Jones Bank ▪ Seward, Neb.

John (PJ) Wharton.....Director
Yampa Valley Bank ▪ Steamboat Springs, Colo.

Chip technology remains key factor in falloff of card-present counterfeit payment fraud

According to 2018 year-end figures reported by Visa,* the abundance of chip-enabled cards in the U.S. (51.1 million) and U.S. merchants accepting those cards (3.1 million) has been a major contributor to the drop in card-present counterfeit payment fraud. Chip-upgraded domestic merchants saw an 80% reduction in counterfeit fraud from September 2015 to September 2018.

This improvement bears out a belief that helped fuel the adoption of chip technology in 2011—specifically, that it would effectively shrink card-present counterfeit payment fraud.

Although the numbers are encouraging, merchants and cardholders must remain diligent when it comes to fraud. The best line of defense will always be people. So if something doesn't seem right, by all means question it.

* Https://usa.visa.com/visa-everywhere/security/visa-chip-card-stats.html.

Business lender training emphasizes practical tools, techniques, strategies

REGISTRATION NOW OPEN

A powerful interactive two-day seminar, **Loan Officer Financial Management Training**, will be held **October 9 and 10** in Denver. The interactive program is focused on building an array of skills that support commercial lenders' success—from financial analysis and problem solving to sales call planning and relationship building.

Created for seasoned loan officers with portfolio, underwriting or calling responsibilities, the seminar uses case studies, individual practice, and small-group work to build confidence and make the learning memorable. Enrolment, open to community bankers, is capped at 24 to allow for individual attention.

Leading the seminar will be **Chris Carlson**, a banking school faculty member, managing principal at Core Academy, and business consultant. Early sign-up is recommended; download the course/registration brochure at **bbwest.com**

An indispensable facet of effective leadership often goes unnoticed—unless absent

Debbie Meyers, Partner, and Dave Nowling, President & Partner
Dunamikos*Group*

You're probably familiar with this observation attributed to Warren Buffet: **"Trust is like the air we breathe – when it's present, nobody really notices. When it's absent, everyone notices."**

All leaders want others to trust them, of course. When trust doesn't exist, everyone in the organization notices. Leadership and trust go hand in hand: You cannot have one without the other.

Studies have shown that organizations with higher levels of trust are more productive and successful, as they benefit from deeper employee engagement and high morale. Further, such organizations are known in the communities they serve for their trustworthiness, integrity and ethical conduct. Getting to that level is anything but effortless: Organizations must work diligently to build an environment of trust both inside the organization and throughout the communities they serve.

Do you believe your bank is built on a strong foundation of trust? Or might a few cracks in that foundation need some attention? What actions can you take to preserve high levels of trust—or restore broken areas of trust?

Let's consider a few key behaviors commonly considered conducive to high levels of trust:

Consistency. Leaders must be consistent in their approach so others know what to expect. Their actions are aligned with their values. They "walk their talk" and keep commitments.

Open and authentic communication. Leaders must be transparent and willing to share. They fill in the gaps and explain the logic behind decisions. They are candid and open. Recognizing that communication goes both ways, they listen to others, they take stock in feedback, and they communicate honestly.

Accountability. Leaders hold themselves to the same high standards they expect others to follow. They accept responsibility for failures, refrain from casting blame, acknowledge others' contributions, and take responsibility for making things right when necessary.

To learn more about measuring the level of trust within your bank, or about training designed to build and sustain a trust environment, contact our consultants at the **Dunamikos*Group***: **303-941-3966** or **303-898-8707**.

Changes in Standards for Safeguarding Customer Information

Continued from p. 6

- ✓ Access to physical locations containing customer information must be restricted to authorized individuals.
- ✓ FIs are required to encrypt all customer information in transit and at rest.
- ✓ FIs will need to adopt secure development practices for applications developed in-house and utilized for transmitting, accessing, or storing customer information.
- ✓ Multifactor authentication is mandatory for any individual access to customer information or internal networks that contain customer information.
- ✓ Audit trails designed to detect and respond to security events are required.
- ✓ FIs must ensure secure disposal of customer information—in any format—that is no longer necessary for their business operations or other legitimate business purposes.
- ✓ FIs will follow procedures to assess the security of devices, networks, and other items to be added to the information system or the effect of removing such items or otherwise modifying the information system.
- ✓ Policies and procedures need to be implemented to monitor the activity of authorized users and to detect unauthorized use of customer information.
- ✓ FIs will conduct continuous monitoring or periodic penetration testing (annual) and vulnerability assessments (biannual).
- ✓ Security awareness training must be brought current to reflect risks identified by the risk assessments.
- ✓ Personnel assigned to information security must be qualified for their positions and also sufficient to properly perform their function.
- ✓ FIs will provide information security personnel with security updates and training sufficient to address relevant security risks.
- ✓ FIs are required to verify that key information security personnel take measures to maintain current knowledge of changing cybersecurity threats and countermeasures.
- ✓ FIs must assess service providers based on the risk they present and the continued adequacy of safeguards.
- ✓ Incident response plans must incorporate notification and reporting requirements.
- ✓ At least annually, the CISO is obliged to report in writing to the board or equivalent governing body: 1) the overall status of information security program, the compliance with the safeguards rules; and 2) material matters relating to the information security program.

If the proposed rule is adopted as written, it will go into effect immediately after publication with the following exceptions to which a six-month grace period will apply:

- appointment of a CISO;
- written risk assessment;
- new elements to the information security program;
- continuous monitoring/annual penetration testing;
- required training for personnel;
- periodic assessment of service providers;
- written incident response plan; and
- annual written reports from the CISO to the board or governing body.

Moreover, FIs with fewer than 5,000 customers will be exempted from these tasks:

- written risk assessment;
- continuous monitoring or annual penetration testing, and biannual vulnerability scanning;
- written incident response plan; and
- annual written reports from the CISO.

Keep in mind the deadline for submitting formal comments is June 3. If you have related questions or would like to read the comments Bankers' Bank of the West will be submitting, please contact **techies@bbwest.com.**

Now Canadian imaging enabled.

Bankers' Bank of the West is pleased to confirm the availability of Canadian imaging, an often-requested service that's stirred up a lot of excitement—for good reason. A few of those reasons:

- Speeds up collection turnaround; avoids mail delay.
- Eliminates concern over the location or possible misplacement of physical items.
- Reduces mailing/shipping expenses.
- No additional processing cost beyond current cash letter fees.
- Often (though not always) banks can use scanners they already own.
- Items exchanged on BIDS are automatically scanned against the OFAC SDN list, simplifying compliance.

Either the full version of BIDS or BIDS Basic is required for Canadian imaging. To learn more or start the process of adding the service, contact your BBW cash management officer or email **ops@bbwest.com**.

Learn about 2019 payments rules.

Next in the series of WesPay training sessions open exclusively to BBW customers is the **2019 Payments Rules Update** on **May 3**. This highly recommended 90-minute webinar will inform your people of new and modified rules. To request the full 2019 course schedule and registration form, email **ops@bbwest.com**.

Just a reminder.

In March, NACHA announced the effective date for the new Same Day ACH processing window will be March 19, 2020. The full bulletin (#2-2019) is posted at **nacha.org** (see "NACHA and the ACH network" menu).

Supervisory practices during recovery from recent natural disasters

Jim Swanson ▪ Senior Vice President–Bank Strategies, a Division of Bankers' Bank of the West

In light of severe storms and resultant damage in portions of the Midwest, the federal banking regulatory agencies have issued new guidance and referenced existing guidance to help banks during the recovery. Guidance provisions are triggered by a presidential declaration of major disaster or emergency. Affected disaster areas are listed at **https://www.fema.gov/disasters**.

Under the guidance, banks working prudently to solve operational or customer-facing challenges will not be subject to regulatory criticism as part of their recovery efforts; they may be able to employ or receive relief from specific requirements. Several areas covered by the guidance are highlighted below:

- Providing potential relief from submission of regulatory reports (Call, FR Y-9C, etc.).
- Encouraging banks to use non-documentary methods to satisfy Customer Identification Program (CIP) requirements under the Bank Secrecy Act when access to normal identification records may be compromised.
- Waiving early withdrawal penalties on time deposits.
- Working constructively with borrowers having difficulties beyond their control due to damage caused by severe weather. This includes implementing prudent loan workout arrangements to extend terms or restructure obligations, waiving late fees, easing documentation requirements, and waiving real estate appraisal regulations for real estate-related loans involving properties in a disaster area.
- Receiving CRA consideration for activities that help revitalize or stabilize a designated disaster area.
- Providing flexibility for organizations having trouble meeting notification requirements for disaster-related branch closings, relocations, and requests to operate temporary banking facilities.
- Giving consumers an option to modify or waiver Regulation Z's three-day rescission requirement due to a "bona fide personal financial emergency."

Reach Jim Swanson at **303-903-9360**

For details, refer to the Federal Reserve SR letter 13-6, FDIC FIL letter-15-2019, or OCC NR 2019-31. You could also contact your regulatory agency to discuss specific questions or operational issues you've encountered.

Changes in Standards for Safeguarding Customer Information

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

On April 4, the Federal Trade Commission's proposed rule, Standards for Safeguarding Customer Information,* was published on the Federal Register for comments under Document 2019-04981.

Why this matters to community banks: The standards lay out provisions on how to implement specific aspects of information security programs for a covered financial institution.

The Commission is recommending changes to mandate more specific security requirements and effectively remove some of the flexibility of the Safeguards Rule currently in place.

A summary of new elements mandated under the FTC's proposed information security program:

- A single qualified individual will be responsible for overseeing and implementing the FI's security program and enforcing its information security program. The FI cannot designate more than one employee to coordinate the program; in addition, that single responsible individual will bear increased accountability. The designee may be an employee of the institution or an employee of an affiliate or a service provider. The title in the document is CISO.

- The information security program will be based on a risk assessment. The risk assessment will describe how the FI will mitigate or accept any identified risks and how the security program will address those risks specifically dealing with the security, confidentiality and integrity of information. The risk assessment needs to be periodically performed and reexamined.
- The FI must impose controls on all information systems for the purpose of permitting access only to authorized individuals.
- The FI must identify and manage the data, personnel, devices, systems, and facilities that enable the FI to achieve its business purposes in accordance with the business objectives and the risk strategy. This necessitates an understanding of all devices and networks that contain customer information, who has access to them, and how they are connected to each other and to external networks.

Continued on p. 4.

*Access the document and instructions for submitting formal comments at **https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information**

Bankers' Bank of the West
1099 18th Street ▪ Suite 2700
Denver, Colorado 80202