BBW News

a publication of Bankers' Bank of the West ▪ www.bbwest.com ▪ June 2011

A MESSAGE FROM THE PRESIDENT

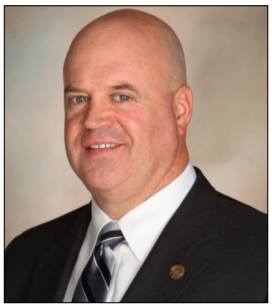
Communication, partnership, and headway in progress

LISTEN. According to Webster's New World College Dictionary, listen means "to pay close attention; take advice."

At Bankers' Bank of the West, we're listening closely when meeting with customers at their banks. As of the end of May, 60% of our 310 bank customers had received a visit at their office from a BBW representative. I'm confident that all customers will have been visited by year-end.

Why emphasize listening? Because you're the number-one authority on what your bank needs from us. We seek your advice on how we can help. Then it's up to us to pull together resources and create solutions that empower you to succeed.

In recent months we've heard that banks are looking for quality loans; that they're worried about evolving, complicated compliance requirements; that they want guidance on how to deal with the regulatory environment; and that some banks are still looking for capital.



Bill Mitchell
BBW President & CEO

Another idea we've heard repeatedly is this: Community banks need a partner to provide solutions that equip them to compete against the big banks—the institutions that always seem to avert the ultimate consequences of their actions.

Providing solutions that will keep community banks efficient and competitive is our prime objective. We'll keep listening—and, in response, deliver the efficiencies, product advancements, technology, and economies of scale you want from your correspondent partner. This has been the formula for our success over the past three decades, and it is our commitment to you now.

When BBW representatives visit your bank, they'll want to hear what's on your mind. They'll also update you on our continued progress toward asset resolution. Some points our officers may review in detail are:

1. BBW's classified assets were cut by one-third over the past 12 months. I believe we have a chance to eliminate another 25% of classified assets by year-end.

2. In the past 17 months, our risk-based capital has increased from just over 10% to 17%. Our leverage ratio reflects a similar increase.

3. Commercial real estate Levels 1 and 2 are now below the 100% and 300% regulatory targets.

4. Through May, we reported a 69 basis point return on average assets. While it's too early to project through December, we have a good chance to end the year profitably.

5. Our liquidity is strong and will remain strong.

6. Our ALLL remains above 6%.

Besides the positive developments above, I want to emphasize another message: BBW remains an active player in lending. Although the economy and regulatory environment have made it tougher to qualify for a participation purchase or direct loan today, rest assured we are more than capable of helping banks with quality credit requests.

We look forward to visiting with you and hope to hear you're enjoying your summer. Thank you for your business.

Inside

Taking note

Shareholder update

The annual meeting of shareholders of Bankers' Bank of the West Bancorp, Inc. (Bancorp) – the holding company for Bankers' Bank of the West – was held in Denver on April 15, 2011. **Brian D. Esch**, the outgoing chairman of the Bancorp board of directors, was succeeded by **Jeffrey C. Wallace**, the chief executive officer of Wyoming Bank & Trust in Cheyenne, Wyoming.

Sitting members of the Bancorp board welcomed Jeff to his new role and thanked the departing chairman with a plaque honoring his service. Brian Esch, president and CEO of McCook National Bank, is both a seasoned banker and an active supporter of his community through leadership, volunteerism and board service.

Information on ownership of the Bancorp, including book value and shareholder benefits, can be found at **bbwest.com**. The next meeting of shareholders is scheduled for April 20, 2012.

Operations, compliance and finance

This spring, 79 community bankers from Nebraska, Colorado, Wyoming, and New Mexico took part in BBW-sponsored Bank Operations Conferences held in Denver, Colo., and Kearney, Neb.

The educational sessions featured four national presenters with deep background in specific areas of interest to bankers with cashier, operations oversight, compliance, and finance responsibilities. In post-conference questionnaires, 95% of respondents said the experience met or exceeded their expectations.

All four conference presentation handouts, along with several white papers, articles on current lending issues, and resources pertaining to other bank functions have been compiled for distribution on CD/DVD.

That compilation is available at no charge, while supplies last, to BBW customer banks upon request from an officer from the institution (one per bank). Please submit requests to *info@bbwest.com*.

BBW News is published by Bankers' Bank of the West as a service to respondent banks. Online versions are available at **www.bbwest.com**. To receive electronically, email *info@bbwest.com*.

Send correspondence to:

Bankers' Bank of the West
Attention Jackie Tall
1099 Eighteenth Street, Ste. 2700
Denver, Colorado 80202
Or email ***jtall@bbwest.com***

Cautionary tale exemplifies need for ACH fraud deterrents

Tracy Hearson, Marketing Coordinator
LendingTools.com

What should have been a pleasant holiday break in 2008 for members of the Western Beaver County School District in Pennsylvania ended in a financial nightmare. District officials returned to work to find that during a four-day break, cyber-criminals had siphoned more than $700,000 out of two of the school district's bank accounts.

Western Beaver's financial institution, ESB Bank, was able to reverse some of the transfers, but the school district was out more than $441,000. Western Beaver subsequently sued ESB Bank in an effort to recover the remaining money.[1] At that point the nightmare became the bank's.

Cases like this are not unusual. According to the FBI, many online fraud cases involve small- to medium-sized businesses with accounts in local community banks.[2]

When the corporate account takeover was discovered, ESB Bank asked the typical questions. How could this have happened? How can it be prevented?

How could it happen?

A number of techniques are used to commit online fraud. Several involve installing a Trojan horse on a victim's computer to intercept personal information. In Western Beaver's case, perpetrators planted a virus on a computer to hack into the school board's computer system. Often malicious software lies inside the web browser, activating when the victim logs into a bank site. When Western Beaver logged into its account, password and account information was intercepted by the malware, thereby allowing the cyber-criminals to log in and initiate more than 74 transactions on 42 accounts.[3]

Following are two common methods used by criminals to install malicious software onto a victim's computer.

► **Phishing Scams**. An unsuspecting user is directed to a fake website through a link in an email or pop-up message. This "bait" often mimics a legitimate business that the targeted victim trusts or does business with—a bank, for instance. The message normally asks the target to verify an account. In responding to the request, the victim reveals the passwords and other sensitive information needed to access the account, and the criminals have the information needed to steal funds via ACH or wire.

► **Keyloggers**, also known as keystroke logging. Criminals place a Trojan horse on a computer to log the keystrokes typed by victims to access accounts. Keyloggers can be inadvertently downloaded through corrupted email message attachments or website links. Without intending to, employees of a business can download a virus from what they assume is a safe source.

How can it be prevented?

Education is essential to preventing online fraud. Your business customers need to know about potential dangers and learn how to mitigate risks. Simple practices, such as limiting Internet access and personal email in the workplace, can limit fraudulent access points. Some financial institutions require standalone computer terminals for business customers who access online accounts and initiate transactions.

Direct safeguards

Bankers' Bank of the West utilizes the correspondent gateway known as the Bankers Internet Data System to provide transaction services through a "Software as a Service" model. In collaboration with LendingTools.com (LTI), BBW has implemented multi-factor authentication for access to BIDS via biometrics. Deemed more secure than passwords, tokens, or other "strong"

Continued on next page

[1]"Crime in the U.S.: Preliminary Annual Uniform Crime Report 2009," U.S. Department of Justice, Federal Bureau of Investigation, September 2010.

[2]Linda McGlasson, "How to Beat Keyloggers," Bank Info Security article, October 11, 2010.

[3]Robert McMillan, "Cyber Attackers empty business accounts in minutes," IDG News Service, August 6, 2009.

Financial options imperative in difficult economic times

Tim Harder, Vice President, Vice President
1st Reverse Mortgage USA

Financial planning is crucial during periods of economic turmoil. The changes that occurred over the past two years have been earth-shattering for many people who thought they had everything covered. Certainly obtaining a reverse mortgage is only one of many financial options for older homeowners, but it can be an especially attractive possibility.

The main concern for people beyond middle age is usually liquidity. Like many Americans, they tend to be house-rich and cash-poor. While they might have enough cash to support themselves, they may not have enough to simultaneously support their parents and children, and absorb rising medical expenses besides. A reverse mortgage would provide them with ample cash to take care of their children until they are financially independent, and their parents in their later years.

Moreover, unlike other financial solutions, a reverse mortgage would allow primary borrowers to remain in the same property. Such an arrangement benefits the borrowers by offering them the flexibility to house multiple generations under the same roof. This can be critical for people wanting to help extended family through economic struggles because downsizing into a smaller home to free up cash may not be a realistic option.

In "A Deal That Could Save Your Parents" (MSN Money, March 9, 2011), personal-financial columnist Liz Weston notes:

"Tougher regulation, new restrictions on fees and a brand-new type of federally backed reverse mortgage that's substantially cheaper have made these loans better deals for more seniors. There's anecdotal evidence that reverse mortgages may be helping some older people avoid foreclosure, replacing unaffordable payments with a no-payment loan, said real estate columnist Tom Kelly, the author of The New Reverse Mortgage Formula."

The article by Weston goes on to say that Paul Lints, a 45-year-old private banker with PNC, is helping his 85-year-old father secure a reverse mortgage that will enable the dad to pay off his first mortgage, home equity loan, and substantial credit card debt.

Here Weston quotes Lints, the son: "My dad's been so strapped … and this will free up $3,000 to $4,000 a month for him, easy. … I told him, 'You worked your whole life. You've done everything a parent's supposed to do. … This is your money and your house.'"

Homeowners at least 62 years old who are facing financial difficulties should be educated on the benefits a reverse mortgage can provide.

To obtain more information about the turnkey reverse mortgage program available through 1st Reverse Mortgage USA, a Bankers' Bank of the West-endorsed service provider since 2008, call your BBW correspondent officer or email *info@bbwest.com*.

Cautionary tale exemplifies need for ACH fraud deterrents

Continued from previous page

authentication methods, biometrics can quickly and easily establish a user's identity.

Other online prevention tactics include monitoring and controlling ACH transactions at the end-user level. Make sure your online vendor software incorporates these additional safeguards to protect you and your business customers:

- Dollar limits on transactions
- SEC code limitations
- Dual controls ad the business level
- Email notifications of ACH file activity
- Complete activity reporting and monitoring
- Full transaction audit trails

LTI's ACH risk management solution incorporates the above safeguards to help you mitigate ACH risk. Also available is an ACH origination service for your business customers that will integrate into the BIDS system. To learn about these and other risk-mitigation tactics, contact any BBW cash management officer at **303-291-3700** soon: Your bank's money, time and reputation could be at stake.

To share with your merchant customers: Ten tips to help keep data safe

The following article is reprinted with permission from First Data Corporation. It is a list of suggestions only, and not intended to be an exhaustive or comprehensive list of data security tips. All trademarks, service marks and trade names referenced are the property of their respective owners.

Your customers expect you to keep their personal cardholder data safe—not an unreasonable expectation, and merchants must take it seriously. Such protection requires merchants to make an ongoing commitment to human and monetary resources, including new technologies, stronger polices and continuous diligence.

► Ensure your business is PCI DSS compliant.

The payment card industry (PCI) establishes and enforces security requirements for its constituents. Ongoing compliance with the PCI Data Security Standard (DSS) is the critical first step toward a successful data security program.

► Review how data is used in your payment system.

Before you can protect it, you must understand the ins and outs of the confidential data in your system:

- What data you have
- Where it resides
- Who is accessing your data
- When and how users access it

► Limit use and storage of sensitive cardholder data within your system.

Use your customers' personal cardholder data only for applications directly pertaining to payments (transaction authentication and daily settlements, for example).

► Minimize access to cardholders' data.

Limit access to customer information only to employees whose jobs require it. Do periodic spot checks to ensure procedures are being followed.

► Conduct detailed background checks before you hire.

Be selective about whom you hire; employees have the most access to your customers' data and systems. Forty-one percent of reported small business fraud in 2007 was committed by employees (National Small Business Administration Survey 2007).

► Make any necessary system changes.

You may have to update existing systems and implement new hardware and software, install firewalls, deploy data encryption technologies, implement data access controls, and track and monitor access to data and networks.

Consider implementing a layered data security approach such as the combination of encryption and tokenization that will allow you flexibility and a solid defense.

► Be on the lookout for signs of skimming.

There has recently been a tremendous rise in card-skimming fraud at the point-of-sale (POS). Skilled fraudsters can reconfigure a payment terminal by adding a skimming device in less than one minute. Payment terminals should be routinely inspected to ensure there have been no changes. Signs that your POS may have been compromised include:

- Changes in the screws or seams of the payment terminals, or unexplained scratches.
- A new or fake label or sticker that has been placed to hide a drill hole.
- Serial numbers that do not match between the payment terminal and the sticker.

► Pay attention to customers' buying behaviors.

Some things to look for include customers who:

- Purchase a large amount of merchandise without regard to size, style, color, or price.
- Don't ask questions on major purchases.
- Try to distract or rush you during the sale.
- Make purchases and leave the store but then return to make additional purchases.

Continued on next page

Check payments evolution prompts creation of National Check Professional Certification

Ellen Heffner, Director of Product Management
Electronic Check Clearing House Organization (ECCHO)

Findings published in "The 2010 Federal Reserve Payments Study" (December 2010) indicate that more than 96% of all checks are processed electronically. Added to this rapid growth in image exchange are the recent Federal Reserve consolidations of check processing locations resulting in one paper and one electronic processing location nationwide. Additionally, many new private sector options for check image exchange exist today. In this environment of change and complexity, it is easy to see that detailed knowledge of how to deal with specific check payment situations is becoming highly diversified—and frequently scarce.

Recognizing the need among industry participants to maintain check expertise, ECCHO is developing a new national program known as the National Check Payments Certification (NCPC). The goal of the NCPC Program, which will be administered by ECCHO, is to provide a certification for check payments professionals who demonstrate an expert level of knowledge across four key subject areas related to check payments: rules and regulations, check operations, check products, and fraud and risk mitigation. Candidates earning a passing grade on the certification exam will be awarded the National Check Professional (NCP) certification.

The NCPC examination will be generally available in the spring of 2012; it will include 120 questions based on the examination blueprint covering specific aspects of each of the four key subject areas. All tests will be offered through PSI LaserGrade, which offers proctored computer-based training facilities across the U.S. as well as several locations in Canada.

The examination questions are being developed through the efforts of a group of subject matter experts, known as the NCPC Editorial Board, drawn from organizations across the industry. The group is working with ECCHO to provide the expertise to build the initial program and maintain the NCPC program long-term. New training options being developed by ECCHO and its training partners will also be available to assist exam candidates in learning more about check-related processes, supporting regulatory requirements, and best practices for handling a variety of payment situations—knowledge that will help them prepare for the examination. After receiving NCP certification, certified check professionals will be required to meet defined continuing education requirements to maintain their certifications.

For more information on the certification, visit the NCPC page on the ECCHO website, **eccho.org/ncpc**. For details on pilot exam prep training or other ECCHO educational offerings, contact **Ellen Heffner**, ECCHO, at *eheffner@eccho.org* or 214-273-3221.

Ten tips for your merchant customers

Continued from previous page

- Make large purchases just after the store has opened or as the store is closing.
- Refuse free delivery for large items.

► Avoid falling victim to phishing scams.

Never click on links that ask for your personal or account information even if the e-mail message appears to be from your payment processor or financial institution. Always type the service provider's address directly into your web browser's address bar to access your account. If you believe you have been a victim of a phishing scam, change your online password immediately and contact your service provider.

► Don't stop now.

Data security is an ongoing responsibility. Frequently audit your payment acceptance practices and systems. Fraudsters are always looking for vulnerabilities and consistently changing tactics to stay ahead of the curve. You should be, too.

Taking proactive steps to keep your customers' sensitive data secure is not a luxury. It is a necessity.

To learn more about Bankers' Bank of the West's merchant programs, contact Mary Ann Elliott-Supples, msupples@bbwest.com.

Feedback and highlights from 2011 Bank Card Conference

The 2011 Bank Card Conference, held May 5 and 6, drew more than 80 bankers, 11 speakers, and a team of vendor-sponsors to the Embassy Suites Hotel in Denver.

A day before the official conference kickoff, early-arriving registrants had the opportunity to tour the CPI card production facility south of downtown Denver to see how cards are made. That afternoon, more than 50 bankers took part in training sessions conducted by longtime BBW employees **Jack Hitt** and **Bill Cruz**. Both sessions—one on merchant processing, and the other on ATM/debit—were rated "excellent" by more than 70% of training participants who complete feedback surveys.

The theme of the two-day conference was "It's a Jungle Out There: How to be a Lion in This New Era of Bank Card," a reference to shifting trends, emerging technology and yet-undefined regulatory environment that require banking professionals to stay current on bank card developments.

The program incorporated networking opportunities, 11 presentations by industry professionals, and scheduled times for banker-vendor interaction. More than 90% of survey respondents gave either a "good" or "excellent" rating to the range and depth of topics covered at the conference, and 93% gave the same high assessment to the importance of the presentations to their banks. One registrant remarked: "I was really impressed … The content was great and informative for me being brand new to these topics."

Speakers touched on a broad range of ideas, from cutting-edge technology to old-fashioned human differences in the workplace. Not surprisingly, a discussion by **Kim Hall** (vice president, First Data) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 drew an especially attentive and inquisitive audience.

With the outcome and timing of Durbin Amendment provisions being uncertain at the time of the conference, Kim offered insights into the interplay of legislative and judicial processes, some potential impacts of Durbin on community banks and consumers, and positions taken by interest groups. She concluded the bank card environment could remain in flux for some time yet.

As regulations take form and educational resources become available, the BBW Bank Card Division will work with its partners to share information and analyses with community banks. Visit **bbwest.com** periodically to check on relevant developments, webinars, and other educational resources.

Finally, be sure to send a representative from your bank to next year's event. To receive an "early alert" notice of the 2012 conference, send your request to *msupples@bbwest.com*.

Other federal activity on the radar screen

Americans for Disabilities Act Standards for ATMs

Became effective March 15, 2011
Compliance date March 15, 2012
Focal points:

- Installation of audio output elements
- Adjustments for height and reach

FDIC 2011 guidance on overdraft policies

Final guidance issued November 2011
Focal point:

- Requires banks to closely monitor automated programs, inform habitual overdraft users of alternatives, and permit opt-outs from non-electronic overdraft programs

More comments about the conference:

"The conference was an enjoyable and informative event... I would definitely recommend this conference to others."

"I learned lots and found the material to be very helpful."

"Current legislation and regulation information is always good."

Banks, bank employees cautioned regarding possible scheme

The Federal Bureau of Investigation has found information suggesting the existence of a fraud scheme aimed at bank employees and banks for the purpose of obtaining sensitive personal, bank, and bank security information.

The persons or group committing the scheme are believed to be capable of using deception and social engineering tactics to impersonate officials from a bank employee's own institution. A perpetrator might call a bank employee claiming to be a bank officer, often using the name of an actual bank officer, to assert an investigation has been launched. The perpetrator commonly instructs the employee to call a toll-free number (800 or 866 prefix) and to "confirm" sensitive personal information or bank security-related information such as PINs, passwords, or authorization codes related to funds transfers.

This scheme underscores the need for financial institutions to periodically review security procedures with their employees and reiterate the importance of never divulging sensitive information if the identity of the other person cannot be confirmed. Further, as criminals become more sophisticated, financial industry professionals should realize new methods of deception are bound to evolve.

Proper care and grooming of your online presence

When seeking information about businesses, Americans now turn to the Internet more often than to phone books or a brick-and-mortar library. This trend has motivated businesses of all sizes and kinds—including community banks—to carefully cultivate their online presence, which extends well beyond the corporate website.

Maintaining and controlling your bank's online presence might involve, among other things:

- Ensuring your address and contact details are kept current on search engine and review sites as well as other media;
- Checking social media and forums to read posts or articles about your business or employees;
- Verifying that no imposters or squatters are using social media or other sites to defame your company; and
- Creating the search engine optimization to drive customer traffic where it belongs.

The question is where to begin. A prudent first step is to establish your own business listing in Google. To help banks that have yet to get started, Bankers' Bank of the West has posted a step-by-step walkthrough on creating and editing your company's Google listing (available at **www.bbwest.com/seo1.pdf**). Be sure to check our website periodically as well for helpful hints on managing your bank's Internet presence.

Bankers' Bank of the West
1099 Eighteenth St. ▪ Ste. 2700
Denver, CO 80202