ALABAMA BANKERS ASSOCIATION

BOARDBRIEFS

A NEWSLETTER FOR ALABAMA'S BANK DIRECTORS

JANUARY/FEBRUARY 2016 • VOLUME 1 • NUMBER 1

IN THIS ISSUE

Potential Benefits of Your Bank Obtaining CDFI Certification

By Rob Carothers

In January 2014, banks began complying with a host of new mortgage-related regulations issued by the Consumer Financial Protection Bureau ("CFPB"), including a new regulation known as the Ability-to-Repay Rule ("ATR Rule"). The ATR Rule imposes a number of requirements on banks that make residential mortgage loans, and failure to follow these requirements can potentially result in liability imposed under the Truth In Lending Act. The ATR Rule creates a safe harbor from liability for loans that satisfy certain criteria (referred to as a "Qualified Mortgage"). This has resulted in many banks altering the types of mortgage products that they offer or otherwise taking on additional litigation risk.

For example, traditionally the balloon mortgage has been a staple of a community bank's loan products. However, under the ATR Rule, a Qualified Mortgage is generally not permitted to have a balloon feature. Thus, a bank offering a mortgage loan with a balloon feature enhances its litigation risk if the loan goes into default because it would not fall within the safe harbor. The ATR Rule does provide an exemption allowing a Qualified Mortgage to have a balloon feature if the bank has less than $2 billion in total assets, originated 2,000 or less mortgage loans during the previous calendar year, and at least 50 percent of its mortgage loans are made to borrowers located in a "rural or underserved" area. The problem with this exemption is that the CFPB's narrow definition of "rural or underserved" excluded many banks in Alabama from this exemption. In December 2015, Congress enacted legislation to broaden the "rural or underserved" criteria but it is yet to be determined what impact this will have when the CFPB issues implementing regulations. There is also a temporary exemption that allows for a balloon feature for certain small lenders (regardless of the rural/underserved criteria) which expires in April 2016.

A possible solution to this problem for many community banks in Alabama is to become certified as a community development financial institution (known as a CDFI) with the Department of the Treasury's CDFI Fund. The CFPB's regulations completely exempt mortgage loans made by certified CDFIs from the ATR Rule (other than restrictions on prepayment penalties). This would allow a bank to make a mortgage loan with a balloon feature without concerning itself with violating the ATR Rule or having to spend the time to determine whether it fits within the small creditor exemption. Further, regardless of whether the balloon feature is an issue for a bank, obtaining CDFI status will be a strong defense should a borrower bring a

lawsuit asserting a violation of the ATR Rule. The CFPB's Small Entity Compliance Guide states "a consumer who obtained a loan that was exempt from the ATR requirements would have no ability-to-repay claim under the ATR/QM rule." It is a safe bet that as loans made under the new ATR Rule begin to season and borrowers default, borrowers and their legal counsel will be quick to assert an ATR violation as a way of stalling foreclosure or negotiating with the lender in order to reduce the amount owed. A bank with a CDFI certification should be able to quickly dispose of any such allegation by citing the exemption and the CFPB's Small Entity Compliance Guide statement.

The process of becoming certified as a CDFI involves filing an application with the Treasury Department's CDFI Fund. There are six criteria that a bank must satisfy to become certified. Five of the six criteria are relatively easy to satisfy. The main issue is whether a bank makes at least 60 percent of its loans to borrowers residing in certain qualifying counties and census tracts. Many communities around the state of Alabama qualify (approximately 60 percent of Alabama counties qualify and many additional census tracts qualify). Currently there are 10 Alabama community banks that have obtained CDFI status. There are also a number of credit unions that have obtained CDFI status.

The feedback from our CDFI clients is that the reporting and monitoring requirements are not significant or burdensome. The CDFI Fund generally does not examine CDFI banks for eligibility compliance (particularly if they have not utilized CDFI status to obtain available grants).

An additional benefit of CDFI status is that it enhances a bank's ability to obtain Bank Enterprise Award grants (which are essentially awards for increasing loans in certain distressed communities). Community banks in Alabama received as much as $265,000 in BEA grants in 2015.

***Rob Carothers** is a partner in Jones Walker's Banking & Financial Services Practice Group whose practice is focused primarily in the area of financial institution regulation where he frequently assists bank clients on a wide range of matters including compliance with federal and state banking laws, mergers and acquisitions, and capital-raising transactions.*

Banks Must Prepare for Increased Cybersecurity Oversight

By W. Brad Neighbors, R. Alan Deer and Scott A. Gray

Bank board members and executives should begin 2016 with an important resolution: proactive oversight of cybersecurity risks. Few risk management events dominate today's news headlines quite like cybersecurity breaches, and for good reason — the fallout can be staggering. Fraudulent transactions, identity theft, angry customers, legal demands, reputational damage, and diversion of management and bank resources are just a few of the consequences that can flow from a cybersecurity breach. Additionally, legal uncertainty surrounding the application of general commercial policies to cover a cybersecurity breach means that banks may have to shoulder the resulting liability and expense. These risks are heightened for community banks. A 2014 study by the New York State Department of Financial Services revealed that smaller banks were less prepared to respond to a cyberattack than larger banks with more significant resources.

Fortunately, an increasing number of resources are available

to help banks of all sizes evaluate their cybersecurity risk. For example:

- The Federal Financial Institutions Examination Council ("FFIEC") has released its "Cybersecurity Assessment Tool." The tool incorporates cybersecurity-related principles from regulatory guidance and allows banks to analyze their cybersecurity risk by completing an Inherent Risk Profile and conducting an additional assessment of their "Cybersecurity Maturity," measured across five different domains.
- In addition to coordinating with the FFIEC to release the Cybersecurity Assessment Tool, the FDIC issued Financial Institution Letter No. 55-2015 in November 2015 outlining additional cybersecurity resources that it has made available as part of its Community Banking Initiative. It includes specific references to the FDIC's Cybersecurity Awareness Directors' College video, which provides an overview of cybersecurity threats and offers steps toward developing an effective cyber response plan in the event of an attack. The FDIC also has created the "Cyber Challenge," a series of exercises designed to encourage discussions between bank management and staff relating to cybersecurity awareness.
- The National Institute of Standards and Technology ("NIST") in the Department of Commerce has produced a cybersecurity framework that is meant to serve as a model for public and private entities. Although the guidance is voluntary, this guidance increasingly serves as a gold standard in cybersecurity preparedness.
- To assist banks with implementation of the NIST standards, the Conference of State Bank Supervisors ("CSBS") issued guidance in December 2014 entitled "Cybersecurity 101: A Resource Guide of Bank Executives," designed to help banks develop effective cybersecurity protocols.

This guidance is a clear signal of the heightened interest of regulators in banks' cybersecurity plans and the standards to which banks will be held. Indeed, in Financial Institution Letter No. 48-2015 released in October 2015, the FDIC called cybersecurity "one of the most significant issues facing the financial services sector."

Cybersecurity risks are not diminishing, as hackers of all stripes, from local individuals to foreign governments, eye the rich repository of customer data that banks possess. As bank regulators look to take increased oversight of cybersecurity protocols, so too should boards of directors and bank executives take affirmative steps to assess their bank's cybersecurity risks, develop a cybersecurity plan (including consideration of cybersecurity insurance policies or endorsements), and develop an effective communications strategy in the event of a cybersecurity breach. Although cybersecurity presents a challenge to all banks, and particularly to community banks, this challenge does not have to overwhelm bank boards and management teams. By taking advantage of regulatory guidance and assistance now available, banks may be able to provide greater protections to their customers and avoid examination criticisms and enforcement measures in the future.



W. Brad Neighbors *is a partner in the Birmingham office of Balch & Bingham where he represents banks and other financial institutions in transactional and regulatory compliance matters and regularly advises clients on privacy and data security issues.* ***R. Alan Deer*** *is also a partner in Balch's Birmingham office where he represents banks and other financial institutions in transactional and regulatory compliance matters and regularly advises clients in the area of corporate governance and board oversight.* ***Scott Gray*** *is an associate in Balch's Birmingham office and is a member of the Financial Services section.*

A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses

By Sarah Glover and J.T. Malatesta

In an environment where the term "data breach" has entered mainstream media and companies are being sued for the failure to exercise proper oversight of cybersecurity risks, all businesses, no matter the size, should strive to safeguard their sensitive data. Further, cybersecurity remains a top priority for financial regulators. Aside from the legal risk, it just makes good business sense. One important facet of a cybersecurity risk management program should be the mitigation of the risk presented by your vendors – both those that store sensitive data and those that have access to your computer systems.

Vendors are consistently cited as primary causes of data breaches, and third party involvement is the highest per capita contributor to the cost of a data breach. The Target, Home Depot, and recent T-Mobile data breaches were all vendor breaches. That is, a third-party service provider served as the initial access point to these organizations' customer data. These high-profile breaches, along with the heightened scrutiny of cyber risk management by regulators, emphasize the importance of including vendor management with your cyber risk management program. The problem is no longer one that can be left to the capable hands of information technology. It has become an enterprise risk management and corporate governance issue, prompting legal counsel, compliance officers, and executive management to join the risk mitigation efforts with respect to third-party service providers.

An effective risk management strategy involves oversight of the vendor throughout the life cycle of the relationship, from due diligence through termination. Guidance from the federal banking regulatory agencies sets forth the regulators' expectations with respect to the selection and monitoring of vendors. This article offers a framework designed to help companies comply with general regulatory guidelines as well as industry best practices, and can apply equally to the selection of new vendors or your assessment of existing vendors.

Phase 1: Due Diligence

Due diligence in selecting or reviewing vendors should be commensurate with both your organization's risk appetite and the nature of your relationship to the vendor. Consider a tiered approach to vendor management, whereby you categorize each vendor by data security risk to your business, taking into account the level and frequency of access to your systems and the volume and type of data you transmit to them. You can then tailor your oversight of the vendor to the vendor's risk profile. Examples of due diligence action items include assessing the financial soundness of the vendor, evaluating the vendor's information security and incident response programs, and asking for the results of the vendor's most recent independent security assessment.

Phase 2: Contract Negotiation

Risk-shifting in vendor agreements is quite common, especially in the technology field. However, given the increased pressure from regulators for businesses to perform intentional oversight of vendors, the traditional template vendor contract will likely change shape, allowing businesses more opportunity to negotiate provisions that mitigate their cybersecurity risk vis-à-vis vendors. Vendor relationships are often the product of multi-year contracts which must typically come up for renewal before new language and requirements can be negotiated, but consider asking for contractual amendments or addendums in the meantime. Contractual provisions that mitigate cyber risk include: requiring the vendor to name your organization as an additional insured on its cyber risk policy, an indemnification provision that covers internal investigation costs following a

data breach, and an exclusion to any limitation of liability if the vendor suffers a data breach.

Phase 3: Monitoring

As with the other phases of vendor management, the nature of any ongoing monitoring should align with the risk profile of the vendor. More extensive monitoring may be necessary for those vendors who pose the greatest risk to your organization. If resources allow, it would be beneficial to have dedicated personnel at your organization responsible for monitoring and evaluating the vendor's data security practices. You could also engage an independent consultant to perform this task. Ongoing monitoring of the vendor could include: ensuring that the vendor conducts regular security training for its employees, restricting and monitoring the vendor's access to your systems, and ensuring that any issues that arise during regular security audits are properly addressed.

The threat vendors pose to businesses is tangible. Fortunately, so are the steps a business can take to mitigate that threat. The key to vendor management – indeed any cybersecurity preparedness program – is deterrence; there is no guarantee that "doing everything right" will absolutely prevent a data breach, but implementing a comprehensive vendor management program is a formidable way to minimize cybersecurity risk to your organization.

J.T. Malatesta *is a shareholder with Maynard, Cooper & Gale, P.C., the chair of the firm's Cybersecurity Practice Group, and a frequent speaker on emerging issues in cybersecurity regulation and data breach litigation.* ***Sarah Glover*** *is an associate with the firm's Cybersecurity Practice Group whose practice focuses on incident response planning, vendor contract review, and data breach response and litigation.*

A look into the 2015 Verizon Data Breach Investigations Report

By Mike Morris

Now that 2015 has come to a close, we wanted to take a look at some of the things we learned relating to cyber security over the course of the year. And, one of the best places we found to get that information annually is the Verizon Data Breach Investigations Report. So, if you have not been able to read the full report yet, here is your chance to get a high-level look on what was covered.

For starters, we thought one of the most noteworthy statistics from the report was that 99.9 percent of all exploited vulnerabilities were compromised more than one year after the vulnerability was actually published. That means that even if significant time has passed after an incident and you may think you are in the clear that is typically not the case, so remember to be vigilant! Additionally, something we found surprising was that only about 23 percent of recipients are opening phishing emails and out of those, only 11 percent are actually clicking on the attachment. This is really good news! Our people seem to be more educated and are starting to better understand cyber threats. They are overall more aware and are doing their best to not put our businesses at risk.

Finally, in today's day and age, as everyone is glued to their mobile devices, the report actually found that these devices were not the preferred vector in data breaches. Everyone really thought this would be the year that more mobile devices would be attacked, and that was not the case. That's good news for phone lovers everywhere – at least for now! In addition to some prominent data, the report points out that your weakest links – which are internal users and corporate cash management customers – are your most vulnerable targets. So it is important to understand what solid controls are and how you can better protect yourself against these types of attacks. During the course of our IT audit work, we have seen many factors that have led to an increased risk of cyber breaches and our findings seem to jive well with what was pointed out in the report. A few of which are listed below:

1. **Lack of email filters** – especially as people started to move over to Microsoft 365 and other cloud-based systems. Those were not designed for security because they have such a wide audience of users. It's important that you get in there and set those email filters to block a lot of these attachments.
2. **Lack of education** – many of the susceptible areas we have found are the same areas of weakness within the organization as it related to education and training amongst internal users. So, make sure to educate your people! You know as they say, an ounce of prevention is worth a pound of cure!
3. **Weak surf controls** – which are spotted by looking at reports that show where people are going on the website, and what type of websites they're visiting. Make sure to tighten up your surf controls on your

machines and only allow access to websites that are absolutely necessary for your people to perform their jobs!

4. **Local administrative rights** – Offering local administrative rights to your internal users gives a much stronger foothold to be able to infect those machines – this is not a practice we would recommend! If your internal users do have local administrative rights, consider revoking them. Unfortunately, it can take some beta testing to get your applications to work correctly, but it can be done

5. **Relying solely on anti-virus at the endpoints** – while this used to be acceptable measure to prevent a cyber-incident, that's no longer the case. We need to look at layered security and be sure we have more measures in place than just that good ole' anti-virus!

6. **Slow response time** – not remediating internal vulnerabilities in a timely manner could have serious pitfalls as well. Even though we pointed out that 99.9 percent of all exploited vulnerabilities were compromised more than one year after the vulnerability was actually published, it is still imperative to stay on top of all vulnerabilities and release patches as quickly as possible.

7. **Lack of application white listing** – Application whitelisting is a computer administration practice used to prevent unauthorized programs from running to protect computers and networks from harmful applications. If you have not done so already, you should strongly consider implementing application white listing on all employee computers.

In addition to everything mentioned above, another area for concern is eBanking services. These are your customer endpoints, and there is risk where any large dollar amount leaves the bank. Also you don't control the computers that initiate these transactions. But unfortunately, hackers can, and they will.

Luckily, there are controls for eBanking:

- First, make sure you're using multi-factor authentication for customers which most eBanking providers have available. You also want to look at "out-of-band verification" so that you can give a onetime password to a cell phone.
- Next, make sure you're putting fraud detection and monitoring systems in place by looking for higher than normal activities or a number of transactions. Then look for a pattern of things that look suspicious which will give you the opportunity to make a decision before the money actually leaves the bank.
- Finally, you have to make sure you're doing employee security awareness as well as customer security awareness training. It is good practice, and you can be a trusted advisor for your customers by helping them understand the risk through different transactions.

Mike Morris *is a systems partner at Porter Keadle Moore, specializing in IT, cybersecurity and risk advisory services for community banks.*

A Walk Down Memory Lane: 2015 Bank M&A Scorecard

By Michael Rediker

In the bank merger and acquisition arena, 2015 saw 284 deals nationally (essentially flat from 2014) and 63 deals regionally (up from 56 in 2014). Deal pricing in 2015 was also up slightly over 2014. Does this mean we are in an M&A boom? To answer this question, we believe it is insufficient to compare 2015 solely with 2014 or even the last five years, but necessary instead to travel back in time and look at 2015 in the context of the last quarter century.

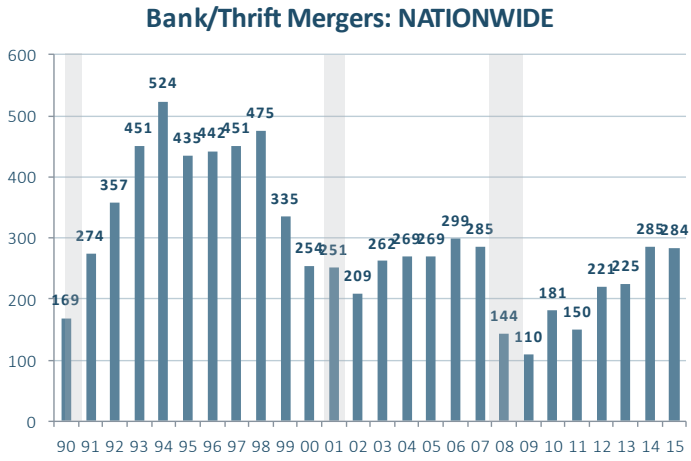
At First Glance, Deal Activity Looks Ho-Hum

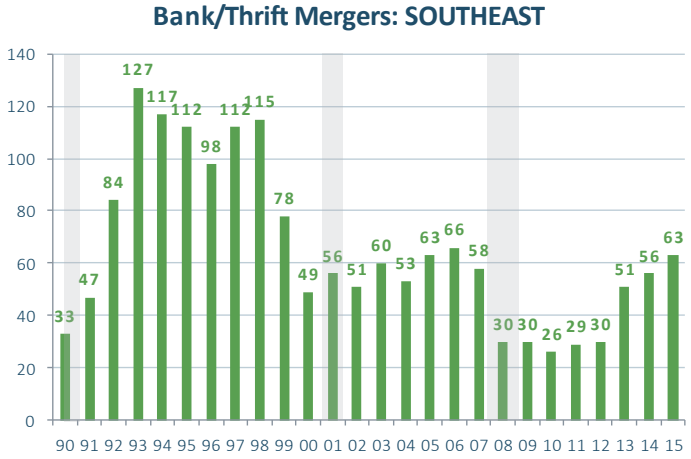
In pure raw numbers, while 2015 was flat (U.S.) to slightly up (southeast) over 2014, it still trails the 1990s when there were routinely over 400 deals nationally (1994 saw 524 deals!). At first glance this implies that deal activity, while noticeably up following the Great Recession, is "off the pace" historically.

Upon Second Look, Deal Activity is ROBUST

However, simply viewing 2015's raw deal count against the 90s is not an "apples-to-apples" comparison because there are less than half the banks today than there were in the early 90s; today there are approximately 6,200 institutions in the U.S. while in 1990 there were roughly 15,000. In other words, we need to look on a relative basis to see if 2015 was depressed by historical standards. We illustrated this in the chart by dividing the number of deals in a given year by the average total institutions in the same year (to calculate average total institutions, we averaged the total institutions at Dec. 31 of a given year with total institutions at Dec. 31 of the prior year).

Upon second glance, 2015 deal activity in relative terms was the highest nationally (4.44 percent of average total banks) in any year going back to 1990 and the highest since 1998 for the southeast (5.83 percent of average total banks).





Note: *All chart data courtesy of SNL Financial or FDIC.*

- *Grey bars represent recessions (Jul90-Mar91; Mar01-Nov01; and Dec07-Mar09).*
- *Southeast: AL, AR, FL, GA, MS, NC, SC, TN, VA and WV.*

What About Deal Pricing?

Does this mean the boom is really here? The answer is "partially." Our preceding chart established that, yes, relative deal activity in 2015 was robust by historical standards. However, activity must be separated from pricing to get a full answer. When looking at pricing in bank mergers, 2015 paled in comparison to most of the last quarter century.

The charts to the right show that the nosedive in pricing around the 2001 recession was pronounced, but that it was nowhere near as severe as the Great Recession (Dec. 2007 to March 2009). Deal pricing in 2015, while up over the 2009-14 period, has only returned to early 1990s levels.

Comparing the post-2009 recession period with the two previous post-recession periods reinforces that we have a long way to the "boom" from a pricing standpoint.

Pricing following the 1990-91 recession topped out in 1998 at Price/Tangible Book of 2.56x (U.S.) to 3.00x (southeast) and Price/Deposits of 28.5 percent (U.S.) to 33 percent (southeast).

Pricing following the 2001 recession topped out in 2006 at Price/Tangible Book of 2.25x (U.S.) to 2.40x (southeast) and Price/Deposits of 25.7 percent (U.S.) to 28.5 percent (southeast).

Comparatively, pricing in 2015 were a median Price/Tangible Book of 1.40x (U.S.) to 1.43x (southeast) and a median Price/Deposits of 17.0 percent (U.S.) to 17.5 percent (southeast).

Demonstrating the severity of the latest (and "greatest") recession, we are six years into the recovery yet 2015 prices were clearly well off the pace of the previous two post-recession periods.

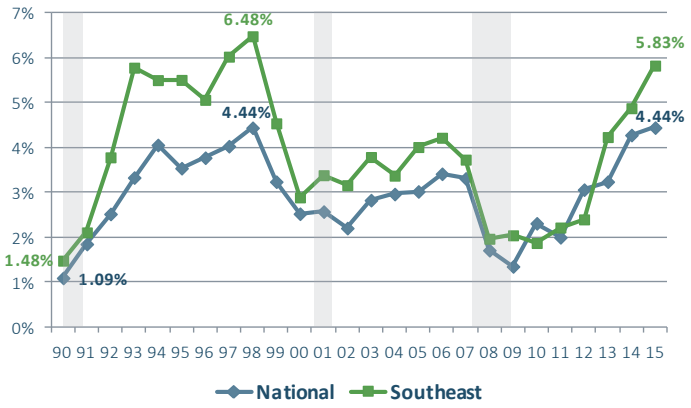
A final interesting observation from the pricing charts is the "boom or bust" pricing of southeastern deals in relation to deals nationally, where deals in the southeast have shown "higher highs" than deals nationally (e.g., 1998) but have also demonstrated "lower lows" (e.g., 2011).

The Jury is Still Out

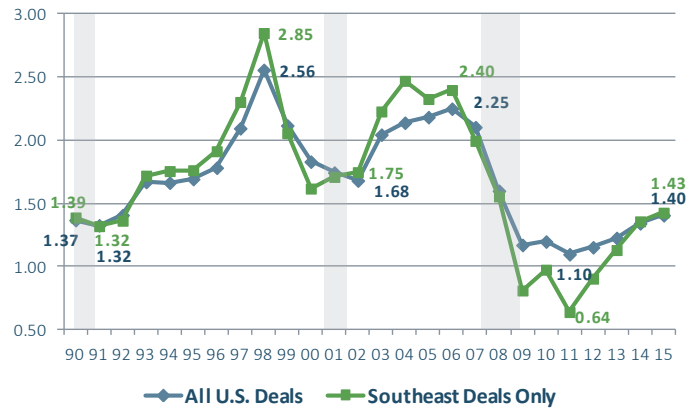
Our journey back in time has yielded conflicting results. On one hand, 2015 saw robust deal activity (in relative terms) by historical standards. On the other hand, deal pricing in 2015 fell far short of historical standards, specifically post-recession pricing. Without robust activity AND pricing, it is probably premature to declare an M&A "boom." If 2016 sees higher deal prices in conjunction with continued high relative deal activity, we can likely say the verdict is in and declare the "boom" upon us.

***Michael G. Rediker**, CFA is an investment banker with Porter White & Company in Birmingham. He routinely provides M&A and other advisory services to community banks across Alabama.*

Mergers to Average Total Institutions

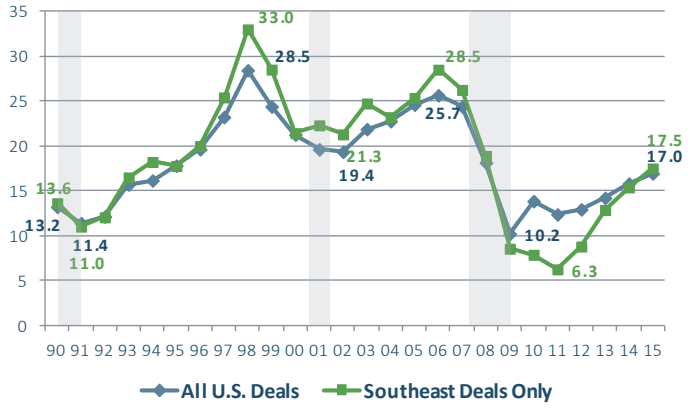


Median Price / Tangible Book (x)



- *Grey bars represent recessions (Jul90-Mar91; Mar01-Nov01; and Dec07-Mar09).*
- *Percentages calculated by dividing mergers in a given year by average total institutions of the same year.*
- *Southeast: AL, AR, FL, GA, MS, NC, SC, TN, VA and WV.*

Median Price / Deposits (%)



- *Grey bars represent recessions (Jul90-Mar91; Mar01-Nov01; and Dec07-Mar09).*
- *Southeast: AL, AR, FL, GA, MS, NC, SC, TN, VA and WV.*

FDIC Advisory on Risk Management Practices for Purchased Loans and Loan Participations

By Jeff Powell

On November 6, 2015, the FDIC issued advisory letter FIL-49-2015 that describes effective risk management practices for purchased loans and loan participations. The FDIC acknowledges that banks may receive certain benefits from the purchase of loans or loan participations, such as achieving growth goals, diversifying credit risk and deploying excess liquidity; however, banks have occasionally faced significant credit losses or even failures, which typically have been due to the over-reliance of the lead bank or third party providers. The FDIC notes that loans to out-of-territory borrowers or borrowers in unfamiliar industries have created particular risks to many banks in the past.

The FDIC recommends the following practices and protections to ensure that purchased loans and loan participations are conducted in a safe and sound manner:

- **Loan Policies** – Banks should create and utilize loan policies for purchased loans and loan participations. The loan policies should outline the procedures for review and approval of purchased and participation loans: define acceptable loan types; establish concentration limits (per borrower, per lead lender, per out-of-territory areas, per business type, etc.); require independent credit and collateral analysis for each transaction; and establish credit underwriting and administration requirements that address the risks and characteristics unique to the loan types purchased.
- **Independent Credit and Collateral Analysis** – Banks should perform the same degree of independent credit and collateral analysis for purchased loans and loan participations as if they were the originating bank.
- **Profit Analysis** – Banks should conduct a profitability analysis of purchased loans and participation activity relative to the rate of return and determine whether the rate of return is commensurate with the level of risk taken.
- **Legal Agreements** - All loan sale or participations agreements should fully set forth the roles and responsibilities of all parties to the agreement and define the rights of the purchasing bank to receive timely information and reports, address remedies upon default and bankruptcy, specify voting rights between the banks, and outline dispute resolution procedures. In particular, the FDIC emphasized that the legal agreement should clearly state any obligations to make additional credit advances, as well as the process regarding all credit decisions if the loan goes into default.
- **Due Diligence and Monitoring** – Banks should use caution and perform extensive due diligence and monitoring when purchasing participations involving out-of-territory loans or borrowers in an unfamiliar industry. In addition, banks should perform due diligence, including a financial analysis, prior to entering into a third-party relationship to determine whether the third party has the capacity to meet its obligations to the purchasing bank. The responsibility to perform appropriate due diligence cannot be outsourced.
- **Audit** – Banks should make sure that purchased loans

and loan participations are included in their audit and loan review programs.

All banks should review Financial Institution Letter 49-2015 and establish updated policies and procedures to comply with these new guidelines, as applicable. Although the FDIC acknowledges the benefits of loan purchases and participations, banks must take appropriate steps to properly underwrite and administer such loan purchases.

Jeff Powell *is a member of Bradley Arant Boult Cummings' Banking and Financial Services Practice Group and is focused on advising financial institutions on corporate, compliance, operational and regulatory matters.*

Selling Stock Through the President's Desk Drawer

By Beth Sims

Look inside the desk drawers of many Alabama community bank presidents and you will find a list of the names of individuals who want to buy or sell the bank's stock. Bank lawyers get asked about these "desk drawer" lists on occasion (often preceded by caveats like: "I'm not sure if this is a great idea but…").

On one hand, all bankers want to provide shareholders with value and service. On the other hand, you don't need to be a securities lawyer to sense that a desk drawer list has the potential for abuse by unscrupulous company insiders or that the list of laws that might apply to a desk drawer system is long. So while these desk drawer lists are a common practice among community banks, they do pose a legal risk to even the most scrupulous and careful presidents who administer them.

Best Practices

If you want to have a desk drawer list of potential buyers or sellers, proceed carefully and follow some best practices, including:

- Keep your involvement to "clerical and ministerial" functions only.
- Potential buyers and sellers should contact each other directly; you should not be involved in communications between the parties.
- The price for the stock should be negotiated by the parties and not you.
- Have a board-approved policy in place for responding to the inevitable question, "What do you think my stock is worth?" Refer potential buyers and sellers to the bank's call reports, audit, or a board-authorized valuation by an independent third party, and encourage potential sellers and buyers to talk to their own advisers.
- You should never handle funds or be involved in payment for securities bought or sold after being matched through the desk drawer.
- Directors, officers, and employees (including and especially you) should never profit from the desk drawer system or receive compensation based on connections made from the desk drawer.
- Directors, officers, and employees (including and especially you) should not be involved with buying or selling stock through the desk drawer. If an insider wants to purchase or sell stock through the desk drawer, talk to counsel first.
- Transactions from the desk drawer should remain occasional and isolated. If the practice becomes common, it may be time to evaluate whether a better, safer system exists, such as the over-the-counter market or a stock repurchase plan.

This is not meant to be a bulletproof checklist, but rather some best practices that might make the desk drawer system less likely to subject you to broker-dealer regulation and/or penalties under securities laws.

Consequences of Violating the Law

There are serious potential consequences to acting as an unregistered broker-dealer, both to you and to the bank. Individually, if you act as an unregistered broker-dealer in Alabama, you could face fines and penalties from the Alabama Securities Commission and federal authorities. Additionally, you face potential liability in court from the buyers or sellers that you matched. Section 29(b) of the Securities Exchange Act of 1934 renders void any contract made in violation of that act or its rule and regulations. Arguably, this provision gives the parties to a transaction arranged by an unregistered broker-dealer a right to void the transaction agreements and unwind transactions that have previously closed. In other words, if you involve yourself too heavily in a desk drawer transaction (or worse, use the desk drawer to buy/sell stock individually), the innocent parties may have the right to unwind the transaction because the transaction was arranged by an unregistered broker-dealer.

For the bank, the use of an unregistered broker-dealer in a transaction could cause the bank to lose any exemption from the registration requirements of the Securities Act of 1933 (as well as from applicable Alabama qualification requirements). Accordingly, the bank may have a difficult time obtaining a legal opinion from its counsel in connection with a future stock offering. It also may subject the bank to civil and criminal penalties, including pursuant to Section 20(e) of the Exchange Act on the theory that the bank aided or abetted the unregistered broker-dealer. Finally, the SEC may bar the bank from conducting private placement offerings in the future, thereby risking its ability to raise capital.

Insiders and the Desk Drawer

Directors and officers buying or selling stock through the desk drawer raises particularly complicated issues. Any time anyone buys or sells stock in any American company (whether public or private) on the basis of material "inside" information that is not publically known, it is a violation of Rule 10b-5. Breaking that rule is what sent Martha Stewart to jail, and it is a common cause of action in cases by disgruntled buyers/sellers on the theory that the insider-party had material information that he or she did not disclose. Because directors and officers frequently know material, nonpublic information about the company, insiders should always be cautious when conducting a transaction in that company's stock. Insiders should certainly never use the desk drawer to "buy low and sell high." Also, the desk drawer should never be used to send a good deal to a friendly insider at the expense of a non-insider. Any manipulation of the desk drawer in that way could expose the bank and the insider to liability, and perhaps even criminal penalties. In addition to Rule 10b-5 issues, there may be state and federal securities law restrictions on the sale of stock by insiders. To summarize a very complicated topic: contact counsel before insiders buy or sell stock, especially if those insiders have passed through the desk drawer.

Beth Sims *is a partner at Butler Snow LLP where she counsels public and private financial institutions on a variety of corporate and securities issues, including equity and debt financings, corporate governance, and public company disclosure matters.*

Board Briefs *is published six times a year by the Alabama Bankers Association.*
Questions? *Call us at (334) 244-9456.*
Visit ABA online at ***www.alabamabankers.com***