ALABAMA BANKERS ASSOCIATION

BOARD**BRIEFS**

A NEWSLETTER FOR ALABAMA'S BANK DIRECTORS

NOVEMBER/DECEMBER 2018 • VOLUME 3 • NUMBER 6

IN THIS ISSUE

Know Your Cybersecurity Providers
Elena A. Lovoy, *McGlinchey Stafford*

A Matter of Value
Nancy A. Bush, CFA, *NAB Research for Banks Street Partners, LLC*

Preparing to Overcome Problems in Bank M&A Transactions
Michael G. Rediker, *Porter White & Co.*

Vendor Risk Management: It's More Than a Checklist
Terry Ammons, *Porter Keadle Moore*

What the Midterms Mean for Community Banks
Brian Malcom, *Waller*

Getting the Debtor's Name Right on the UCC-1 is Important
Laurence Vinson, *Bradley*

Virtual Currency Regulation: What Do Alabama Bankers Need to Know?
Erica Barnes, *Maynard Cooper & Gale*

Know Your Cybersecurity Providers

FFIEC Issues Alert Reminding Financial Institutions of OFAC's Cyber-Related Sanctions Program

by Elena A. Lovoy, McGlinchey Stafford

Although investments in information security have reached an all-time high, successful cyberattacks on financial institutions continue to increase. As innovations in technology drive new strategic initiatives at financial institutions, these innovations also open new doors for cyber-criminals. The increasing reliance on third-party service providers, who in turn use a myriad number of sub-providers, to provide these enhanced technology options also means that a financial institution's cybersecurity and vendor risk management programs must be able to effectively and proactively measure and respond to these ever-changing risks to protect the financial institution's digital fortress. One of the risks that should be addressed in any state-of the-art cyber-risk management program is a vintage compliance issue.

What is the Cyber-related Sanctions Program?

On Nov. 5, the Federal Financial Institutions Examination Council (FFIEC) issued a joint statement (Joint Statement) reminding financial institutions of the risks of entering into transactions or maintaining relationships with entities identified in the cyber-related sanctions list maintained by the Office of Foreign Assets Control (OFAC). The Cyber-Related Sanctions Program was implemented by OFAC on April 1, 2015 in response to Executive Order 13694, as amended on Dec. 29, 2016, to address the threat to the national security, foreign policy, and economy of the United States from the increasing prevalence and severity of malicious cyber-enabled activities originating from, or directed by, entities located, in whole or in substantial part, outside the United States.

OFAC has issued sanctions against entities who are responsible for, are complicit in, or that have engaged in, certain malicious cyber-enabled activities, including by providing material and technological support to malicious cyber-actors that have targeted organizations in the United States. In the Joint Statement, the FFIEC noted that some of these sanctioned entities claim that they are based in the United States and offer their services to financial institutions.

How does the Cyber-related Sanctions Program Impact Vendor Relationships and Transactions?

The OFAC compliance requirements, which have been in place for decades, have not changed. United States persons (and persons otherwise subject to OFAC jurisdiction), including financial institutions, must ensure that they are not engaging in trade or other transactions with any sanctioned person or entity. This includes any person or entity named on OFAC's Specially Designated Nationals List (SDN List) pursuant to Executive Order 13694, as amended.

The FFIEC noted that this broad prohibition on transactions with a sanctioned entity would even extend to certain routine information technology transactions, such as the download of a software patch from a sanctioned entity. The continued use of products or services from a sanctioned entity, directly or indirectly through a third-party service provider, may increase operational and OFAC compliance risk for a financial institution and result in violations of law, the imposition of civil money penalties, possible enforcement actions, and damage to a financial institution's reputation.

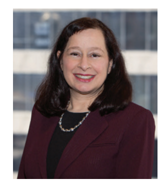
What should a Financial Institution do to Ensure its Cyber-risk and Vendor Management Programs Incorporate OFAC's Cyber-Related Sanctions Program Requirements?

Financial institutions should develop a tailored, risk-based OFAC compliance program, which includes sanctions list screening and other appropriate measures. OFAC has noted that "[a]n adequate compliance solution will depend on a variety of factors, including the type of business involved, and there is no single compliance program or solution suitable for every circumstance."

Cyber-criminals, whether sanctioned persons or entities, may use social engineering or target vulnerabilities in security software to gain access to sensitive network infrastructure areas at financial institutions or to devices that allow access to such networks. As part of its cyber-risk management program, a financial institution should identify these potential vulnerabilities and adopt measures to ensure that data is protected, including programs that block malware. The Joint Statement reminds financial institutions that cyber-risks can also come from any sanctioned persons or entities so institutions should assess their individual OFAC sanctions compliance risks, identify potentially impacted relationships and transactions, ensure that their sanctions screening systems are updated, and confirm that they have processes and procedures in place to comply with the sanctions. The FFIEC noted that addressing the risks from possible transactions with sanctioned entities "requires a high degree of collaboration across a financial institution's OFAC compliance, fraud, security, IT, third-party risk management, and risk functions."

A financial institution should assess the risk of having or continuing to use software or services from a sanctioned entity and take appropriate corrective action. Since third-party service providers, or their sub-providers, may also be using the products or services of a sanctioned entity, a financial institution should ensure that it understands how its third-party service providers ensure compliance with the OFAC requirements. The FFIEC noted that if a financial institution is obtaining a critical service from a sanctioned entity and that service cannot be immediately replaced; it should be replaced "at the earliest possible time."

Although the Joint Statement does not impose any new regulatory requirements and was issued by the FFIEC for informational purposes only, it serves a reminder to financial institutions that cyber-risks can come from many different sources. The Joint Statement also highlights the interconnectivity of an institution's cyber-risk, vendor management, and OFAC compliance programs. Compliance programs that remain in a silo may present OFAC-related compliance and other operational risks. Although Trickbot banking Trojan modules, ATM Jackpotting, Quakbot malware variants, WannaCry, and similar catchy cyber-names may grab the headlines, sometimes compliance is simply cross-functional and old-fashioned. Don't let cyber-criminals in the front or back door; check the SDN List.



Elena A. Lovoy is of counsel in the Birmingham office of McGlinchey Stafford and concentrates her practice in privacy and cybersecurity issues impacting financial services and other companies. She routinely assists companies in the management of data privacy incident responses and operationalizing global, federal, and state privacy requirements. She also focuses on banking, mortgage lending and servicing, and consumer financial services regulatory compliance matters at both the federal and state levels. She can be reached by email at elovoy@mcglinchey.com or by telephone at (205) 725-6407.

A Matter of Value

by Nancy A. Bush, CFA, NAB Research, LLC, Distributed by Banks Street Partners, LLC

With profuse apologies to T.S. Eliot, April is NOT the cruelest month. As any Wall Streeter—or indeed, any investor—knows, that ignominious descriptor belongs to the month of October, which is the period in which stocks generally get clobbered. That is a historical fact dating back to October 1929, when the first real market crash of the modern era began, resulting in a decline that went on for years and gradually reduced the stock market to a paltry 10 percent of its pre-crash level.

The October that has just passed was not that bad, but it was no barrel of monkeys either, and it was particularly cruel to our group of bank stocks. Of the 18 Southeastern banks that we monitor, only two—BB&T Corp. (BBT) and Wells Fargo & Co. (WFC), ironically—did not go down during the month of October, and price declines in the rest of our surveyed stocks ranged from 6.1 percent for Ameris Bancorp (ABCB) to a whopping 18 percent for Synovus Financial Corp. (SNV), which is obviously still battling the FCB Financial Holdings (FCB) merger blues. This markedly subpar performance was particularly noteworthy given the fact that the BKX (KBW Nasdaq Bank Index) declined "only" 5.7 percent in October, outperforming the 6.9 percent decline for the S&P 500.

But now that it's early December and the midterm elections are thankfully behind us (without disastrous effect, so far), is it time to treat the experience of October as ancient history and take a new look at these companies? We believe so. There has, after all, been an aura of doom and gloom hanging over the bank stocks for some time now, mostly due to the realization on the part of the markets that the Fed would be true to its word in pursuing a course of "normalization," no matter how many rate increases that might take. The resultant rising costs of deposits for the banks—especially for some of the smaller banks in competitive markets—has become an issue of concern for investors, as has the high level of loan payoffs and the resultant subdued pace of lending activity.

It strikes us that it may be time to drag out an old concept regarding the bank stocks—that of value investing, and indeed whether these stocks may qualify as "value" stocks. And for those who might need a reminder on what value investing is, we quote that unimpeachable source, Investopedia: "Value investing is an investment strategy where stocks are selected that trade for less than their intrinsic values. Value investors actively seek stocks they believe the market has undervalued... Typically, value investors seek to profit off this irrationality by selecting stocks with lower-than-average price-to-book ratios, lower-than-average price-to-earnings ratios and/or higher dividend yields."

We will readily admit that applying the concept of value investing to bank stocks in the past has often been a fool's errand, despite the success achieved by such legendary investors as Peter Lynch and Warren Buffett in championing some of these stocks. Mr. Buffett particularly has made billions on buying stakes in banks when they are down—his purchase of a preferred stock from Bank of America Corp. (BAC) in the wake of the Financial Crisis netted him billions a few years ago as BAC and its stock strongly recovered—and he has continued to stand behind his holdings of Wells Fargo's stock even in the face of its well-known challenges to its reputation and profitability. These two exemplary investors have historically seen something in bank stocks that has eluded others and they have been (mostly) handsomely repaid for their vision, and admittedly for their timing as well.

The problem with value investing in bank stocks is contained within the word "intrinsic;" we would admit that intrinsic value is a quality that may be in the eye of the bank stock beholder. Banks are, after all, largely opaque pools of assets that may be of varied quality and whose ultimate performance characteristics may not be fully known at the time of investment. The real value of any bank and its portfolio tend to become known only in times of stress, when the disposition of those assets may come at a steep discount and thus future cash flows are stressed and are likely to decline.

The change in the regulatory regime in the last decade has been such that those negative events—sudden deterioration of asset quality and declines in expected cash flows—have become much less likely than in the run-up to the Financial Crisis, and thus our thought that value investing may (finally) be a concept that is truly applicable to the bank stocks. In our view, the focus on asset quality (enforced through the various stress-testing regimens) and the requirement for strong levels of core deposit liquidity have made much less likely the sudden deteriorations that have been a feature of the banking industry in the past and have given the concept of "value" in banking stocks a decidedly dubious past.

Do these select Southeastern stocks represent a value opportunity now? They are selling at a collective P/E multiple of roughly 75 percent of the S&P 500's P/E multiple, based on the Street's consensus estimates for 2019. While this is not bargain basement cheap, it is inexpensive relative to the 85-90 percent relative valuation of recent months and seems to us to be overly punitive based upon recent earnings trends and future earnings potential. Trends in 3Q18 earnings results were certainly better than respectable and pointed to building momentum in lending volumes—which have been adversely impacted by a high level of loan payoffs in the last two quarters—and a cooling impact of deposit pricing competition on net interest margins. And best of all, the traditional killer of bank stock valuations—deteriorating credit quality—has reared its ugly head in only a few specific (and predictable) instances and in the higher quality banks is notably absent.

How about dividends? As an investor who invests first and foremost for cash flow, we must admit that this group of stocks looks particularly attractive. The problem with buying bank stocks for dividend income and dividend growth has been the tendency of banks to crash and burn (due to a credit quality and liquidity crisis) every decade or so and to cut (or omit) their dividends as a result. In this regard, the rigor of the stress-tests for the major banks and the degree of regulatory oversight for the industry generally has served to keep dividend growth to sane and sustainable levels and to ensure that dividends will remain uninterrupted in coming years.

While we concede that it may take a few more years for the investing public to believe that bank stocks are trustworthy dividend growth stories, we do believe that the likelihood of that happening is greater than at any time in our career. We would also point to attractive dividend yields—in the 3-percent-plus range—for major Southeastern companies like BB&T (3.3 percent) and SunTrust Banks Inc. (STI) (3.2 percent) as being particularly attractive presently, and the dividend yields of growth banks such as United Community Banks (UCBI) and Synovus (2.4 percent and 2.6 percent, respectively) to be also worthy of note.

Perhaps it is best to characterize our view of this group of Southeastern stocks as "value-specific" investing, as there are those that we monitor who are dealing with issues of past strategies and disadvantageous competitive positions that are yet to be overcome. But when we look at some stocks in this group, it is hard to see anything other than histories of high credit quality, conservative management and judicious and measured deal-doing, and we think that the present atmosphere of investor indifference has created attractive opportunities in these names.

Let us close with a look at a company that ticks all those boxes—that of South State Corp. (SSB), which is one of the Southeastern growth banks that we most admire. This company encompasses the credit quality discipline of the old Wachovia (the one headed by John Medlin), the attractiveness of strong fee-based businesses (fiduciary and asset management), and thoughtful and careful mergers, most recently Park Sterling in Charlotte, NC. For all this quality, investors would pay roughly 1.9x tangible book value, 12x next year's earnings, and receive a dividend (recently increased) of $1.44 per share (for a 2.0 percent yield.) Well—what's not to like about that?

To read NAB Research's disclosures for the preceding commentary, please follow this link: http://www.BushOnBanks.com/disclosure.shtml.

This commentary was provided by Nancy A. Bush, CFA of NAB Research, LLC and is being distributed by Banks Street Partners, LLC. The views of the author do not necessarily represent the view of Banks Street, and Banks Street has neither directed nor had editorial oversight over the content. Material in this report is from sources believed to be reliable, but no attempt has been made to verify its accuracy. Past performance is no guarantee of future results. Banks Street Partners actively seeks to conduct investment banking in the financial institutions and services sector, including with companies named in this report. To learn more about Banks Street Partners, please visit www.BanksStreetPartners.com.

Preparing to Overcome Problems in Bank M&A Transactions

by Michael G. Rediker, Porter White & Co.

In recent months, the merger and acquisition market in community bank stocks has revived from the moribund state prevailing during and after the Great Recession of 2007-08. As the number of deals has picked up, so has the number of problems encountered in divestiture transactions which are frequently once in a lifetime transactions for community bankers with little or no practical experience with these types of deals. This brief reports on some of the problems we have observed during the last couple of years with the objective of preparing our readers (particularly readers who are potential sellers) to avoid similar problems in their deals should they come to pass.

Beware of deals that result in market concentration.

Antitrust is one of the areas that bankers seldom face unless they are involved in an acquisition where the surviving entity has large market share. The possibility of antitrust issues is increased by the fact that the law in this area is way behind the times because it fails to recognize the growing market share of non bank lenders (e.g., credit unions) and mortgage companies, competition from large brokerage firms (many of them with bank affiliates) which pursue both depository and lending relationships, and the reality that with a smartphone one can deposit a check or take out a loan from a financial institution in another part of the country. Because antitrust law no longer makes sense a deal needs an expert lawyer and sometimes an expert economist to survive a challenge in this area.

Data processing termination fees. Many, if not most, community banks outsource their data and financial processing under multi-year contracts. These contracts frequently call for termination fees that are material in relation to the consideration offered by a buyer in the event of a sale of the bank. The best time to negotiate these fees is at the time of initial solicitation of proposals for data processing outsourcing. By the time a divestiture letter of intent is signed, it is too late.

Falling acquirer stock prices in transactions involving, in whole or in part, acquirer stock. Regulatory approvals in bank divestitures can take a number of months during which the market price of an acquirer's stock will undoubtedly fluctuate and may decrease materially even without adverse events in the business of the acquirer. To keep the deal from falling apart it is important to provide for a range of values within which the parties are obligated to close. A decline in the acquirer's stock price may be more readily acceptable if the deal value is higher than obtainable in a cash deal or the sellers benefit from a tax free exchange.

Employment contracts. Banks frequently enter into employment contracts with one or more of their principal officers and these agreements sometimes provide for large payments in the event of a change in control of the banks. It is important that these employment contracts be negotiated with the possibility of the sale of the bank in mind and that the contract terms be commercially reasonable. Overly generous payments may lead to a reduction in the sales price received by the stockholders and may also put the contracting officer in a conflict of interest position as his or her duty to shareholders comes into conflict with personal financial interests.

Keeping your crystal ball shiny to deal with minority dissenters. In every merger and acquisition transaction the parties worry about whether they are receiving (paying) too little (much), and sometimes minority stockholders bring appraisal actions seeking a higher value for their shares. If you are a seller the best way to become comfortable with the transaction price is to have a firm handle on what your bank is worth as an independent business over the next five to 10 years. Is the consideration you are being offered more than you think your bank is worth if it stays independent (this can happen in a transaction fair to both parties when the acquiring bank and the acquired bank are worth more together than they are apart, when 1+1 is more than 2)? How do you convince your directors, and ultimately your stockholders, that the deal price is more than you are worth as an independent entity?

The answer is that you should prepare and update annually a strategic plan and a three-to-five year forecast of operations with accompanying discounted cash flow analysis. If you will do this over time you and your board will gain confidence in your judgement of the value of your bank and be in a position to react definitively to purchase proposals that you solicit or otherwise receive. Discounted cash flow valuations based on forecasts done by management in the regular course of business are generally respected by courts in the event there is a challenge from minority shareholders leading to appraisal actions, and you will be in a position to defend against dissident stockholders with "made as instructed" valuation experts in tow.

Michael G. Rediker, CFA is an investment banker with Porter White & Company in Birmingham. He can be reached at (205) 458-9135 or rediker@pwco.com. Since 1968 Jim White has advised businesses, individuals, non-profits and munici-palities on a wide range of financial matters. He founded Porter White & Company in Birmingham in 1975 and presently serves as chairman. Jim can be reached at (205) 252-3681 or jim@pwco.com.

Vendor Risk Management: It's More Than a Checklist

by Terry Ammons, Porter Keadle Moore

Risk management and cybersecurity are again top of mind for financial service providers heading into 2019. Recent data breaches at sizeable organizations have posed a significant question for these bankers: "Does our bank have the proper safeguards to defend against tomorrow's cyber attack?"

Likewise, federal regulators have also indicated their desire for banks to more stringently manage and oversee their risk management efforts. In particular, these regulators are spending an increasing amount of time examining the role data liquidity plays in banks' operations, particularly as it relates to the data moving between banks and their vendor partners.

Of course, engaging and working with third-party vendors, such as fintechs, has become a key tactic in a financial institution's ability to serve and engage customers. Working with these vendors however, entails a certain degree of risk as potentially critical consumer information flows from the bank's network and on to the vendor's.

Just as cybersecurity threats pose a risk to banks' daily business and internal networks, in order to mitigate future reputational, operational and legal damages, banks must take a more active approach in overseeing their vendor relationships.

Different Levels of Risk

Because of the nature of their business and the sensitive personal and financial data in their care, banks have a higher threshold than other industries when it comes to developing their risk management programs. Federal regulators are constantly monitoring for potential missteps, and consumers are becoming more vigilant in their scrutiny of financial service providers as well. This means bankers must take the added step of ensuring their risk management programs hold up to the highest level of inspection.

Not all threats are equal when it comes to risk management, however, and the first step to creating a modern risk management program is to stratify risk categorically. Most bankers recognize that some vendors pose a more serious threat of risk to an institution, yet many continue to treat all vendors equally, applying the same level of risk to each regardless of type of service or sensitivity of data shared.

For example, most financial institutions are leveraging one vendor for their instant issuance technology, and another for their mobile banking platform. While both vendors play a role within the institution's technological framework, the mobile banking vendor is potentially logging and storing significantly more important data from the bank within their own servers, presenting an opportunity to potentially be compromised if the vendor is not as stringent with its security protocols.

So, how do bankers securely manage the data moving throughout their organization? While internal intrusions are as much of a risk for banks as external ones, what could be more risky than allowing data to leave? After all, once data is outside of a bank's network, bankers have little to no control over it, and it's up to the vendor to hold up their end of the data security bargain.

Due Diligence

Once all of a bank's risks have been identified, categorized and are actively tracked, it's up to the bank to conduct its own due diligence and ensure its vendor partners are upholding their end of the contract. The end-product of this is typically a requirement on the vendor's part to provide documentation and reporting that both validates and demonstrates its security protocols. Unfortunately however, this is usually only done at the start of a relationship, as conducting further analysis can be time consuming and often treated as an unnecessary, cumbersome expense.

In reality, successful due diligence is an ongoing effort rooted in how well a bank and vendor can collaborate and communicate with each other. While it is a vendor's job to maintain the security controls and safeguards established at the start of the relationship, cybersecurity threats are constantly evolving. Banks, by taking the added step of continuously working with their vendors, and not viewing it as a once-a-year, check-the-box situation, can better protect their own networks, and in turn, their customers.

Keep in mind however, that with so many potential avenues of attack, a cybersecurity breach can still occur. Whether it's missing a patch or an employee clicking a malicious email link, a bank's risk management strategy must include steps for how to mitigate damage once a breach has occurred. Every institution wants to avoid this situation, but when and if one does transpire, the bank must take a three pronged approach of remediation, mitigation and finally, acceptance. This allows the bank to fix or correct any damages, prepare for any similar attacks in the future and create a more robust strategy for responding to future cybersecurity threats.

Effective risk management is often a balancing act between meeting the latest security standards, managing evolving regulatory requirements and the recognizing the potential for malicious actors to create new, and oftentimes more sophisticated, traps. There is no finish line when it comes to compliance and protecting consumer information – rather it's an ever moving target that requires constant review and evaluation.

Terry Ammons, CPA, CISA, CTPRP is systems partner at Porter Keadle Moore (PKM), an Atlanta-based accounting and advisory firm serving public and private organizations in the financial services, insurance and technology industries. Ammons is also host of PKM's podcast GroundBanking. To learn more, please visit http://www.pkm.com/groundbanking/

What the Midterms Mean for Community Banks

by Brian Malcom, Waller

It is finally over. No more robocalls. No more yard signs. No more poorly-produced television commercials. The midterms are behind us. A few results are still being counted, but the landscape is clear. Democrats will have a majority in the House, and Republicans will have a majority in the Senate. But what does this mean for community banks?

In the past two years, the Republicans controlled the House, the Senate and the White House. Because of this, Republicans pushed an aggressive legislative agenda and sought to provide relief from regulatory burdens for community banks, along with tax cuts. Community banks can expect that the Democrats will seek to halt those efforts in the 116th Congress and position themselves to renew regulations in the 117th Congress. Time will tell whether the Democrats will actually have the courage to undo the tax cuts.

Senate

The Republicans retained their hold on the Senate, so there will be little change in the way of leadership. Those changes will come in the chairs of certain committees. Current Banking Committee Chairman Sen. Mike Crapo (R-Idaho) is the favorite to take control of the Senate Finance Committee, so long as Sen. Chuck Grassley (R-Iowa) remains as the chair of the Judiciary Committee. Sen. Orrin Hatch's (R-Utah) retirement will leave that chair vacant. If Sen. Mike Crapo makes this move to run the Senate Finance Committee, a community banker will likely take the helm of the Senate Banking Committee: Sen. Pat Toomey (R-Pennsylvania). Sen. Toomer was a founder of Team Capital Bank, a community bank in Bethlehem, Pa. before becoming a U.S. Senator.

With Sen. Toomey at the helm, the Senate Banking Committee would likely continue its push to decrease the regulatory burden for community banks, but the divided Congress would make meaningful changes less likely. Sen. Toomey favors reforms to the

Dodd-Frank Act, wants to make it easier for businesses to grow capital, and wants to limit some of the powers of the FDIC and the CFPB. Sen. Toomey's goals should be welcomed and supported by community bankers, and they are in line with the goals of the GOP as a whole. Bipartisan support for any of these goals, however, will likely not happen in the upcoming Congress.

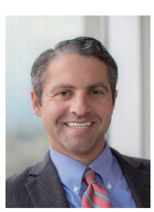
Bipartisan support for some issues seems unlikely for the Senate Banking Committee, but the parties may work together on non-partisan issues. The remaining Democrats on the Senate Banking Committee will likely be more outspoken in their opposition to regulatory reforms. Sen. Sherrod Brown (D-Ohio) will likely continue to oppose any attempts to reform Dodd-Frank. Both parties will likely continue to support legislation that curbs money laundering, terrorist use of financial networks, enterprise reform, and reforms to the Bank Secrecy Act. It is not clear whether the cannabis industry will be a partisan issue for the Senate Banking Committee, but legislation relating to cannabis banking will likely be considered during this upcoming Congress.

House

Republicans took a big hit in the House. Democrats picked up more than more than 29 seats and may pick up more still. In January 2019, Democrats will be in the majority for the first time since 2011. This means there will be more noticeable changes in the House. Rep. Nancy Pelosi's leadership team will likely take the helm, although there could be some change regarding who is at the top. Some Democrats are calling for new leadership, and some Democrats are happy to let Pelosi take over again.

Notably, the House Financial Services Committee will see new leadership and have a large number of new members. Rep. Maxine Waters (D-Cal.) will likely be the chair of the committee, and will seek to enact a far more liberal agenda than her predecessor through the committee. There is ample evidence to suggest that Waters will oppose any effort at regulatory reform for the banking industry, and she may even seek to enact new regulations. Waters favors increased regulatory oversight for the banking industry. Banks can expect increased regulatory activity for this committee for at least the next two years.

Banks should only expect bipartisan support for non-partisan issues, like Bank Secrecy Act reform, data security, and anti-money laundering. Moderates from both sides of the aisle will likely agree to move on these issues. Partisan issues will likely not get much traction in the 116th Congress.



Brian J. Malcom is a partner at Waller in Birmingham. Top banks and financial institutions seek his counsel in all areas of litigation, including contract disputes, trust and fiduciary litigation, consumer claims, and bond and warrant claims. Brian was profiled in 2017 by the Birmingham Business Journal as one of Birmingham's Rising Stars of Law. He was also named a Top Attorney for Banking Law in 2018 in Birmingham Magazine's annual peer-reviewed survey.

Getting the Debtor's Name Right on the UCC-1 is Important

by Laurence Vinson, Bradley

Alabama banks and other secured parties sometimes have difficulty completing the UCC-1 financing statement form in the manner provided by Article 9, "Secured Transactions," of the Alabama Uniform Commercial Code with respect to debtors that are registered organizations, according to an unscientific survey by the author of a sample of UCC-1s filed in the Office of the Secretary of State of Alabama. If an error in completing a UCC-1 causes the UCC-1 to be ineffective, the secured creditor will not have a perfected security interest in collateral that would have been perfected by filing an effective UCC-1. Common potential problem areas include incorrect debtors' names, incorrect secured parties' names, and misspellings.

To be sufficient a financing statement must (1) provide the name of the debtor, (2) provide the name of the secured party, and (3) indicate the collateral covered by the financing statement. If the financing statement is related to real property, such as a fixture filing, additional information also is required.

Name of the Debtor

If the debtor is a registered organization such as a corporation, limited liability company, or limited partnership, a financing statement sufficiently provides the name of the debtor only if the financing statement provides the name of the debtor indicated in the record which shows the debtor to have been organized and which is filed as a public record in the state in which the debtor was organized. In Alabama, in most cases the applicable public record is the certificate of formation filed in the office of the judge of probate of the county where the registered organization was formed, including any filed amendments to the certificate of formation. A copy of the certificate of formation is forwarded by the judge of probate to the Secretary of State of Alabama. The names of registered organizations formed in Alabama and the names of debtors on UCC-1 financing statements filed in the Secretary of State's office are searchable on the website of the Secretary of State of Alabama. These online databases are not the official record, however. In the case of a discrepancy between the name of a registered organization on file in the Secretary of State's online databases and the name shown on the organization's certificate of formation, the name shown on the certificate of formation will control.

Banks and other secured parties often include the debtor's jurisdiction of organization after the debtor's name in the space for the "Debtor's Name" on the UCC-1. For example, if the debtor's name as shown in its certificate of formation is "Acme, Inc.," the debtor's name may be shown on the UCC-1 as "Acme, Inc., an Alabama corporation," Thus, the name provided as the "Organization's Name" on the UCC-1 includes the debtor's name, and it also contains information in addition to the debtor's name shown on the debtor's certificate of formation. This practice leads to the question whether the name shown on the UCC-1 provides "the name of the debtor" as required for the financing statement to be sufficient.

A financing statement which substantially satisfies the requirements of Article 9 is effective even if it has minor errors or omissions, unless the errors or omissions make the financing statement "seriously misleading." As a general rule, a financing statement that fails sufficiently to provide the name shown on the certificate of formation of a debtor that is a registered organization is seriously misleading. However, if a search of the records of the filing office under the debtor's correct name, using the filing office's standard search logic, would disclose a financing statement that fails to provide the name of the debtor shown on the debtor's certificate of formation, the name provided does not make the financing statement seriously misleading. Fortunately, it appears that if a search is made under the name "Acme, Inc.," for example, the search logic used in the UCC database of the Alabama Secretary of State – at least as applied to an unofficial search on the Secretary of State's website – will disclose a financing statement that provides the debtor's name as "Acme, Inc., an Alabama corporation."

If another creditor or a trustee in bankruptcy of the debtor were to ask a court to determine that the secured party's financing statement is ineffective because it provides information in the "Organization's Name" box in addition to the name of the debtor shown in its certificate of formation, it would be incumbent upon the secured party to offer in evidence a search report issued by the Secretary of State in response to a request submitted solely in the correct name of the debtor which report discloses the financing statement filed by the secured party with the additional information in the box for the debtor's name (e.g., the report shows the financing statement filed naming the debtor as "Acme, Inc., an Alabama corporation"). The best practice in order to avoid this risk and potential expense is for the secured party to provide as the name of the debtor on the UCC-1 only the debtor's name exactly as indicated on the debtor's certificate of formation, without adding any additional information.

The procedures of the Alabama Secretary of State describe some aspects of the search logic used to search for UCC-1s filed in that office:

> (3) Rules applied to search requests. Search results are produced by the application of standardized search logic to the name presented to the filing officer. Human judgment does not play a role in determining the results of the search. The following rules apply to searches.
>
> (a) There is no limit to the number of matches that may be returned in response to the search criteria.
>
> (b) No distinction is made between upper and lower case letters.
>
> (c) Punctuation marks and accents are disregarded.
>
> (d) Words and abbreviations at the end of a name that indicate the existence or nature of an organization [e.g., "Inc.," "Corp.," "LLC"] as set forth in the "Ending Noise Words" list as promulgated and adopted by the International Association of Corporation Administrators are disregarded.
>
> (e) The word "the" at the beginning or end of the search criteria is disregarded.
>
> (f) All spaces are disregarded.

The search logic used for UCC-1 searches by the Secretary of State of Delaware is very similar to that used by the Secretary of State of Alabama. This is good news for banks and other secured parties in Alabama, because many borrowers which are registered organizations are organized under Delaware law. The only correct place to file most financing statements which name a registered organization as the debtor is in the UCC filing office in the state where the debtor was organized.

The standard search logic used by the filing offices in some other states is not as forgiving as the search logic used by the Alabama Secretary of State appears to be. For example:

- A bankruptcy court in Virginia held that a financing statement was insufficient where the abbreviation "Inc." was omitted from the name of the debtor on the filed UCC-1.

- A bankruptcy appellate panel, in a case where the debtor's correct name was "EDM Corporation," held that a financing statement that provided the name of the debtor as "EDM Corporation d/b/a EDM Equipment" was ineffective under the search logic used in Nebraska. The secured party in that case argued that its financing statement sufficiently provided the debtor's name because the words "EDM Corporation" were included in the name provided. The appellate panel disagreed, saying that the financing statement did not provide the name of the debtor and that it was seriously misleading.

- A bankruptcy court in Texas, in a case where the debtor's correct name was "Jim Ross Tires Inc.," held that a financing statement that provided the debtor's name as "Jim Ross Tires, Inc. dba HTC Tires & Automotive Centers" was ineffective. The court said the addition of the dba name conflicts with the purposes of the indexing system and the administrative procedures for indexing and searching UCC records filed with the Texas Secretary of State.

- A federal court in Wisconsin, in considering a financing statement where the secured party accidentally included a space between "Inc" and the period following those letters, thereby providing the debtor's name as "ISC, Inc ." (rather than "ISC, Inc."), held that the financing statement did not sufficiently provide the name of the debtor and was seriously misleading. Apparently, the search logic in that state treats a space the same as a letter of the alphabet. As a result, incorrectly adding the space before the period created a "misspelling" of the debtor's name that would cause the search logic not to disclose the financing statement filed by the secured party.

- A bankruptcy court in Texas, in a case where the debtor's correct name was "BFN Operations LLC", held that financing statements filed in Michigan and Tennessee that provided the debtor's name as "BFN Operations, LLC abn Zelenka Farms" were ineffective because the standard search logic used in those states would not have disclosed the financing statements in a search made using the debtor's correct name.

Name of the Secured Party

A number of Alabama banks put their bank's name in the "Secured Party's Name" box on the UCC-1, followed by additional information such as "an Alabama Banking Corporation" or "an Alabama State Bank." As noted above, to be effective a financing statement must "provide the name of the secured party." While Article 9 goes into considerable detail in describing when a financing statement sufficiently provides the name of the debtor and when an error in the debtor's name shown on the financing statement is not "seriously misleading", no similar rules are provided with regard to the sufficiency of a secured party's name or the effect of an error in the name of the secured party provided on the financing statement.

It seems that the correct name of a secured party, followed by additional information such as "an Alabama Banking Corporation", should not cause the name of the secured party shown on the UCC-1 to be insufficient because it is not seriously misleading and also – and primarily – because searches for UCC-1s are not performed in the name of the secured party. Still, the best practice is to provide only the secured party's correct legal name, without any additional information, in the space for the name of the secured party on the UCC-1.

Misspellings and Similar Errors

Spelling counts. If the debtor's name as shown on the UCC-1 is misspelled or contains similar errors, the UCC-1 very likely will be ineffective. UCC lien searches are performed by word searches in the correct name of the debtor, and a misspelling of the name of the debtor on the UCC-1 almost certainly will cause the debtor's name to be "seriously misleading" because the UCC-1 will not be disclosed in a search using the correct spelling of the name of the debtor. For example, debtors' names that begin with the word "Alabama" are fairly common in Alabama. A search of the online UCC records of the Alabama Secretary of State using the misspellings "Alabma," or "Albama" turns up UCC-1s that have been filed with that misspelling shown as part of the debtor's name. Those UCC-1s likely will be deemed to be ineffective if the error was made by the secured party and not as a data entry error by the filing office, because a search of the debtor's correct name using the standard logic of the filing office likely will not turn up those financing statements.

For example, a bankruptcy court in Florida held that a financing statement that provided the debtor's name as "John Bean Farms, Inc." was seriously misleading where the debtor's correct name was “John’s Bean Farm of Homestead, Inc.” And, in the first of the two Texas bankruptcy court cases described above, a UCC-1 filed by another creditor named the debtor as “Jim Ross Tire Inc.” instead of “Jim Ross Tires Inc.” (the “s” in “Tires” was omitted). The court found that the UCC-1 was not effective because a search under the debtor’s correct name using the standard search logic of the filing office would not disclose the UCC-1 on which the “s” in “Tires” had been omitted.

Conclusion

The importance of providing the debtor’s name on the UCC-1 exactly as it is shown on the debtor’s certificate of formation cannot be overstated. If the debtor’s name provided on the UCC-1 is not the name indicated on the debtor’s certificate of formation, and if a search of the UCC records under the debtor’s correct name made using the standard search logic of the filing office would not disclose the UCC-1, the UCC-1 is “seriously misleading” and will be as ineffective as it would if it had never been filed.

Larry Vinson regularly counsels financial institutions of all sizes on new CFPB regulations, bank regulatory and product questions, and all aspects of state and federal consumer credit compliance. On questions relating to the Uniform Commercial Code, he is a resource for the firm's clients and for other lawyers both inside and outside the firm. He served as Chair of the Alabama Law Institute advisory committees on Revised UCC Article 9, "Secured Transactions," Revised UCC Article 3 and Article 4, and Revised UCC Article 1 and Article 7.

Virtual Currency Regulation: What Do Alabama Bankers Need to Know?

by Erica Barnes, Maynard Cooper & Gale

The financial press cannot get enough of virtual currency, from Bitcoin to its thousands of more obscure cousins like Ethereum or Monero. Virtual currency is either a great invention or a total failure; the end of traditional banking or a call to innovation; speculation or cutting-edge investment; and a privacy tool or a money laundering device. Whatever it is, virtual currency does not appear to be going away. So, what do Alabama bankers need to know?

The Regulatory Landscape Remains Unclear

Less than five years ago there was virtually no legal means to spend Bitcoin or formally speculate on its value. Ten years ago it did not exist. Now, anyone with an Internet connection can legally purchase multiple virtual currencies using a bank account; speculate on their value using futures contracts; and invest in their future through initial coin offerings (ICOs). The brave pay their satellite bill at DISH Network or buy a throw pillow at Overstock with virtual currency.

Yet, the United States has no comprehensive federal regulatory scheme governing virtual currency’s creation or use. The IRS views it as property subject to gains and losses, while the CFTC calls it a commodity. The SEC does not consider Bitcoin and Etherium securities, but says some ICOs may be. FinCEN characterizes virtual currency exchangers and payment processers as money transmitters who must comply with the Bank Secrecy Act (BSA) and anti-money laundering (AML) requirements. Federal courts have fairly consistently applied federal money laundering statutes to virtual currency transactions, but the legal landscape is far from clear.

At the state level the situation is even murkier. Some states, like New York, have tried to license virtual currency businesses while others have ignored them completely. Some states, like Alabama, have modified their statutes to cover virtual currency, while others, like Tennessee, have issued guidance specifically stating that their money transmitting laws do not apply to virtual currency. The Alabama Monetary Transmission Act, passed in August 2017, makes clear that certain currently unregulated entities (not banks or broker-dealers) exchanging virtual currency or processing virtual currency payments are money transmitting businesses and must provide regulators with extensive information about their business, register, and keep records of their transactions.

International virtual currency regulation is also a patchwork. Federal and international regulators indicate that more comprehensive and cohesive regulation is on the way, but nothing concrete appears imminent.

Traditional Bank Interaction with Virtual Currency Is Increasing

Despite this uncertainty Alabama banks, cannot avoid virtual currency completely.

First, Alabamians are acquiring and investing in virtual currency. A handful of Alabama businesses accept virtual currency in exchange for goods. Major virtual currency exchangers like Coinbase are licensed in Alabama. According to coinatmradar.com, there are 13 virtual currency ATMs operating from Huntsville to Mobile. In a Sept. 24 press release, the Alabama Securities Commission indicated that it had 21 active investigations involving ICOs and had issued eight related Cease and Desist Orders.

Alabamians may be asking their banks to service their virtual currency businesses, assist them with accepting virtual currency, consider their virtual currency holdings in evaluating their creditworthiness, or help them effectuate third party transactions.

Most traditional institutions refuse to accept, hold, or exchange virtual currency, although some, like Goldman Sachs, have considered it. Many institutions refuse to bank virtual currency companies because of regulatory concerns, but some like Silvergate Bank in San Diego market themselves to such companies. Due to volatility and AML concerns, some institutions prohibit customers from purchasing virtual currency with institution credit cards or wire transfers and refuse to consider virtual currency investment profits in lending. The landscape is changing daily, so Alabama bankers must continuously reconsider their bank policies and risk tolerance in these areas.

Second, virtual currency transactions are international, largely anonymously, confirmable and irreversible, making them an ideal tool for criminal activity. Criminals from sophisticated international identity thieves to high school marijuana dealers are buying and selling their product using virtual currency. Most criminals must still interact with financial institutions to convert their illegal profits to fiat currency to spend.

As licensed virtual currency exchange platforms begin to implement better AML procedures, criminals may turn to unlicensed exchangers who are willing to accept cash in person, by mail or via gift or spending card to exchange. These businesses often cannot manage their cash without financial institutions. Although traditional AML techniques can effectively identify these criminals, AML/BSA officers must understand virtual currency, current schemes, and evolving regulations to spot problems.

In the world of virtual currency, answers are rare and evolving, but banks regardless of size cannot ignore the issue. Banks should ensure BSA/AML officers receive training on current virtual currency schemes and regulations and develop policies regarding banking entities accepting or investing in virtual currency; facilitating virtual currency purchases via wire, credit card, or ACH; and recognizing virtual currency or proceeds as asset for lending purposes.

Erica Barnes is a shareholder in the firm's White Collar Defense and Investigations section and a member of the General Litigation Practice Group. She focuses her practice on assisting individuals and entities in connection with state and federal criminal matters, conducting internal investigations, litigating and resolving false claims act proceedings, anti-corruption and anti-fraud compliance, and civil litigation involving a criminal or governmental component. Erica also has experience in a wide variety of commercial litigation matters and has represented defendants in individual and class actions involving contract, employment, shareholder, and securities claims.

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.

ALABAMA BANKERS ASSOCIATION

445 Dexter Ave., Suite 10025 | Montgomery, AL 36104

Phone (334) 244-9456 | Toll Free (800) 239-7338