Focus on the Process: Reexamining the Role of Directors in Lending
by William E. McCartney

On Oct. 25, a civil jury in the United States District Court for the Northern District of Georgia issued a $5 million verdict in favor of the Federal Deposit Insurance Corporation, as receiver for The Buckhead Community Bank, against a number of the failed bank’s former directors and officers. This recent verdict is renewing concern over director liability for lending losses and should prompt financial institutions across the country to revisit the functions of their boards of directors in the lending process.

In November 2012, the FDIC brought a civil action against nine former officers and directors of The Buckhead Community Bank alleging they were negligent with respect to making numerous acquisition, development and construction loans and commercial real estate loans. The FDIC contended that the former officers and directors failed to follow the fundamental tenants of banking in administering the loan approval process and managing the bank’s loan portfolio by approving 13 specific loans (the trial focused only on 10 of the loans). The FDIC presented evidence of the former officers’ and defendants’ deviation from the bank’s approved loan policies and regulatory requirements through what the regulator characterized as failures to understand the purpose of the loans, obtain or review property appraisals prior to loan approval, verify reported income and net worth of borrowers and guarantors, analyze borrower and guarantor debt obligations, require independent underwriting of participation loans, consider criticisms from third-party loan review consultants, require borrower equity, and comply with loan-to-value requirements. The losses resulting from the former officers and directors’ alleged negligence with respect to these loans exceeded $22 million.

In defense of FDIC’s allegations, the former directors and officers argued, somewhat successfully, that their approval of the subject loans were protected by the business judgment rule. The business judgment rule is a presumption that the decisions of the officers and directors of corporations are made in good faith, which precludes some, but not all, claims of negligence against bank officers and directors. Generally speaking, the business judgment rule focuses on the reasonableness of the process used to reach a decision, and not the consequence of that decision. The rationale for this rule, and the application of the rule to bank directors and officers, was explained early on in American jurisprudence by the Alabama Supreme Court in Godbold v. Branch Bank, which reasoned that assigning liability to bank directors for any error in decision-making would be “manifestly wrong” and that the “inevitable tendency of such a rule, would be hostile to the end proposed by it, as no man of ordinary prudence would accept a trust surrounded by such perils.” Godbold v. Branch Bank, 11 Ala. 191, 199 (Ala. 1847). In other words, without the business judgment rule as a defense to decisions undertaken in good faith, it is unlikely that anyone would ever agree to serve as a director.

When analyzing a defense based on the business judgment rule, courts distinguish between claims of unreasoned and uninformed decisions and unreasonable decisions. FDIC v. Loudermilk, 761 S.E. 2d 332, 335 (Ga. 2014). The focus was on the process such officers and
In the wake of this verdict, bank directors must reexamine (a) the processes and procedures enacted by their financial institutions in underwriting and loan approval, and (b) who carries the burden for ensuring compliance with these processes and procedures. In order for directors and officers to avoid forfeiture of the business judgment rule in the event their decisions eventually lead to losses resulting in litigation, bank directors and officers must ensure that their institution’s underwriting process and loan policies are being followed by those tasked with approving loans and that the loan policies are sufficiently detailed and rigorous to promote informed decision-making, with specific attention to larger or more complex commercial credits. Financial institutions must also reconsider, where appropriate, the involvement of the board of directors in the day-to-day credit decisions, such as the underwriting and approval of individual loans. There should be thoughtful consideration as to which individuals at the financial institution have the time, information, and expertise to adequately evaluate large or complex credits, and which individuals possess skills or resources better suited to focusing on strategic management decisions, such as the underwriting process and loan policies.

William E. McCartney is an associate at Reynolds, Reynolds & Little, LLC where he represents financial institutions in transactional matters, regulatory compliance, and lender liability disputes.

Managing CRE Concentration
by Murray Bibb

Recent regulatory scrutiny of commercial real estate (CRE) loan concentration should come as no surprise to any bank executive, director, or investor. CRE concentration, in and of itself, is not an indication of heightened risk to a banking institution’s capital base; however, lenders that are above, or approaching, interagency guidance thresholds have undoubtedly been questioned by regulators as to the level of portfolio and credit risk management processes for tracking and mitigating any potential risks from concentrations in the CRE portfolio.

For reference, in December 2015, citing observations of increased loan originations, competitive market pressures, and weakening underwriting standards the board of governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency issued an interagency statement regarding prudent risk management for CRE lending, and renewed attention to guidance issued in 2006 pertaining to CRE concentration.

The 2006 guidance addresses the risks of concentration in CRE lending by specifically citing two supervisory criteria: (1) aggregate loans for land acquisition, construction, and development (ADC) in excess of 100 percent of a banking institution’s total risk-based capital; and, (2) total non-owner-occupied CRE loans (including ADC loans) in excess of 300 percent of a bank’s risk-based capital, AND growth in CRE lending of 50 percent or more during the prior 36 months.

Whether you think the guidance criteria is appropriate, or that a sophisticated credit risk management framework is in place, the current spotlight on CRE concentration from bank regulators is not going away – listen to just about any third quarter earnings call for confirmation of this. Therefore, banks of all sizes and shapes need to fully understand how (and why) its regulators view the risks associated with increased CRE concentration, and what measures they deem necessary to protect a bank, its shareholders, and its stakeholders.
depositors against significant adjustments in prevailing CRE market conditions.

Let’s be clear that the supervisory CRE concentration guidance does not constitute a “hard limit” on the size of a CRE loan portfolio, but rather sets forth indicators at which enhanced risk management practices should be followed, including but not limited to loan-level and CRE portfolio stress-testing. If a bank is operating with CRE concentrations above the supervisory thresholds, and its regulators are not satisfied with its credit risk and portfolio management processes, then it may be identified for further supervisory examination, and in certain cases, be required to raise new capital or maintain existing capital well above “well-capitalized” minimums.

To show that a banking institution fully understands the risks in its CRE portfolio, practical credit risk management procedures must include bottom-up approach to the segmentation and monitoring of its loans. Even if a bank’s CRE concentration is nowhere near the guidance criteria, industry standard best practices in identifying, quantifying, and managing risks associated with CRE lending can be applied to other loan segments to establish the foundation of a sound bank-wide portfolio and credit risk management framework.

Segmentation involves properly capturing and classifying loans by product type, loan purpose, geography, industry, collateral type, market correlation, and any other descriptive or quantifiable category. Credit risk monitoring uses that segmented data to track the loan portfolio over time against certain benchmarks and other leading economic indicators to ensure an appropriate risk-adjusted return is achieved, as well as to establish a proper allowance for loan losses (ALLL). Further assessment of unsystematic credit risk involves monitoring asset quality over time, specifically loan performance, credit exceptions, risk-rating migration, as well as changes in collateral value, occupancy rates, rental rates and operating expenses.

Overall, it appears that the regulatory focus on CRE concentration, combined with increased capital reserves required for so-called High Volatility Commercial Real Estate (HVCRE), has caused some banks to tap the brakes to a degree with respect to new CRE loans, affecting slightly lower competition, and even some pricing relief, for the active players still in the market.

Murray Bibb is an investment banker with Porter White & Co. in Birmingham and advises banks and borrowers across the state on a variety of lending matters. He served over a decade at two publicly-traded Alabama banks in senior credit officer capacities. He can be reached at (205) 458-9122 or murray@pwco.com.

The Internet of Things: Is It Viable and Transformational, a Security Headache, or the Regulatory Wild, Wild West?
by Helen Kathryn Downs

In the financial services arena, the Internet of Things (“IoT”) may implicate all three scenarios, offering unprecedented opportunities for innovation and transformational change, while presenting some vexing challenges. Yet the number and utility of “smart” devices that operate through the Internet—the basic components of the IoT—are poised to expand exponentially. These developments will likely have a significant impact not only on financial services but also in our homes, office buildings, factories, and other structures, the operation and infrastructure of cities and towns, and the health care, transportation, agriculture, energy, security, and surveillance industries. The IoT may fundamentally alter how people identify themselves, interact with one another, and make use of routine things in their day-to-day lives – from the bathroom scale to the closest ATM machine.

It has been predicted that by 2025, the IoT may encompass more than 60 billion “smart” devices. This next stage in the digital revolution will likely spark a myriad of new products, businesses, and services, impacting on the U.S. economy by an estimated $90 billion annually.
This much innovation during the next eight to 10 years may trigger some unease, especially on the heels of the disruption caused by online banking services, increased regulation, and mobile banking (not to mention Amazon, Bitcoin, competing FinTech startups, and Blockchain). But two basic banking principles remain central when evaluating and navigating the IoT: 1) Know your customer; and 2) Balance measurable benefits—such as a better customer experience—against the cost of adding IoT devices to your current digital infrastructure and consumer applications, with a special focus on embedded security features.

The Internet of Things: How it Works

The Internet was built from content and communications by or about people, reviewed or used by people. In 2008, the number of things connected to the Internet began to outstrip the number of people connected. The IoT will add millions of everyday things, like refrigerators, contact lenses, and restaurant tables, to the mix—seemingly lifeless objects that traditionally have not communicated at all. New technologies make it possible for small sensors to be placed into these things that can sense, listen, touch, communicate, and control information, essentially creating a new form of speech. Based on the latest Internet protocols (IPv6), each sensor is assigned a unique identifier so that it can send and receive information to and from the Internet and other things equipped with wireless sensors.

These sensors can collect, monitor, and search for information. The sensors’ data are then sent wirelessly either to other sensors to signal or control something, like an adjustment to a home thermostat when the original sensor detects sunset, or directly to the cloud for further analysis. A gateway may be employed so that only the most pertinent information moves to the cloud or to enhance security. Increasingly sophisticated software and data analytics convert these numerous tiny bits of sensor data into useful information, which is then delivered through apps or other processes to consumers and businesses.

Sensors and related infrastructure are being placed in the heart of our homes, work spaces, factories, and cities, forming the basis of current and future IoT functionality. Smart phones, tablets, wearable devices, and other devices such as Amazon Echo are interacting more and more often with these small, smart pieces of computer hardware.

How Is the Internet of Things Affecting Banking Today?

What IoT innovations are happening in the banking sector? What are the key considerations for a bank that wishes to embrace the IoT and set its brand apart through meaningful enhancement of products and services?

Innovations and pilot projects by banks in the IoT space over the past several years reveal several insights. For example, Westpac New Zealand bank, an IoT pioneer, explored uses for Google glass—a cutting-edge wearable technology in 2014 that operated by voice commands. Customers did not embrace the technology, which led to several takeaways. First, customers view their finances as intensely personal information and may be uncomfortable accessing it through voice commands where they can be overheard. Second, customers prefer steps that provide assurance their accounts are secure, such as swiping and entering a device passcode, whether or not those steps encompass the latest technology.

Another initiative by Westpac involved the installation of iBeacons (IoT sensors) in its branches. If a customer opted in by uploading her picture in the bank’s mobile app, she would be greeted by name when entering the branch. Westpac has explored other uses for iBeacon, such as seamless payments to retail partners when a customer orders at a café or restaurant, without having to wait on a check.

U.S. Bank has invested in augmented reality—a digital overlay of real-world objects using IoT sensor technology. For example, the nearest ATM machine and bank branch might appear on a smart phone’s map function. The bank has also looked into IoT to manage secure payments.

Based on these and other initiatives, lessons learned include defining which applications (or enhancements to existing apps) customers will actually use, rather than assuming or relying on vendors touting technology that customers have not yet adopted. Listening and talking to customer sentiments and tracking their needs remain key. In addition, security concerns are paramount for banks and their customers, if additional IoT devices are connected that have little or no inherent security to detect hacking or other vulnerabilities. Thus, IoT innovations and products should be evaluated not only for the benefits provided but also for embedded security features and long-term support for device patching, tracking, and protection. A multi-faceted security approach continues to be central in managing risk.

With the IoT, it becomes more important than ever to identify who is connecting through a specific mobile device. BBVA has invested in multi-factor authentication for Spanish customers who wish to open accounts remotely using selfie photographs, which are cross-checked against photo ids through new facial recognition technology, followed by a video chat to complete the process. USAA Bank was the first in the U.S. to deploy facial and voice recognition for customers to log into its mobile app, which many customers preferred over a lengthy PIN or password. As additional security, device identification took place in the background, with an encrypted token sent from the customer’s device to USAA during each log-in.

Several European banks are enlisting new behavioral biometrics, in which embedded sensors and software learn up to 500 routine movements that uniquely identify the user, such as the amount of pressure applied when tapping the screen and the angle at which the phone is generally held. This generation of biometrics can also detect malware by identifying machine-automated activity.

In our highly connected world, the IoT has and will continue to enable physical objects, such as ATM machines and bank branches, to send, receive, and exchange information in entirely new ways. With so many IoT products and processes in motion, the only constraints on innovation are the outer limits of one’s creative thinking.
To avoid costly mistakes, however, IoT initiatives should grow out of a comprehensive understanding of customer needs, preferences, and use of existing technology, with data analytics that facilitate convenient, real-time transactions and improve the overall banking experience. Existing regulations and oversight for mobile banking, consumer protection, privacy, and security will probably apply equally to the IoT, but unanswered questions remain about exactly what laws will govern this new technology. Because the IoT does not fit neatly into any existing regulatory framework, financial institutions must maintain robust security and privacy protections. For any IoT initiative, identifying potential threats and vulnerabilities during the developmental phase and building in security and privacy protections will be a crucial part of effective risk management.

Helen Kathryn Downs is with Butler Snow and has a wealth of litigation experience. She has been recognized by The Best Lawyers in America for her work in product liability litigation and by Alabama Super Lawyers.

What the Election Means to the Financial Services Industry
by Larry Lavender

With the election of Donald Trump as president and the return of Republicans to majorities in both houses of Congress, the potential for significant regulatory relief for the banking industry has never been greater. Because President-elect Trump did not make financial services reform a major issue during the campaign, it is more likely that Congress will be the main source of regulatory relief for the banking industry.

In Congress, the most likely vehicle will be House Financial Services (HFS) Committee Chairman Jeb Hensarling’s (R-TX) Financial CHOICE Act, which would exempt banks that maintain 10 percent leverage capital from many rules including the CCAR stress test, size limits, living-will requirements, and the Basel III and Volcker rules. In addition, it would replace the Orderly Liquidation Authority with an expedited bankruptcy process and make the Consumer Financial Protection Bureau (CFPB) overseen by a five-member commission and subject to the annual Congressional appropriations process. It also would eliminate the CFPB’s authority to declare practices abusive.

The Trump transition team includes few recognizable Washington-based financial services operatives, though his campaign finance chairman and Treasury Secretary nominee Steven Mnuchin is a former Goldman Sachs executive. As the probable lead Congressional contact for the Trump Administration, Vice President-elect Mike Pence is likely to have a major impact on legislative policy and his close friendship with House Republicans, especially Rep. Hensarling, will elevate the CHOICE Act to an even more prominent place in the financial services policy agenda.

President Trump will likely attempt to fire and replace CFPB Director Richard Cordray very early in his tenure. He will probably also try to end the appeal of the recent federal court decision that provides the legal authority for that firing. There have been some discussions in think-tank and legal circles trying to develop a theory under which the new president could immediately fire Cordray. How the new president handles this will be an early indicator of how aggressive the new administration will be on financial services issues.

While he probably will not immediately remove incumbents, the comptroller of the currency and chairman of the Federal Deposit Insurance Corporation will be eventually replaced when their terms end in March 2017 and November 2017, respectively. President Trump likely will move quickly to fill the vacancy in the office of Vice Chairman for Supervision at the Federal Reserve. These several appointments will have a major impact on examination and compliance issues for banks.

115th Congress Agenda, Committees

Republicans are almost certain to recognize that they must display real and substantive progress on the “change” that was promised in...
the campaign. That will dictate a very busy first 100 days with long weeks in session for Congress. The Senate and House calendars for next year have been published and indicate a very aggressive schedule with long weeks in session in both houses. During the first 26 weeks of the year, the Senate will be in session for 19 five-day weeks, two four-day weeks and one three-day week, with only four weeks out of session. The House has a similarly busy schedule planned.

In addition to Dodd Frank reforms, the Department of Labor Fiduciary Rule will also probably be a target for change. Even though legislative action will be required to change the fundamental basis of the Fiduciary Rule, the new president will be able to appoint a secretary of labor who can delay implementation and rewrite it in a form more acceptable to the financial advisor community.

As for Congressional committees of jurisdiction, the Senate Banking Committee membership will likely remain at 12 Republicans and 10 Democrats. Sen. Mike Crapo (R-ID) will be the new chairman, though Alabama Sen. Richard Shelby will remain a very influential member of the Committee. There will be two vacancies on the committee from the Nov. 8 defeat of Sen. Mark Kirk (R-IL) and retirement of Sen. David Vitter (R-LA).

On the House side, the HFS Committee membership will likely remain at 34 Republicans and 26 Democrats. Chairman Hensarling has two years left before he is term-limited. Ranking member Maxine Waters (D-CA) will remain in that position. Through retirement or defeat, at least three members of the committee will not be returning in the 115th Congress.

Introduction to Blockchain Technology for the Financial Sector

by Kristen F. Johns

Editor’s Note: The following article originally included numerous footnotes citing additional research on the topic discussed in this article. If you would like the footnoted version of this article, please contact the editor at shildebrand@alabamabankers.com.

Blockchain, or distributed ledger technology, has captured the attention of the financial services and banking industry as an alternative platform for certain processes and systems. A survey by IBM of 200 financial market institutions found that 14 percent of the institutions surveyed indicated that they would have a commercially-scaled blockchain in production in 2017. That number increases to 56 percent by 2020. In addition, Lael Brainard, a member of the U.S. Federal Reserve’s Board of Governors, noted in a speech at the Institute of International Finance that blockchain technology “may represent the most significant development in many years in payments, clearing, and settlement.” But what is it?

What is Blockchain Technology?

While there is not one generally accepted definition, distributed ledger technology essentially allows parties to create immutable records of transactions and transmissions in a secure, transparent platform. Blockchain is a more colloquial term for this technology.

“Distributed” describes the platform’s structure. Much of the computing world operates within a centralized framework. For example, money and data are sent to a controlling entity that provides goods and services (e.g., Facebook, Amazon, etc.). A person orders a product from Amazon; Amazon itself takes the order, records the transaction, processes the payment, and ships the product. Amazon typically controls all parts of the transaction. Blockchain technology shifts control by moving from a centralized structure to a decentralized or distributed structure. Either of these decentralized or distributed platforms, or hybrids of each,
can be implemented within an ecosystem or network of entities or individuals. Blockchain technology shifts the responsibility for facilitating and confirming each transaction into the hands of more than one entity. It does this by allowing data to be stored across its network, through software unique to the particular blockchain. Transactions are validated through database replication and subsequent authentication by those entities participating in the transaction within the blockchain network.

“Ledger” refers to the longitudinal and permanent record of time-stamped, verifiable transactions. Each transaction is recorded using cryptographic validation and is arranged in batches of data. Each batch of data is called a block. Each block references and identifies the previous block through sophisticated encryption technology, forming a secure chain of recorded transactions.

Use of blockchain technology creates an unchangeable record of a transaction. As iterated above, this record is not stored in one location, but is distributed to others and maintained by database and computational replication. Any entity with the proper software, operating within the platform, can view the record of a particular transaction, which cannot be changed or reversed. This decentralized structure, combined with an auditable ledger of transactions, is the disruptive technology primed for adoption in appropriate applications in a rapidly changing economy.

**How is Blockchain Technology Currently Used?**

The pace of technology is trying to keep up with demand. While in some applications blockchain technology is in its relative infancy, with the notoriety of Bitcoin, blockchain technology is most well-known in the financial services industry. Bitcoin is the dominant virtual currency platform, but additional platforms exist (e.g., Ether) and continue to emerge. For example, Zcash was launched at the end of October, initially one unit of Zcash trading around $1,000 US and hailing itself as a more secure, more private alternative to Bitcoin.

The adoption of this technology is in its early stage in the United States, but the pace of adoption is accelerating with the help of consortiums. For example, R3 is a consortium of the world’s leading financial institutions comprising more than 70 banks, vendors, and other companies. Synchrony Financial, the largest provider of private label credit cards in the United States, recently joined the consortium. R3 is providing an open source ledger called Corda through the Hyperledger project, an initiative through the Linux Foundation. Corda is intended to provide the platform for blockchain applications in the banking and financial industry. As noted in one of the findings in the August 2016 World Economic Forum report, adoption of blockchain technology “will require deep collaboration between incumbents, innovators and regulators.”

The R3 consortium is one resource aligning stakeholders and its open source initiative invites innovators to address the enduring challenges facing the financial sector: privacy, security, and integration with existing systems.

As another example, in a September speech to the Council of Institutional Investors, a non-profit organization dedicated to institutional investment issues, Delaware Chancery Court Vice Chancellor J. Travis Laster addressed complexities related to corporate voting systems and how such structures have been a basis for errors. He proposed that distributed ledger technology could “provide better accuracy, greater transparency, and superior efficient for settling securities trades and voting in corporate elections.” He also called for the speedy adoption of the technology in order to begin addressing some of the concerns he aired. “Someone is going to do this,” he said. “If a judge can see it, the opportunity is pretty obvious.”
The precise legal implications of this technology are still unclear. What is clear is that distributed ledger technology is arriving in the U.S. financial services sector. Bankers, lawyers, lawmakers, and regulators need to pay attention and learn more about the technology, its potential uses, and the myriad of forthcoming legal issues.

Kristen Johns is a transactional attorney in the Intellectual Property Practice Group at Waller Lansden Dortch & Davis, LLP.

**Lenders Beware: Fraudulent Transfer Pitfalls Despite Innocent Intentions**

by Jesse S. Vogtle Jr. and Jeremy L. Retherford

Mention the term “fraudulent transfer” and you’ll get a banker’s attention. The term conjures up an image of a deceptive borrower hiding assets under the cloak of night in an effort to keep those assets out of the hands of creditors. Such is the quintessential example of a fraudulent transfer based in actual fraud. In other words, the borrower transferred property with the actual intent of frustrating the efforts of creditors in collecting their debts. However, there is a second type of fraudulent transfer based upon constructive fraud. Unlike with a fraudulent transfer based on actual fraud, a transfer may be avoided based upon constructive fraud regardless of the parties’ intent. In fact, a lender with the best of intentions may find itself the subject of an action to avoid a constructively fraudulent transfer if it is not careful.

Consider the following scenario. Acme Home Builders is developing two residential neighborhoods. Acme Home Builders set up two separate limited liability companies as the legal entities developing each of the two neighborhoods (Company 1 and Company 2). Bank made construction loans to each of the companies to finance the developments. Sales in both neighborhoods become sluggish. As a result, Company 1 finds itself unable to make its loan payments to Bank, but is in need of more cash. Bank agrees to lend Company 1 additional funds so long as Company 1 can provide it with additional collateral as security. Company 1 has no unencumbered assets, but Company 2 (its sister company) owns property on which no liens exist. Acme Home Builders (as parent of Company 1 and Company 2) proposes that Company 2 grant a mortgage to Bank to secure its loan to Company 1. If Bank enters into this transaction, it may find itself named as a defendant in a fraudulent conveyance action.

Fraudulent conveyance laws seek to prevent two types of fraud: actual fraud and constructive fraud. Under constructive fraudulent conveyance laws, a conveyance may be deemed fraudulent despite the parties’ best of intentions. A chief purpose of avoiding transfers unsupported by reasonably equivalent value is to protect unsecured creditors from the depletion of the debtor’s assets. In general, a prima facie case of constructive fraudulent conveyance is proved if it is shown that an insolvent debtor transfers property without receiving reasonably equivalent value. In the above scenario, the pivotal question is whether Company 2 received reasonably equivalent value when it granted Bank a mortgage to secure Company 1’s debt.

Courts find that reasonably equivalent value can be received as either a direct benefit or an indirect benefit. Direct benefits are typically straightforward and easy to spot. For example, there would be no question that a debtor receives a direct benefit when it grants a lender a security interest in property valued at $1 million when the debtor receives a loan from lender in the amount of $1 million. However, the answer becomes less clear when, as in the above scenario, the debtor does not receive the loan proceeds of the loan secured by the debtor’s assets. Company 2 arguably will not receive a direct or indirect benefit if it grants Banks the proposed mortgage since the loan proceeds will go to Company 1 and not Company 2. On the other hand, it could be argued that Company 2 will benefit from the transaction since Company 1 and Company 2 share an “identity of interests.” In other words, because the companies both

---

**IT’S ALMOST IMPOSSIBLE TO KEEP UP WITH EVERY SINGLE FINANCIAL REGULATION. WE SAID ALMOST.**

<table>
<thead>
<tr>
<th>PHONE NUMBER</th>
<th>800-762-2426</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEB ADDRESS</td>
<td><a href="http://www.balch.com">www.balch.com</a></td>
</tr>
</tbody>
</table>
are owned by Acme Home Builder, what benefits one company benefits the other.

The assessment of reasonably equivalent value is a question of fact. Courts review the issue on a case-by-case basis. The Court of Appeals for the Eleventh Circuit has noted that a court must be given “considerable latitude” deciding whether reasonably equivalent value was received in a transaction. Courts have developed no clear guidelines to employ when determining whether an indirect benefit is of sufficient enough to defeat a fraudulent conveyance attack. On several occasions, courts have found that entities are so related that they do share an “identity of interest” such that benefits to one will flow to the other. At the same time, courts also have found that while a benefit was received, it was not concrete enough to constitute reasonably equivalent value.

The Bottom Line
Lenders should be particularly cautious of a transaction that could be scrutinized should one of the parties to the transaction file bankruptcy. By better understanding the law of fraudulent transfers a lender can be better situated to protect itself in the event its borrower defaults.

Leases, New Standard Results in Substantial Changes
by Bill Curtis

After a decade of deliberations, the Financial Accounting Standards Board (FASB) has issued its new lease standard with the publication of Accounting Standards Update (ASU) No. 2016-02, Leases (Topic 842). Banks should evaluate the ASU’s impact on both their loan customers and their own balance sheets and regulatory capital. For public companies, the new rules apply to fiscal years starting after Dec. 15, 2018 (including interim periods within those years). Nonpublic companies have until fiscal years starting after Dec. 15, 2019 (and for interim periods within those years).

Currently, under Generally Accepted Accounting Principles (GAAP), leases are classified either as “capital” or “operating.” Entities are required to recognize capital leases with an asset and liability on the balance sheet, while only disclosing future obligations resulting from operating leases. Today, most leases are off-balance-sheet operating leases. The FASB believes current practice makes it difficult for financial statement users to compare companies that own their assets with companies that lease them. Under the FASB’s new standard, substantially all leases, including today’s operating leases, will be recognized by lessees on the balance sheet through a right-of-use asset and corresponding lease liability.

The new rules classify leases either as “finance” leases (similar to capital leases) or “operating” leases using criteria substantially similar to what is used today to classify leases as either capital or operating. The new standard will require lessees to recognize on their balance sheets assets and liabilities for all leases with terms of more than 12 months, regardless of their classification. In other words, with the exception of short-term leases, off-balance-sheet treatment will be obsolete. Initially, entities will treat all leases similar to capital leases, recording a right-of-use asset and a lease liability. Both the right-of-use asset and lease liability will be measured using the present value of the minimum lease payments over the lease term. The discount rate is the rate implicit in the lease

Our approach to serving clients does more than just meet regulatory requirements. For 98 years our goal has been to build relationships through commitment, quality work and dedication to our clients.
or the lessee’s incremental borrowing rate. Nonpublic entities will be permitted to make an accounting policy election to use a risk-free rate.

Expense recognition will depend on how a lease is classified. For finance leases, entities will amortize the right-of-use asset, generally on a straight-line basis over the life of the lease. For the lease liability, this will be amortized similar to repaying a borrowing by recognizing interest expense and reducing the liability as lease payments are made. This means they’ll recognize higher expenses early in a lease’s life and lower expenses later on. For operating leases, companies will recognize lease expense on a straight-line basis. The lease liability and right-of-use asset for an operating lease will be adjusted to the present value of the remaining lease payments through the life of the lease.

When the new rule takes effect, loan customers with significant operating leases will experience an immediate balance sheet increase in assets and liabilities. The FASB has stated it believes lease liabilities resulting from operating leases should be classified as operating liabilities rather than debt. If loan covenant details do not define the lease liability as operating liabilities rather than debt, this could cause some customers to appear to be in violation of loan covenants that place limits on overall debt or require certain debt-to-equity ratios. The impact on specific borrowers will depend on their particular circumstances and the language of their loan agreements (especially the definition of “debt”).

Bankers should review existing loan covenants and consider modifications to avoid unnecessary contraventions. Keep in mind that the new rules simply change the way operating leases are reported - they have no bearing on a borrower’s creditworthiness or ability to repay. As you review existing loans and discuss new ones, consider developing new covenant models that provide sufficient cushion to withstand upcoming lease accounting changes.

For banks that lease their facilities, equipment or other fixed assets, the new lease accounting rules may have a significant impact on their own balance sheets. It’s still unclear how this will affect regulatory capital calculations. To avoid unpleasant surprises, banks should analyze the potential impact of the new rules well before they take effect. Banks should assess how the new standard will impact their financial statements as well as their systems, controls, and processes surrounding leases. As a first step, consider all your bank’s leases. If you find that recognizing those leases on your financial statements will significantly impact key ratios, then coordinate with any affected counterparties, such as lenders, to address concerns and revise agreements as appropriate. Also, don’t forget to assess internal key metrics and performance measures to determine if and how they may be impacted by this change.

Bill Curtis, CPA, is a partner with Mauldin & Jenkins, LLC in the Birmingham office. Curtis is directly involved in and responsible for service to financial institution clients. Client engagements include opinion audits and tax services for private as well as SEC registered companies, internal control opinion audits, and internal audits, and benefit plan audits.

Inside Verizon’s 2016 Data Breach Investigations Report
by Mike Morris

Threat intelligence has come to the forefront of the financial service industry. In today’s environment, it is critically important to monitor the cyber threat landscape to identify and mitigate emerging risks before they impact our organizations.

Threat intelligence can take several forms, from scanning news headlines to seeing real-world examples (and identifying lessons learned), monitoring cybersecurity court cases, and reading articles that summarize the current threat environment. Threat intelligence is an iterative process. Once threat intelligence is obtained, the next step is to identify what lessons can be learned, whether key mitigating controls (i.e. the controls that can prevent or deter emerging threats) can be implemented (or have already been implemented), and periodically testing these controls for...
effectiveness.

A very good source for threat intelligence is Verizon’s annual Data Breach Investigations Report. The report contains a collection of real-world breaches and details about security incidents that occurred over the previous year. The areas covered include: breach trends, points of focus, vulnerabilities, phishing trends and statistics, and much more.

In this article, we will take a closer look into Verizon’s 2016 Data Breach Investigations Report.

The 2016 report covered 64,199 incidents spread across 21 industries, out of which 2,260 were determined to be breaches. The threat actors identified in these breaches are almost entirely (roughly 80 percent) external to the organizations they are targeting. It is no surprise the nearly 80 percent of the attacks were financial in nature and roughly 12 percent were determined to be espionage.

We preach to our clients the importance of educating employees on reporting suspicious activity, monitoring security logs in a timely manner, having a strong incident response plan and having vetted forensics companies on call, because when a hack occurs, time is of the essence. Verizon’s report justifies our argument. The report notes that 81.9 percent of the breaches took only minutes to achieve and in 98.6 percent of the breaches, information was exfiltrated (i.e. taken out of the organization’s network) in seven days or less (29.3 percent was in 60 minutes or less).

During security testing for our clients, we also identify systems that are missing patches. The root cause is that these systems have not been included in the company’s overall patch management process. The Verizon report confirms this as well. The report states that, “All that patching is for naught if we’re not patching the right things.” The common applications where we identify missing patches include Adobe, Java and VMWare. Ensuring that all applications are included in our regular patch management process can help us strengthen our network environments. The key finding in this area is that older vulnerabilities are still targeted by attackers and that a methodical approach that included all systems is still better than quickly patching only a few systems.

The report reiterated that the main cause of a network breach is still through phishing emails. The main goal of phishing is still to install persistent malware on the user’s machine to gain a foothold to attack a company’s internal network. The key finding related to phishing in the report is that 13 percent of people click on phishing attachments. That number increased from 11 percent in the 2015 Verizon Data Breach Investigations Report. Our recommendations to our clients are in line with the report’s, which is to configure our email systems to filter out unwanted emails from ever reaching our users’ inboxes, which takes the bad decision out of our users’ hands. When we test our clients’ email filters, we almost always find recommendations for improvement. Other recommended controls include: ensuring that there is regular security awareness training and testing, segmenting your user workstations from your servers, and monitoring outbound network traffic.

Once the attacker gets a foothold through a user’s bad decision to click on a phishing email, the hackers will use stolen, weak or default credentials to further their attacks. The key finding related to credentials is that static credentials are still being targeted by both hackers and malware and that 63 percent of data breaches involved weak, default or stolen credentials. During our testing, we consistently find default credentials being used within organizations. Malware containing keystroke loggers can capture a user’s keystroke, negating complexity and password length. Also, easily-guessed passwords are extremely bad, especially when used on static service accounts. Multifactor authentication can help address these issues.

For default credentials, having an installation checklist for new system implementation that addresses the removal of default credentials can go a long way in removing the threat of default credentials within your organization. Removing local administrative rights from user workstations and implementing application whitelisting can assist in keeping the keystroke loggers from infecting your users’ computers. Finally, training your users to never disclose (especially over the telephone) or write down their passwords is extremely important.

Web application attacks are still a significant target of attack, especially in relation to electronic banking applications that allow the transfer for funds. The primary breach is through social engineering attacks on financial institution customers, the use of the Drirdx malware and use of keystroke loggers to capture user credentials. Late last year, a bank’s customer, who could initiate wires and automated clearinghouse transactions through the website, was hacked. The customer used multifactor authentication provided by the bank to help protect the transaction. The hacker realized this and called the customer pretending to be the bank (and used the bank’s name on the caller ID.) The hacker was able to “social engineer” the number on the token used for multifactor authentication and initiate fraudulent wires from the customer’s computer. In these instances, customer security awareness training is paramount in preventing these hacks from occurring. We typically see weak or nonexistent customer security training in these areas. You must also ensure that your vendors providing the e-banking platforms are performing secure coding (i.e. testing application changes for security risks before implementing them in the production environment) and are testing their systems for cyber resilience (i.e. the e-banking systems are secured and regularly tested for vulnerabilities and identified vulnerabilities must be quickly remediated).

Another area covered by the report includes insider and privilege misuse. The Verizon report recommends that we monitor our users closely, block universal serial bus (USB) drives and other mass storage devices from being used in your organization, and being careful of data leakage. Insider abuses can take months, or even years, to identify. We have seen instances where disgruntled employees have attempted to steal customer information to take to another institution as competitive
intelligence. We have also seen insiders use other users’ accounts to hide their activity, such as waiving of NSF fees for their spouses/friends. During our audits, we usually identify active accounts for terminated employees on key systems long after the employees are gone, which could be used for unauthorized access either by the former employees or their coworkers.

The report also noted that in this year’s data, assets were lost more than 100 times more frequently than they were stolen. The primary losses were related to laptop computers, but also include other mobile devices with company information, including smart phones. We are still seeing instances where smart phones, especially those for senior managers who resist the controls, are not encrypted on bring-your-own-device (BYOD) personal smartphones. We also see instances where laptops are not running full-disk encryption. Training users to protect assets and quickly report them when they have been lost or stolen is critical.

Crimeware, especially ransomware, has been growing exponentially over the last few years, and that trend is expected to continue. Also, “command and control” (a.k.a. “C2”) malware, that includes keystroke loggers, is another area that continues to grow. According to the Verizon report, C2 attacks are still among the top threat to power hackers are trying to get in; however, ransomware is a close second and has closed the gap significantly this year. According to the report, the three major ways that the crimeware is getting installed includes email attachments, web drive by attacks (where users browsing an infected website can get infected) and email hyperlinks. We previously mentioned the importance of email filters and user training to help thwart the risks of email attachments.

The training can also help thwart emails with hyperlinks, although automatically clicking on hyperlinks is a hard habit for users to break. Also, you must patch your browsers and other web surfing tools, such as Adobe Flash. Finally, it is time to revisit your web surfing filters and block all unneeded categories to prevent users from browsing to non-business-related websites. We also need to strengthen our user computers (a.k.a. “endpoints”) using antimalware/antivirus software, removing local administrative rights, considering application whitelisting to only allow approved applications to run on user machines, and removing Windows Powershell, disabling the ability to run Macros.

In summary, it is critical that your organization implement a threat intelligence process to identify emerging risks and to implement controls to mitigate those risks. This article is only discussing the high-level information contained in the report; it is a valuable exercise for your organization to read and react to the information in the report. The annual Verizon Data Breach Investigations Report is a great resource to include in your threat intelligence arsenal to help you better secure your network from current risks and to look for trends that may lead to future risks.

Mike Morris, CISA, CISSP, is Systems Partner at Porter Keadle Moore.

**Appellate Court Decision Holding CFPB Unconstitutional Promises Significant Implications**

In a landmark decision, the U.S. Court of Appeals for the D.C. Circuit held that the Consumer Financial Protection Bureau’s (CFPB) structure violated the Constitution’s separation-of-powers requirements. In PHH Corporation v. Consumer Financial Protection Bureau, No. 15-1177 (D.C. Cir., filed 2015), a majority of the Court held that the CFPB’s structure violated the Constitution because the agency was headed by a single director who could only be removed by the president for cause. The unanimous panel further held that the CFPB had erred in its statutory interpretation of RESPA (as well as its refusal to honor past regulatory guidance of the statute), and thus reversed the large damages imposed against PHH. The decision has significant implications, not just to the lending community, but also to any highly regulated industry.

**Background**

In 2014, the CFPB brought an administrative enforcement action against PHH Corporation, a mortgage lender, alleging violations of certain anti-kickback provisions in Section 8 of the Real Estate Settlement Procedures Act. PHH defended against the claims, arguing that its conduct was based on express statutory guidance authored by the Department of Housing and Urban Development, when it was the agency charged with interpreting the statute. An administrative law judge found in favor of the CFPB and ordered PHH to disgorge approximately $6.5 million in illegal fees. PHH used the administrative procedure to appeal to the CFPB’s Director, who not only affirmed PHH’s liability, but increased the disgorgement amount to $109 million. PHH then sought judicial review of the agency decision in the U.S. Court of Appeals for the D.C. Circuit.

**D.C. Circuit Holds Statute Unconstitutional**

In a lengthy opinion written by Judge Brett Kavanaugh and joined in full by Senior Judge Raymond Randolph, the Court held that because the CFPB is headed by a single director who can be removed by the president only for cause, it was neither an executive agency nor an independent agency that comport with the Constitution’s separation-of-powers requirements. The Court began by noting the fundamental role the separation-of-powers doctrine serves in the U.S. Constitution and the long-standing precedent from the Supreme Court maintaining that, in order for a regulatory agency to be constitutionally constructed, it must either be accountable to the president as an executive agency or a true independent agency. The Court further held that central to an agency’s independent status is its governance by a board of commissioners or directors instead of a sole director. The Court based this requirement on two principles: (1) the reasoning behind the Supreme Court’s decision in Humphrey’s Executor v. United States, 295 U.S. 602 (1935) that recognized the constitutional validity of independent agencies based on their ability to operate as “a body of experts appointed by law and informed by experience,” and (2) longstanding historical
practice and precedent of structuring independent agencies to be headed by a panel of commissioners or directors. After analyzing and ultimately distinguishing two of the three examples offered by the CFPB of other independent agencies headed by a sole independent director (the Court noted CFPB’s proposed example of the Federal Housing Finance Agency, but declined to take it as an example of historical practice given that it was created around the same time as the CFPB), the Court concluded that CFPB’s organizational structure was unprecedented in independent agency history. Based on recent decisions from the U.S. Supreme Court in Free Enterprise Fund v. Public Company Accounting Oversight Board, 561 U.S. 477 (2010) and NLRB v. Noel Canning, 134 S. Ct. 2550 (2014), which emphasized the role of historical practice in addressing separation-of-powers questions, the Court concluded that the CFPB’s novel structure gave too much unaccountable power to the agency and its director and therefore held it to be unconstitutional.

Although the Court concluded that the CFPB’s structure violated the Constitution, the Court stopped short of ordering the agency to unwind operations. Instead, it ordered that the restriction on removal of the director only “for cause” should be stricken. Having ordered that provision stricken, the Court deemed it to be severed from the rest of the statute, allowing the CFPB to continue to operate as an executive agency. The Court considered the possibility of ordering the CFPB to be reorganized into a multi-member body, but declined to do so given the possibility of gridlock over appointments, as well as the threat of judicial overreach. However, the Court did note that Congress had the option of enacting legislation reorganizing the agency in that fashion. That may prove to be the most expedient approach, given the danger (or at least perceived danger) of abrupt, politicized decision-making by an agency that is completely beholden to the president.

Having addressed the headline-grabbing constitutional issue, the Court then turned to address the merits of the case—which, despite the lack of fanfare, may prove more meaningful in practice for institutions subject to the CFPB’s regulatory reach. The Court ruled against the CFPB on both of the merits issues presented for review, holding that the agency could not penalize a company for actions conducted in reliance on previous agency guidance concerning an interpretation of federal law and that the CFPB was in fact limited to a three-year statute of limitations in bringing administrative enforcement actions against firms allegedly in violation of regulations.

Senior Judge Randolph joined the majority decision authored by Judge Kavanaugh, but also wrote separately to express his belief that the administrative law judge that initially considered the case against PHH and wrote a recommendation should have been considered an “inferior Officer” under the Constitution, and thus was not properly appointed to the case when he was assigned by an administrative law judge acting on behalf of the Securities and Exchange Commission and CFPB. Judge Karen Henderson dissented from the majority’s constitutional holding, noting that she did not believe the Court needed to reach that issue, but joined the majority’s holdings regarding the merits of the CFPB’s claims.

Implications of Ruling
The scope of the Court’s constitutional ruling remains to be seen. In other instances where courts have held that regulatory agencies were unconstitutionally structured, the remedy was to undo the effect of any administrative enforcement actions still pending, although the agency retained the ability to start over again with its enforcement efforts under a new constitutional structure. The PHH Court avoided that issue by choosing to address the merits of the CFPB’s interpretation of the statute. Going forward, however, major questions remain unanswered regarding the effect of past and pending agency enforcement conduct, which, according to the D.C. Circuit Court, has taken place under an unconstitutional structure. Factors such as the finality of the rulings in those actions and their method of resolution (i.e., a contested adjudication versus a settlement) will probably dictate whether those rulings remain fully binding. We anticipate those issues to be vigorously litigated in the coming weeks and months.

Aaron Chastain is an associate with Bradley and represents financial services institutions, healthcare companies, and other businesses in a broad range of litigation and compliance-related matters.
Want to Start a Bank?
by Jenny McCain and Ryan Brooks

It has been a while since there has been any meaningful activity in the chartering of de novo banks. We are far from the pre-Recession heyday of the early and mid-2000s, when approximately 140 new banks were formed in the United States annually. In fact, during the five-year period from 2010 to 2015, only two new banks were chartered nationwide. It has been nearly nine years since our banking attorneys formed the last two new banks chartered by the state of Alabama that are still in operation: Oakworth Capital Bank, based in Birmingham (opened March 31, 2008), and Progress Bank & Trust, based in Huntsville (opened Feb. 4, 2008). The extreme decline in bank charters over the last decade, coupled with an increasingly burdensome regulatory environment and historically low interest rates, have led many observers to wonder whether de novo banks are merely a relic of community banking’s gilded past.

Against this backdrop, the FDIC held an outreach meeting at its Atlanta office on Nov. 29, 2016, as part of its Community Banking Initiative that explored the process for acquiring and maintaining a de novo charter in a post-Great Recession world. The meeting’s presenters included representatives of the OCC and state banking departments (the chartering authorities for national and state banks, respectively), as well as the Federal Reserve and FDIC. The FDIC has hosted similar events in a few of its other district offices in recent months. To our knowledge, these meetings are the first of their kind for the FDIC, and we believe that the FDIC’s effort to reignite the conversation about the de novo chartering process bodes well for the future of community banking. However, the clear message from the meeting was that, while the regulators are ready, willing and even eager to work with applicants in obtaining charters and deposit insurance, interested parties should be prepared to undergo an intensive application process and to be subject to close scrutiny during the entire de novo period. Other key takeaways from the meeting are described to the right.

The application procedure itself is largely unchanged. The mechanics of the chartering process have not changed in several years. As in the past, the process is driven by the state or federal chartering authority, in conjunction with the FDIC, who separately but concurrently considers the application for deposit insurance. The Federal Reserve may or may not be involved at a later point, depending on whether the bank desires to be a member of the Federal Reserve System or to create a bank holding company.

A specific but flexible business plan is critical. As in the past, the business plan remains one of most important components of the application. The challenge for applicants will be finding the “sweet spot” between including a reasonable level of specificity and providing sufficient flexibility from the outset to take advantage of unforeseen business opportunities. Among other things, the business plan must show that the bank will achieve profitability within the first three years of operation and must be based on “reasonable and supportable” assumptions.

Capital is still king. Perhaps one of the greatest shifts in the balance of the factors considered in chartering a new bank is the extent to which capital adequacy drives the ultimate decision from the regulators. In short, both the structure and amount of a proposed bank’s capitalization are of particular interest to the regulatory authorities. The bank’s capital structure should be tangible and transparent and based primarily on loss-absorbing common equity, and key investors should also be able to demonstrate a sound financial history. Enhanced vetting is likely for any foreign, institutional or particularly large investors. Moreover, the capital projections included in the application should clearly show that capital levels are sufficient to support operations through at least the first three years of operations, providing for a leverage ratio of at least 8 percent throughout, without reliance on "just in time" capital.

The people make the bank. As those who have been through the biographical and financial reporting process can...
attest, regulators have a keen interest in knowing as much as possible about the background and qualifications of a bank’s decision makers. Candidates who served at failed or troubled banks could be rejected unless they can establish that they were not personally responsible for the prior bank’s troubles (such as those brought in to turn around a failing bank). Applicants whose business plans reveal an elevated risk in a particular risk area, such as BSA/AML or cybersecurity, must also demonstrate a plan for adequate staffing in these areas.

Compliance issues should be addressed upfront. In the post-Dodd-Frank regulatory environment, the authorities are particularly interested in the control systems that the applicant intends to implement to ensure compliance with a number of laws, specifically including the Community Reinvestment Act and fair lending statutes. Among other things, applicants should propose a reasonable and executable plan for the adoption of appropriate policies and procedures, employee training, ongoing monitoring by the board and management, handling consumer complaints and auditing the effectiveness of the bank’s programs. The presenters emphasized that compliance is the ultimate responsibility of management and cannot be outsourced away. As a result, applicants should be prepared to submit a carefully considered plan for third-party vendor management, compliance staffing and related matters.

At the close of the meeting, the FDIC emphasized that it is “ready and waiting” for new banks to apply for deposit insurance and that it looks forward to candid and productive communications with interested parties throughout the application process. This is a new message from the regulators.

Jenny McCain is co-chair of Maynard Cooper’s Banking Group. With more than 17 years of experience, Jenny is recognized by The Best Lawyers in America for Banking Law and by Chambers USA: America’s Leading Lawyers for Business for Bank Regulatory expertise. Ryan is an associate in the Banking, Securities Regulation & Corporate Finance, Mergers & Acquisitions and Cybersecurity practices at Maynard Cooper. Ryan’s practice is focused on helping clients in the financial services industry navigate the complex regulatory framework governing their operations.