ALABAMA BANKERS ASSOCIATION

BOARD**BRIEFS**

A NEWSLETTER FOR ALABAMA'S BANK DIRECTORS

JANUARY/FEBRUARY 2019 • VOLUME 4 • NUMBER 1

IN THIS ISSUE

Three Takeaways from the Ascension Data Breach

by Fob James, Burr & Forman

On Jan. 23, TechCrunch reported that more than 24 million mortgage and banking documents were left exposed on the internet in an unprotected environment for approximately two weeks. Ascension, which provides data analytics and document management services to the financial industry, stored sensitive documents, some of which were a decade old, on an unprotected server that anyone with an internet connection could potentially access. The exposed documents were part of a service provided by Ascension where it converts paper documents to electronic format. These documents belonged to customers of some of the largest banks in the country, including Wells Fargo, Citigroup, and Capital One. The information exposed included sensitive personally identifiable information such as customer names; addresses; dates of birth; social security numbers; and account numbers. It is unclear at this time whether hackers accessed this treasure trove of data and sold it on the black market.

This incident illustrates three key concepts that banks should implement to mitigate the loss of sensitive customer data and reduce risk.

First, banks should focus on developing policies that promote data storage minimization. If the bank stores less data, especially personally identifiable information ("PII"), the risk and resulting impact of a breach decreases. Data disposal is also required under Alabama law. Specifically, Alabama's Breach Notification Law ("SB318") requires businesses to dispose of records containing sensitive PII pursuant to law, business need, or regulation.

Implementing a solid data disposal policy also makes breach notification easier on the back-end. For example, the Ascension breach exposed documents going back to 2010. If the bank and/or its vendors unnecessarily maintain records of former customers, and do not maintain those customers' current contact information post-breach, the bank runs the risk of having to notify those customers by publication through major media outlets and the bank's website. This method can be costly and a public relations nightmare. For the data and records that the bank must maintain pursuant to law or business need, the key is properly storing that data and maintaining updated customer contact information.

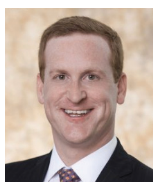
Second, the bank should encrypt PII that the bank or its vendors store electronically. This is one of the best methods to protect data because even if a hacker obtains access to encrypted files, customers' PII remains protected in many cases. The records exposed in the Ascension breach were not encrypted, thus the data was free for a hacker to download with minimal effort. Had Ascension encrypted the data with a secure encryption key, a hacker would have been required to jump through significant hoops in order to unlock the data. With such a barrier in place, the transaction cost is high, and a hacker is likely to focus on an easier target.

Like data disposal, encryption is helpful on the back-end of a breach. Under most states' breach notification laws (e.g., SB318), encrypted data is exempt from reporting and notification requirements unless there is reason to believe the encryption key was also misappropriated.

Third, as part of the bank's vendor management program, the bank should make sure that agreements with third-party vendors that process or store customer data include indemnification provisions so the bank is indemnified from any liability in connection with the loss of data while under the vendors' custody or control. Vendors should be required to represent that they will adhere to state, federal, and international privacy laws (if applicable). Ideally, vendors should also agree to: (i) implement data protection programs and maintain robust data security policies and procedures; (ii) maintain adequate cybersecurity insurance; and (iii) report any breach and/or handle breach response, including any breach notification or reporting requirements.

While the three takeaways above are not an exhaustive approach to mitigate liability and prevent intrusions, they should be considered by banks that are interested in protecting customer data.

Fob James is an attorney in Burr & Forman LLP's Birmingham office where he practices in the firm's Cybersecurity and General Commercial Litigation practice groups.



The Beneficial Ownership Rule – An Overview

by Charles R. Moore III, Bradley

On May 11, 2018, a new rule—commonly referred to as the Beneficial Ownership Rule—took effect to establish additional customer due diligence requirements for banks and other financial institutions. The Financial Crimes Enforcement Network (FinCEN) issued the rule under the Bank Secrecy Act as part of its anti-money laundering (AML) framework. This article serves as a refresher for banks as they continue to work through the requirements of the Beneficial Ownership Rule.

General Rule; Helpful Resources

Under the Beneficial Ownership Rule, federally insured banks and other covered financial institutions must establish and maintain written procedures that are designed to identify and verify ***beneficial owners*** of ***legal entity customers***. Generally speaking, this means that when an entity customer opens a ***new account*** at a bank, the bank must ***identify*** and ***verify*** the identity of each individual who owns 25 percent or more of the entity, and one individual who controls the entity.

As with many rules that apply to banks, the details of the Beneficial Ownership Rule are important. Certain terminology, including the definitions of "beneficial owner," "legal entity customer," "new account," and "account," provide exceptions to the rule's general requirements. In addition, in both the rule itself and related publications, FinCEN addresses common scenarios, frequently asked questions, and other considerations related to the rule.

Key points of the Beneficial Ownership Rule are addressed below. For additional information, institutions can access the full rule at 31 C.F.R. § 1010.230 and can find FAQs and other guidance from FinCEN on FinCEN's website at https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule.

Identification and Verification

The Beneficial Ownership Rule requires banks and other covered institutions to have risk-based customer due diligence procedures that enable them to:

(a) Identify the beneficial owner(s) of each legal entity customer at the time a new account is opened. An institution may accomplish this either by obtaining a certification on a FinCEN-developed form, or by obtaining the information required by the form by another means.

(b) Verify the identity of each beneficial owner identified to the institution, according to reasonable and practicable risk-based procedures. For banks, those procedures must contain—at a minimum—the elements required for verifying the identity of customers that are individuals under the Customer Identification Program (CIP) rules. Those elements generally consist of the individual's name, date of birth, address, and identification number.

An institution may rely on the information supplied by the legal entity customer's representative regarding the identity of its beneficial owner or owners, provided that the institution has no knowledge of facts that would reasonably call into question the reliability of the information.

Definition of "Beneficial Owner"

The Beneficial Ownership Rule defines the term "beneficial owner" to mean each of the following:

(a) Each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer. This is the "ownership prong" of the rule.

(b) A single individual with significant responsibility to control, manage, or direct a legal entity customer, including (1) an executive officer or senior manager (e.g., a CEO, CFO, COO, managing member, general partner, president, vice president, or treasurer); or (2) any other individual who regularly performs similar functions. This is the "control prong" of the rule.

For any particular legal entity customer, the number of individuals that must be identified as "beneficial owners" under the rule will vary from one to five. Under the ownership prong, up to four individuals—and as few as zero individuals—must be identified, depending on their ownership percentages. Under the control prong, one individual must be identified. It is possible that in some circumstances the same person or persons might be identified pursuant to the ownership prong and the control prong.

Definition of "Legal Entity Customer"

The term "legal entity customer" means (a) a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or similar office, (b) a general partnership, and (c) any similar entity formed under the laws of a foreign jurisdiction that opens an account. The definition of "legal entity customer" does not reach sole proprietorships or unincorporated associations, because neither is a separate legal entity from the associated individual(s).

While the definition of "legal entity customer" covers many entities that banks deal with on a day-to-day basis, several types of legal entities are given special exclusions from the definition. Those exempt entities include, among others, many state or federally regulated financial institutions, state or federal departments or agencies, publicly-traded companies, other SEC-reporting companies, registered investment companies and advisers, registered public accounting firms, and state-regulated insurance companies. Institutions should consult the full rule and the FinCEN resources cited above when considering whether an entity is exempt from the Beneficial Ownership Rule.

Notably, if an exempt entity owns 25 percent or more of the equity interests of a legal entity customer, no individual need be identified for purposes of the ownership prong with respect to that exempt entity's interests. (If an individual related to an exempt entity has significant responsibility to control, manage, or direct a legal entity customer, however, the individual may need to be identified under the control prong.)

Definitions of "New Account" and "Account"

The Beneficial Ownership Rule largely focuses on due diligence that must be conducted at the opening of a "new account," which means an account opened by a legal entity customer on or after May 11, 2018. As applied to banks, the term "account" means a formal banking relationship established to provide or engage in services, dealings, or other financial transactions, including a deposit account, a transaction or asset account, a credit account, or other extension of credit. The term "account" also includes a relationship established to provide a safe deposit box or other safekeeping services, or cash management, custodian, and trust services.

The term "account" does not include a product or service where a formal banking relationship is not established with a person, such as check-cashing, wire transfer, or sale of a check or money order. The rule and its accompanying guidance also exempt certain other types of accounts from its scope, including certain types of accounts to finance insurance premiums, certain types of accounts to finance the purchase or leasing of equipment, and rollovers of certain CD accounts.

FinCEN views loan renewals, CD rollovers, and similar events as new banking relationships, and therefore as "new accounts" for purposes of the Beneficial Ownership Rule. FinCEN acknowledges, however, that the industry generally does not treat those types of events as new relationships. Accordingly, FinCEN has issued guidance that relieves institutions of collecting beneficial ownership information upon the rollover of most CDs, the renewal of safe deposit box rentals, and the renewal of some loans, commercial lines of credit, and credit card accounts, if the renewal does not require underwriting review and approval (see FIN-2018-R004 for details). For other types of loan renewals, FinCEN requires institutions to either collect beneficial ownership information at each renewal after May 11, 2018, or to have their customers re-confirm beneficial ownership information previously submitted. Notably, though, if a legal entity customer certifies its beneficial ownership information to an institution in connection with a loan, and the customer also agrees to notify the institution of any change in its information, the institution may rely on that agreement as an ongoing certification for subsequent renewals of that loan, absent knowledge to the contrary (see FAQ #12, FIN-2018-G001, for details). Institutions should consider adding this type of customer agreement to their loan and renewal documents.

Conclusion

In an effort to further curb money laundering activities, the Beneficial Ownership Rule imposes new due diligence requirements on banks and other financial institutions. Under the rule, institutions must identify between one (1) and five (5) "beneficial owners" of their "legal entity customers," and they must verify the identity of those individuals. The rule applies to the opening of "new accounts," which generally include both newly originated accounts and renewals and rollovers of existing accounts, subject to certain exceptions.

Although this article raises the key points of the Beneficial Ownership Rule, it does not cover many of the subtleties of the rule. Institutions can find significant guidance on the rule in both the rule itself (31 C.F.R. § 1010.230) and on FinCEN's website (https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule).

Charles Moore is a partner with Bradley. He has substantial experience in commercial finance, including mortgage warehouse lending, real estate finance, and bank holding company lending. Moore also commonly handles change in bank control act matters, bank holding company act matters, formation and capital raising activities of banks and bank holding companies, and other bank regulatory matters.

Credit Concentration Risk Management Back in Regulatory Focus

by Chris Couch, McGlinchey Stafford

Late last year the Office of the Comptroller of the Currency identified "concentration risk management" as a top supervisory concern for 2019. Subsequently, the Federal Reserve raised interest rates twice, the US economy witnessed the worst annual returns for the main equity benchmarks since 2008 and stocks witnessed the worst December since 1931. As a result, Boards should revisit the idea of concentration risk, how to identify it, and strategies for mitigating it.

As the Comptroller's Handbook points out, concentration risk is a close cousin to credit risk:

> Credit risk management does not conclude with the supervision of individual transactions, it also encompasses the management of pools of exposures whose collective performance has the potential to affect a bank negatively even if each individual transaction within a pool is soundly underwritten. When exposures in a pool are sensitive to the same economic, financial or business development, that sensitivity may cause the sum of the transactions to perform as if it were a single, large exposure.

Issue

Loans to unrelated borrowers that share a common characteristic could pose considerable risk to a bank's earnings and capital where the common characteristic becomes a source of weakness. For instance, loans to separate real estate developers or home builders may have very different borrower profiles and sound underwriting. Each, however, may be exposed to long-term interest rates in that the ultimate take-out financing is driven by consumer purchases. Given the disparity among borrowers, these loans might be expected to perform independently of each other. Their common exposure to consumer end-users, though, particularly when geographically similar, may make them perform (or underperform) as a common whole.

Additional Complication

As the example above indicates, concentrations can accumulate across products, geographies and business lines. This can make concentrations harder to spot and harder to protect against. Products containing the same types of risks under different labels and in different units can mask some exposures and risks. On their face, HELOCs and developer loans may not seem to have much in common. Given their shared exposure to long-term interest rates, though, a Board might want to review them collectively.

Defining Concentrations

From a regulatory perspective, "concentrations" are aggregate commitments and exposures – on a firm-wide basis – that exceed 25 percent of the bank's capital. Not all pools will support this threshold, though, and banks should determine – based on volatility, correlation to other pools, and similar measures – how narrowly to define "concentration" for any given pool. From an underwriting perspective, Boards should consider the following (among other things) when assessing pools and concentrations:

- interrelations among counterparties/borrowers
- common sources of repayment (including guarantors)
- independent borrowers with common suppliers or customers
- common industries and economic sectors
- geographic location or areas served

Mitigation

Once identified, Boards should recognize that mitigation strategies vary from pool to pool. Some include:

- Modify underwriting standards to strengthen credit portfolio
- Expand portfolio to include non-correlated borrowers
- Actively monitor and manage low-quality assets
- Sell participations or whole loans
- Alter exposure limits or credit risk standards
- Hold additional capital to adjust for the additional risk

The fundamental responsibility for identifying and managing concentration risk lies with the Board. In light of the OCC's supervisory priorities for the year and the topsy-turvy nature of the current economy, directors should revisit their bank's approach to concentrations, correlated pools, and the risk associated with each.

Chris Couch is a partner in McGlinchey Stafford's Financial Institutions practice, where he advises banks and boards of directors on corporate compliance, operational risk, and commercial lending matters.

Watch Out for Personal Liability Under the FDCPA

by Brian Malcom, Waller

The Second Circuit recently upheld a court order holding two individual co-owners and co-directors of several corporate debt collector entities personally liable for over $10 million after such entities violated the Federal Trade Commission Act (FTCA) and the Federal Fair Debt Collection Practices Act (FDCPA).

In Federal Trade Commission (FTC) v. Federal Check Processing, Inc., the FTC brought suit against 13 corporate debt collector entities and the two co-owners and co-directors of those entities. The FTC alleged that the defendants' combined debt collection practices violated the FDCPA and FTCA. The corporate defendants' business consisted primarily of collecting payday loan debts, which they bought from consumer-debt creditors and compiled into debt portfolios.

The U.S. District Court for the Western District of New York granted summary judgment. In so doing, the court found that the co-owners and co-directors directed nearly all of their approximately 25 employees, telephone debt collectors, to routinely contact debtors by telephone and falsely identify themselves as "processors," or law enforcement personnel, accuse debtors of check fraud or a related crime, and threaten the debtors with criminal prosecution if they did not pay their debts.

Moreover, on certain occasions, the collectors called friends, family members, employers, or co-workers of debtors, informing them that the debtors owed a debt, had committed a crime in failing to pay it, and faced possible legal repercussions. If debtors or other interested parties sought further information about the debt, the collectors typically refused to provide such information. The court held that the corporate defendants had violated the FTCA and FDCPA, and that the two individual co-owners and co-directors were personally liable for $10.85 million, the amount of money that the defendants had received because of the violations.

On appeal, one of the individual defendants did not contest the district court's conclusion that the corporate defendants violated the FTCA and FDCPA. Instead, he argued that the court erred by concluding that he was personally liable for the violations and setting the measure of equitable monetary relief as the total proceeds of the debt collection enterprise. The Second Circuit, however, affirmed the district court's ruling that the individual defendant had both sufficient authority over the corporate defendants, as well as knowledge of their practices, to be held individually liable for their misconduct as a matter of law. Indeed, the individual defendant was a co-founder, co-owner, co-director, and general manager of all but potentially one of the corporate defendants. He also maintained a personal office within the corporate defendants' office and a desk in the "collection call" area from which dunning calls were made by the companies' employees. Finally, he had signature authority with respect to the companies' bank accounts, and in the more than four years at issue, received approximately $1.3 million in compensation from the corporate defendants.

Further, the Second Circuit concluded that the district court's disgorgement assessment was in an appropriate amount because it was a reasonable approximation of the total amounts received by the defendant companies from consumers as a result of their unlawful acts.

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.

Disrupt or Die: The Community Bank's Guide to the BB&T - SunTrust Merger

by Murray Bibb, Porter White & Co.

It was a run-of-the-mill Thursday morning — save for the record high temperatures approaching 80 degrees during the first week of February 2019 — as I was enjoying a pre-daylight cup of coffee and reading the *Wall Street Journal* on my iPad®, when a news alert appeared that caught my attention. The headline read, "BB&T and SunTrust to Combine in Merger of Equals to Create the Premier Financial Institution." Wait, what?!? Did I need another cup of coffee? Had I misread the article? Was this #FakeNews?

The answers were all "no," although I did have another cup of coffee…or two. Purely on the surface the tie-up appeared to make all the sense in the world. The initial shock was simply that there had not been a bank deal anywhere near the size and significance of the proposed MOE between Winston-Salem, NC-based BB&T Corp. and Atlanta, Ga.-based SunTrust Banks, Inc. since the high-priced stock deals of the mid-2000s. In fact, the day prior to the announcement, one veteran bank analyst wrote a timely opinion piece championing the returns generated from the operating leverage, or scale, derived from successful MOEs.

To be clear, this article isn't about the BBT-STI merger per se. However, for context alone, the combination — an all-stock transaction valued at approximately $66 billion — is the 8th largest U.S. bank deal ever (as ranked by deal value at the time of announcement) and is the single largest U.S. bank deal since the J.P. Morgan-Bank One merger in 2004, creating the 8th largest bank holding company in the U.S. with $442 billion in assets.

Since it's probably not a stretch to assume that if you are still reading this, then the merger announcement caught your attention as well. And what often gets lost in the midst of all the water cooler talk around pricing multiples (1.77x of tangible common equity and 10.0x earnings) and management teams (almost uncomfortably egalitarian) are the ways that strong competitors look to take advantage of the intended and unintended consequences of a deal as significant as the BBT-STI merger.

Retaining (good) customers is a constant battle given the current competitive forces, causing bankers to often spend as much time focused on not losing accounts as opposed to generating new ones. Large-scale operating changes involved in a complex merger can also give more reason for competitors to recruit a bank's most valuable asset: its human capital. Conversely, if any banking talent becomes disenchanted throughout a merger process, the deal can become exactly their incentive needed to explore different opportunities.

A prima facie case of how industry consolidation can impact a banking landscape can be seen no further than in Birmingham. When banks merge, operations staff are almost always "stream-lined." But when banks merge with overlapping footprints, client-facing employees are also displaced, voluntarily or involuntarily. Even today in Birmingham, it isn't uncommon to hear someone mention Central Bank of the South and First Alabama Bank, or even more contemporary name likes AmSouth and SouthTrust, when referring to local banking giants like Regions, BBVA Compass and Wells Fargo. The point is that people identify with and are loyal to other people, often much more than they are to the company that person represents. For further proof, look no further than the organizers' resumes of the many successful de novo banks and bank re-capitalizations in Alabama over the last 15 years.

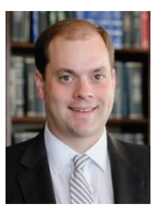
Possibly the most curious part of the BBT-STI announcement was the revelation of plans for the combined company to establish a new corporate headquarters in Charlotte, N.C. under a new brand. Even though the company will maintain its community banking and wholesale banking centers in Winston-Salem and Atlanta, this decision could be an unnecessary risk to add to the already challenging process of merging two banks that each have over $200 billion in assets.

Interestingly, BB&T and SunTrust have surprisingly little retail overlap given their respective sizes in the southeast. According to estimates, the combined company will have to divest ap-proximately 740 branches with $1.27 billion of deposits, mostly focused around Atlanta, Washington, D.C. and Miami. Beyond mandatory divestitures, the extent of any plans to consolidate or shutter other branches is unknown. Conveniently though, the topic of retail networks is the perfect segue into the final item we'd like to discuss, which is giving more than a perfunctory consideration of branch sales.

No amount of market research or feasibility study can be done to gauge the decision-making process of retail and commercial customers. Of course, a certain amount of customer attrition is always assumed from any merger; however, fintech advances combined with the unabridged access to information have commoditized certain financial services products to the point that switching costs have effectively been eliminated.

Considering the attractiveness of low-cost core deposits in the current banking environment, there would likely be a long line of suitors interested in purchasing any branch under consideration to be closed. Now, a 10 percent premium on a branch with $20 million in deposits might amount to a little more than a rounding error on the financials of larger institutions. So, while the upside of selling branches on a discretionary basis may be limited, it can far outweigh the potential liability of carrying the real estate for closed or unprofitable branches.

As the old adage goes, the long-term success of any business combination depends on three things: execution, execution and execution. The BBT-STI merger will be followed closely by banks of all shape and sizes to see not only how they might benefit from any potential disruption from the deal, but also how the current regulatory framework in Washington will consider big bank M&A in the coming years.



Murray Bibb is an investment banker with Porter White & Company in Birmingham.

Your Organization has Grown: Now What? A Few Considerations

by Jenny McCain, Maynard Cooper & Gale

As your bank grows either organically or through a merger/acquisition, it's important to make sure the internal operations, overall organizational structure and "governance" considerations grow with it. Banking organizations that have historically operated in the $100-$200 million asset size face new considerations when they cross the $250-$300 million benchmark. Operations activities that historically may have been more informal in nature should be reconsidered. For instance, management needs to be sure accounting, risk and product decisions are adequately documented within the institution. Additional loan and deposit compliance resources will be needed (which means additional expenses need to be budgeted). On the staffing side, the chief lending and chief credit officer positions are often split once a bank reaches the $250-$300 million size. The bank and holding company's organizational chart should be reviewed to determine whether any new management is needed, in particular whether a chief operations officer or similar position is needed. Internal audit is generally still outsourced. It's important also to make sure your compensation plans are competitive as your institution grows. At the board level, make sure you include organizational risk and strategic planning in your board's agenda and discussions.

Once your bank has $500 million in assets as of the first day of its fiscal year (based on its most recent 12/31 call report), additional accounting and internal control federal regulatory requirements come into play, including requirements for annual independent audits, additional requirements that apply to the board's audit committee, and annual report by management on compliance with S&S laws and ICFR. In addition to other requirements/criteria, audited financial statements must include HUD-mandated testing and report from the audit firm. The federal regulations also include specific requirements that the audit firm must meet. From an internal perspective, the board's audit committee must be comprised of outside directors, a majority of which are independent of management. The audit committee must meet at least quarterly. Management has requirements regarding internal controls and reporting once a banking organization reaches this $500 million threshold. Clearly, more formal procedures and reporting becomes necessary at this point in bank's life cycle. A board of directors should (1) maintain a board approved set of written criterial for determining whether a director serving on the audit committee is an outside director and is independent of management and (2) consider the "independence" issue" not only from the standpoint of the individual director, but also from the position (standpoint) of the persons or organizations with which the director has an affiliations.

These are just a few of the issues that banking organizations and their management need to consider as they cross key asset thresholds. We advise many bank holding company and bank boards and CEOs on how to prepare for growth and what to do once they reach the next asset level, whether it be $250 million, $500 million, $1 billion or more.

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.

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

2019 CONVENTION & TRADE SHOW

JUNE 9-12

The Broadmoor
Colorado Springs, Colorado