Texas Bank Report

Texas Department of Banking, Charles G. Cooper, Commissioner

February 2022

In This Issue:

Succession Planning
Fintech Partnerships
Application Pitfalls
Virtual Currency Custody Services

Commissioner's Comments

"I commend Texas banks for their efforts in serving the needs of their customers in these unique times ..."

If asked in March 2020, I doubt anyone believed that we would still be dealing with COVID-19 and its various strains in January 2022. Yet here we are, and the virus continues to be amongst us.

Many observers anticipated tough times for the financial service industry in the early days of the pandemic. However, nearly two years later, this has not transpired as most state-chartered banks are doing well, and asset quality issues are limited. I commend Texas banks for their efforts in serving the needs of their customers in these unique times while protecting their health and the health of their employees.

That is not to say there are no challenges facing Texas banks. Deposits have grown significantly since year-end 2019 and, given low interest rates – at least for the time being – and equally low loan demand, the result has been a significant decline in net interest margins.

Another concern driven in part by the pandemic has been an exodus of tenured employees from the workplace. Faced with an aging workforce, it is imperative that your bank create or update its succession plans for board members and key executive staff. I encourage you to review the status of your bank's current personnel and board situation due to the importance of such planning.

Whether we are in good or bad times, the banking industry is increasingly threatened by cybercrime. This risk was highlighted in late 2021 by the discovery of another flaw, this time in an obscure but widely used piece of internet software known as Log4j. It is similar to some other vulnerabilities that you have received alerts on. These cyber alerts can be so frequent that we can be tempted to discount them. While they may be more commonplace, risk management practices need to remain robust.

As of this writing, the heightened geopolitical tensions in eastern Europe increase the probability of cyber threats to the financial sector. I cannot overstate the importance of remaining vigilant against these threats. Cybersecurity is everyone's responsibility, and we all must do a better job.

On a positive note, the Texas economy continues to rebound despite the emergence of the Omicron variant of COVID-19. December labor market data from the Texas Workforce Commission reports the state's unemployment rate was 5.0%, down from 5.4% at the beginning of fourth-quarter 2021. Nearly every major industry group expanded at years end, led by the state's energy sector which comprises so much of Texas' overall business activity.

Our economy is as dynamic as it is diverse with a strong and varied base of production categories as well as ongoing emergence in several sectors. Texas continues to present an attractive environment for doing business, as demonstrated by the recent relocations of Tesla, Oracle, Samsung, and Hewlett-Packard, to name just a few corporations that now call the state home.

The future of the Texas economy continues to remain bright. In the meantime, we hope you enjoy this latest edition of the Texas Bank Report and offer you best wishes for a successful 2022.

Charles G. Cooper
Banking Commissioner

Authority of Texas State-Chartered Banks to Provide Virtual Currency Custody Services to Customers

Industry Notice 2021-03 (republished)

Issued June 10, 2021

This notice affirms that Texas state-chartered banks may provide customers with virtual currency custody services, so long as the bank has adequate protocols in place to effectively manage the risks and comply with applicable law.

Texas state-chartered banks have long provided their customers with safekeeping and custody services for a variety of assets. These services play a crucial role in the business of banking as customers look to banks to offer secure and dependable storage. While custody and safekeeping of virtual currencies will necessarily differ from that associated with more traditional assets, the Texas Department of Banking believes that the authority to provide these services with respect to virtual currencies already exists pursuant to Texas Finance Code § 32.001.

Virtual currency is an electronic representation of value intended to be used as a medium of exchange, unit of account, or store of value. Virtual currencies do not exist in a physical form. Instead, they are intangible and exist only on the blockchain or distributed ledger associated with that virtual currency. The owner of the virtual currency holds cryptographic keys associated with the specific unit of virtual currency in a digital wallet. The keys enable the rightful owner of the virtual currency to access and utilize it further.

What virtual currency custody services a bank chooses to offer will depend on the bank's expertise, risk appetite, and business model. For instance, the bank may choose to allow the customer to retain direct control over their own virtual currency and merely store copies of the customer's private keys associated with that virtual currency. Alternatively, the bank may cause the customer to transfer their virtual currency directly to the control of the bank, creating new private keys that are then held by the bank on behalf of the customer. As with the method of custody services, several secure storage options are available to the bank, each of which has distinctive characteristics pertaining to level of security and accessibility. The bank will have to determine which storage option best fits the circumstances.

The Department has previously determined that custody services may be provided by a Texas state-chartered bank in either a fiduciary or non-fiduciary capacity. In providing such services in a non-fiduciary capacity, the bank acts as a bailee, taking possession of the customer's asset for safekeeping while legal title to that asset remains with the customer. The extent of the bank's duties regarding the asset depends on the custodial agreement between bank and customer but generally, the bank owes its customer the duty to use proper care to keep the asset safely and to return it unharmed upon request.

A bank proposing to offer custody services in a fiduciary capacity must possess trust powers, which may require a charter amendment and/or compliance with 7 Texas Administrative Code § 3.23 prior to doing so. In its fiduciary capacity, the bank has the authority to manage virtual currency assets as it would any other type of asset held in such capacity.

Prior to a bank entering a new line of business, such as offering virtual currency services, it is incumbent on management to conduct due diligence and carefully examine the risks involved in offering a new product or service through a methodical risk assessment process. Should management and the board of directors decide to move forward, effective risk management systems and controls must be implemented to measure, monitor, and control relevant risks associated with custody of digital assets.

Necessary controls consist of administrative controls, such as policies and procedures; technical controls, such as access controls and authentication; and physical controls, such as protection of hardware and data specific to the virtual currency held. The bank should also confirm the existence of adequate coverage with its insurance carrier.

Due to the technical nature of holding virtual currency, the bank may choose to establish a relationship with a service provider with expertise in handling virtual currency. Therefore, it is incumbent on the bank to maintain a strong service provider oversight program that addresses risk in the service provider relationship from the first steps of due diligence through a potential termination of the service provider relationship. More information on outsourcing technology services can be found in the Federal Financial Institutions Examination Council's *IT Examination Handbook for Outsourcing Technology Services*.

If you have any questions regarding the provision of virtual currency custody services, please contact Marcus Adams, Assistant General Counsel, via email at marcus.adams@dob.texas.gov or by phone at (512) 475-1236.

Succession Planning is Planning for Success

By: Gordon Anderson

Succession planning, for a variety of reasons, is a topic often unaddressed by community banks.

Between establishing and monitoring policies and procedures, keeping pace with regulatory changes, navigating cybersecurity concerns, and overseeing the bank's overall performance, bank boards of directors have multiple and significant responsibilities. Its members may simply not have had the time to develop a solid succession plan.

The issue can also be a sensitive one, much like discussing your will with family members. As some community banks are family owned; the issue can become even more delicate. Finally, some board members may just not know how develop a plan or where to start.

At its most basic level, a succession plan is a strategy for transferring roles when key individuals resign or retire, and the lack of one can leave your bank in a vulnerable position. Having a plan in place can help stabilize your bank's operations and avoid disruptions when a long-tenured director or officer departs. Plus, succession plans offer banks an opportunity to assess the skills and competencies of potential executives and identify and cultivate these individuals.

Directors often come from the ranks of the legal profession or business professions that require certain aptitudes and skill sets. However, just as boards seek to diversify the business backgrounds of its members to enhance its pool of knowledge and expertise, a good succession plan is also your opportunity to address another element often missing among board members: a diversity of age.

Age diversity in the boardroom is an important consideration. According to Bank Director magazine, the median age of board members who participated in a 2019 compensation survey was 64. Seventy-two percent of CEOs surveyed were 55 or older, and 2% were older than 74.

A range of ages among board members allows for the transfer of practical experience and institutional knowledge, which can help transition your bank into the future. Plus, younger members may have a greater appreciation for technology than older members and be better positioned to offer counsel and insight regarding mobile banking, virtual currencies, cybersecurity, and other aspects of our modern financial system.

There are, however, a myriad of challenges facing community banks when considering the topic of succession. This is especially true for small and rural banks, where the depth of talent may be limited relative to larger institutions.

The Department suggests keeping various characteristics in mind when searching for a successor, including the following:

Honesty and Integrity	Puts bank interest ahead of personal Avoids actual & perceived conflicts of interest in life, work, and while serving Thinks independently, rather then simply following the pack
Engagement	Is inquisitive Provides constructive guidance and opinions Asks tough questions and expects satisfactory answers Voices constrcutive dissent when appropriate
Analytical Skills	Draws analogies between past experiences and current challenges Is willing to lean and develop new skills Is strategically engaged but operationally distant
Business	Possess financial, business and managerial acumen Actively engages in the field of employment Has connections with other businesses and industries
Community	Has knowledge of the communities served Actively engages in and with community groups
Banking	Has a basic understanding of banking, regulatory systems, laws, and regulations Is willing to fill knowledge gaps
Has Time To	Learn the business & pursue professional development opportunities Staying abreast of bank affairs Commit to Board Activities - Preparing and attending meetings, reviewing examination and audit reports, & ensuring responsiveness
Complementary Attributes	Independent of bank management Posesses a skill set that complements those of the other directors Has skills that support the bank's long-term vision Enhances board member diversity

Promoting an existing bank officer may be the preferred route, but it may not always be possible. Conversely, electing an outside director may not always be easy. Being elected to the local bank's board once bestowed a certain status on a member of the community. That may no longer be the case, as the fear of personal liability may dissuade some individuals from seeking a leadership position.

Finding qualified candidates within the community who understand the complexities of the banking industry may also be an obstacle difficult to overcome.

One avenue you may consider exploring to solve this dilemma is to invite members of the community to serve as an advisory director. Serving in an advisory capacity allows these individuals to learn more about the banking industry and determine if they have the time, let alone the desire, to serve as a director.

Another bonus to this approach is it allows the current directors a chance to evaluate the candidates and determine who is the best fit for this important role. However, banks are reminded that confidential information may not be disclosed to an advisory director unless the board minutes reflect an appropriate business need for such a disclosure and the disclosure is made pursuant to a written confidentiality agreement between the bank and the advisory director.

Drafting a succession plan will not be accomplished overnight. Developing the right strategy for your bank will require much thought, frank conversations with your board, and time to seek out prospective board members.

All of which means you should not put crafting a plan off any longer. Start the discussion now and make it your board's top priority. After all, it is your bank's roadmap for future success.

Remember Your CISO When Planning for Succession

By: Gordon Anderson

Just as the development of a succession plan for directors is essential for ensuring the business continuity of your bank, it is equally essential your institution develop a similar plan for your Chief Information Security Officer (CISO).

It is true that every employee is responsible for supporting your institution's information security, compliance procedures, and cybersecurity efforts. However, no one plays a more critical role than the CISO, but the position is often among the most difficult to fill due to a limited pool of qualified applicants and a highly competitive market.

Yet many banks approach CISO succession planning as an afterthought. Research by Bank Director magazine shows that while acknowledging the importance of a succession plan, less than half of banks responding to a 2018 survey reported having a long-term and emergency succession plan in place. Twenty-five percent of executives and board members who participated in the survey expressed dissatisfaction with their bank's planning efforts.

Succession planning can significantly reduce staffing uncertainties and ensure continuity in your information security/cybersecurity processes. Given your CISO is responsible for Federal Financial Institution Examination Council (FFIEC) compliance and regulatory requirements, any slip up in these areas can result in operational, regulatory, and reputational risks. Additionally, the CISO is a critical second line of defense that is necessary for effective challenge of technology controls and management of risk across your organization.

Banks, therefore, must be prepared and know how to proceed in the event the CISO leaves, is unavailable for an extended period, or unable to perform his or her job functions. This requires not only identifying alternate staff members for this key position, but also adequately training them well in advance.

This is more than just good business sense. The FFIEC IT Examination handbook requires banks to include cross training and succession planning in your business continuity plan, ensuring backup personnel are identified not just for this but all key positions.

Strategies for succession planning will necessarily differ depending on the size, type, and goals of your institution. However, Safe Systems, a Georgia-based provider of IT services to community banks and credit unions, suggests some basic steps to follow:

- Assess requirements and responsibilities — A good place to begin the planning process is to understand the primary responsibilities, expertise, and requirements of the CISO position. Although this continues to evolve, Safe Systems identified 35 distinct elements in seven categories ranging from information security to BCP, Business Continuity Planning, Vendor Management, and Strategic IT planning.

- Evaluate internal talent — Identify which employees may be the most qualified to take on these tasks, bearing in mind that you will likely need multiple resources. Commit to cross training these individuals through hands-on training, classroom education, and mentorship.

- Recruit externally — If there is a shortage of internal talent to fill the CISO role, institutions might consider identifying potential resources outside their organization, such as a virtual ISO service.

A succession plan for your bank's CISO is a matter of information security. Should any breach appear in your operations, it could impact your institution across the spectrum: senior management, employees, customers, shareholders, and other stakeholders. You need to get this right the first time.

However, banks should remember succession planning in general is not a one-and-done undertaking. Because of the evolving nature of information security/cybersecurity, it is a continual exercise, and succession plans should be reevaluated on a regular basis and updated as needed.

Effective succession planning and cross training will make any transition involving your CISO a more positive experience for everyone in your institution.

Bank Application Pitfalls

By: Jared Whitson

The Department experienced an increase in conversion, de novo charter, and bank merger and acquisition (M&A) applications in 2021. The post-pandemic economic recovery continues to gain momentum, making the Lone Star State an attractive destination in which to conduct business. Furthermore, consolidation in the banking industry continues primarily to promote synergies and improve economies of scale, enhance digital capabilities, diversify credit risk, retain/obtain talented employees, or expand geographic footprint. With consolidation, however, comes opportunities for de novo organizations to start with a clean slate, possibly utilizing technological advances to grow organically.

While management's initial focus might be centered on the market reaction of a planned merger, regulatory expectations should also be considered to ensure a smooth transaction that closes within the applicants desired timeframe. Applications via conversion, M&A or de novo charter should consider the following elements:

* Communicate with your regulators as soon as possible. Depending on the type of application, an examination of the target bank may be necessary which could extend the application process. Additionally, the Department recommends contacting regulators prior to application submission to address any questions or con-

cerns, help facilitate the transaction, and obtain insight to potential areas of concern.

* Implications of putting key processes and projects on hold in anticipation of a merger should be carefully considered. The target bank is expected to continue operating until consummation. The Department's expectation is that sound risk management processes will continue until consummation of the sale.

* For M&A applicants, the expectation is banking services will continue at all locations post acquisition. The Department will require that banks continue providing at least the same level of services to their communities, and that the market area is not abandoned.

* Key executive management positions should be determined prior to submitting the application. The expectation is the applicant will have identified all key employees for the organization, and ensured they are qualified to perform their duties. For all proposed executive officers, especially the chief executive officer, the individual should have prior experience performing this role. In addition, consideration to who will constitute the board of directors needs to be well thought out.

* In any situation, ensure integration risks with the target bank are appropriately identified. The expectation is that enhanced due diligence will be performed to identify risks with the proposed merger or acquisition. The application should provide specific action plans outlining how these risks will be mitigated during the integration process. Systems integration and cost are also essential with planned mergers to ensure business continuity. Banks have experienced post acquisition operating issues due to inefficiencies from redundant, incompatible, or outdated systems and systems integration failures resulting in operational losses.

* For mergers of equal applicants, the expectation is the surviving institution will have robust risk management processes post acquisition. This is especially applicable for larger organizations that substantially increase in asset size. Policies and procedures governing enterprise risk management, audit, information technology and BSA/AML programs are expected to be sufficient for the size of the institution.

* When filing an application, ensure the capital structure is adequate for the planned market area and proposed activities. This is especially relevant for de novo applications entering major metropolitan areas (i.e., Dallas, Houston, Austin, San Antonio). While the level of capital is primarily dictated by the business plan, organizations in larger market areas, based on current conditions, are typically expected to have at least $30-$35 million in capital to be competitive in these markets under a traditional banking model. Smaller markets typically are not required to have this level of capital. In fact, while the Department welcomes de novo applications of all sizes, we particularly encourage applications for banks in the smaller and rural markets. Recently, groups have also been increasingly interested in utilizing technology to deliver products and services as a key part of their business plan, which can help reach a broader market. Regardless of the approach, the expectation is capital levels will accommodate the risk outlined in the proposed business plan and sustain the entity's capital needs for the first three years following consummation. The applicant should explain in detail why the capital structure is adequate based on the market area and proposed business plan.

* Confirm the correlation between the business plan and projections is reasonable. The business plan should incorporate management's vision and encompass all proposed business lines. If technology delivery systems are an integral part of the bank's business model, the projections need to be realistic in terms of growth and capitalization levels. The business plan should mirror the proformas submitted with sound assumptions. The assumptions used should provide granular detail validating the reasonability of the proformas. Proformas should include base, worst, and best scenarios with consideration for economic impacts, interest rates, loan growth, etc. Prior to submitting the application, an independent, third-party review of the business plan should be performed.

If you have any questions relating to applications, contact Corporate Director Mark Largent at mark.largent@dob.texas.gov or 512-475-1351.

Fintech Partnerships with Banks

By: Jesse Moore and Kevin Wu

The rapid pace of change within the financial services industry continues to be driven by customer preferences, constant innovation, access to new technology and, more recently, the effects of the pandemic. The landscape of financial services is constantly evolving, creating unique market opportunities as well as challenges. Financial institutions face many hurdles as they strive to remain competitive, maintain customer retention, attract new customers, improve customer experience, grow deposits, enhance operational efficiency, and increase lending, all while meeting established business goals and implementing the strategic plan.

To address these opportunities and obstacles, banks and fintech companies are increasingly establishing partnerships to improve the bank's operational efficiencies, allow fintech companies access to payment systems, provide the bank with new customers, and/or diversify the bank's funding sources. These partnerships also present additional opportunities for banks to develop new or unique market niches, diversify income streams, and provide more appealing or targeted products to customers.

In Texas, the economic conditions and business environment are ideal for innovation, and fintech companies are increasingly seeking to partner with Texas banks. Furthermore, fintech has emerged to address the challenging employment environment and fill operational gaps at some community banks with new hardware, such as interactive teller machines and video chat capabilities to enhance website-based customer service. The rapid growth in the virtual currency industry is resulting in the convergence of virtual currency related fintech companies with other major components of the financial services industry.

The Federal Reserve issued guidance in September 2021, Community Bank Access to Innovation through Partnerships that focuses on the benefits, risks, and challenges posed by operational technology partnerships, customer oriented partnerships, and front-end fintech partnerships. Bankers should be cautious about rushing to remain competitive as unnecessary legal and reputation risk may result if customer data is not protected properly, or regulatory issues may arise if the bank has not ensured compliance in all areas.

Partnership Types

- **Operational Technology Partnerships** seek to reduce errors, improve efficiencies, and reallocate employees and resources to other areas. Technology solutions for customer relationship management, marketing, workflow prioritization solutions, credit underwriting, fraud detection, BSA/AML reporting, and/or security enhancements function in the background to improve efficiencies and productivity. Ensuring resources, staff training, and technical expertise are available to manage these new technology solutions is vital for banks adopting new platforms.

- **Customer-Oriented Partnerships** focus on customers' needs from banks, such as facilitating the opening of new accounts with online tools, integrating third-party applications for person-to-person money transmission, enhancing existing mobile deposit platforms, and even possibly offering virtual currency custody fiduciary services for wealth management customers. These partnerships also provide agility and resilience for banks needing to remain consistently operational for customers, as well as to improve customer service in times of duress such as the rapid rollout of the Paycheck Protection Program. During the pandemic, bankers adopted or expanded the use of many existing technologies that in prior years were not even considered viable.

- **Front-End Partnerships** are less common but seek to enhance a bank's existing technological capabilities while partnering with a fintech's growing digital customer base.

Fintech partnerships offer online mortgage applications, new debit card features, and many other services; however, these new companies often have little to no experience with bank supervision and regulation. Enhanced oversight over these partnerships is needed to be consistent with due diligence expectations from a vendor management perspective. Careful contingency planning is important when conducting due diligence, to evaluate the disconnection costs and other associated fees. Previous guidance issued by federal and state banking agencies remains applicable for conducting due diligence.

It Starts with Due Diligence

Committing to innovation and establishing a sound due diligence process are important decisions the board of directors of a community bank must analyze prior to engaging in a fintech partnership. Additionally, managing risks in cybersecurity, credit, operational fraud, insurance, etc., needs to be ongoing and performed consistently with the bank's board-approved due diligence program and vendor management program. Appropriate audits must be performed, and adequate policies, procedures, and internal controls established to guide the partnership and protect the bank's interests. Community banks that partner with fintech companies with aligned strategies, priorities, and objectives (regarding purpose, regulatory compliance, and common technologies utilized) are best positioned for success.

The due diligence process requires banks to manage a variety of potential risks, and a significant amount of information must be obtained and analyzed – possibly through on-site visits, audit reports, filings, and other independent reviews of the company. A review of the fintech company's information security program and proposed contractual obligations should be among the key items to evaluate. For example, some business plans resulting from a proposed fintech partnership may require the fintech to obtain a money transmission license or obtain a written determination from the Department regarding licensing requirements.

Third-Party Risk Management

Third-party risk management has evolved and involves a thorough process. Developing the necessary digital and technical infrastructure may be necessary with a fintech partnership. For these situations, a comprehensive analysis must be performed on the technical connections, interfaces, and legal obligations of all parties regarding data governance issues, customer privacy-related data, or even customer account login credentials. Furthermore, the legal agreements must be carefully drafted to comply with multiple regulatory agencies and ensure prioritization, protection, and privacy of the bank's confidential customer data. The Federal Financial Institutions Examination Council: Outsourcing Technology Services Booklet dated June 2004 provides comprehensive guidance for outsourcing technology services to third parties.

More recently, third-party risk management program guidance was modernized to incorporate the industry changes as outlined in August 2021 by the FDIC, Federal Reserve, and OCC: Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks. Expanding upon the previously established Vendor Management concepts, this new guidance evaluates six key topics all banking organizations should incorporate into their due diligence and analysis regarding these fintech companies. Many of these concepts are built upon examination principles and procedures, and although familiar the guidance provides specific case studies and other detailed discussions for review.

1. **Business Experience and Qualifications:** Reviewing the business experience and expertise, strategic goals, and qualifications are necessary to determine the partnership's ability to meet the bank's needs.
2. **Financial Condition of the Fintech Company**: Analyzing financial reports, reviewing audit reports, requesting public filings, and understanding funding sources are similar to credit underwriting concepts and necessary to determine the future viability of the company.
3. **Legal and Regulatory Record of Compliance**: Evaluating the fintech company's legal and regulatory knowledge and posture, its experience in the industry and regulatory framework, and any additional available public filings are other tools necessary to assess the company properly.
4. **Risk Management and Internal Controls**: Risk management policies, procedures, and processes should be documented and available for sharing. The company's internal control environment should be assessed to determine its level of sophistication. Audits should be requested and reviewed to determine the effectiveness of the company's risk management and internal controls.
5. **Information Security Framework and Operations**: The company's Information Security framework is vital to understanding how the bank's customer data can be protected, privacy ensured, and staff training/testing is ongoing.
6. **Operational Resiliency**: Can operations continue through a variety of disruptions? Program continuity and change management concepts should be incorporated into the due diligence review to determine if continuity and resilience planning is commensurate with the critical nature and type of activities that the company is handling for the bank. Requesting business continuity, incident response planning, disaster recovery plans, training plans, and test results are all elements that need to be reviewed and analyzed.

Virtual Currency Custody Services

The Department issued Industry Notice 2021-03 on June 10, 2021, to affirm that Texas state-chartered banks may provide virtual currency custody services. Virtual currency and digital commodities represent another class of assets in which Texas state-chartered banks have the authority to provide safekeeping and custody services for their customers. It should be noted that if a bank is proposing to offer these unique custody services in a fiduciary capacity, the entity must possess trust powers.

The industry notice outlines regulatory expectations and focuses on proper due diligence, vendor management programs, and risk management systems and controls relevant to the custody of digital assets. The adequacy of insurance is another factor to be considered prior to entering a new line of business like this.

Licensing

Legal, contractual, and licensing are additional important considerations to be evaluated when entering into a fintech partnership. Banks must determine if licensing is required for any fintech companies providing money services, money transmission, currency exchange, and/or other financial services in Texas. Under the Texas Money Services Act (§ 151.003(5) of the Texas Finance Code) a company acting in an agency capacity for a bank is excluded from licensing and regulation provided that the Department has issued a written determination letter that the statutory conditions for the exclusion are satisfied. The business plan, flow of funds, marketing materials, and contracts and agreements are all key considerations in such a determination.

Bank-Related Marketing by NonBanks

Banks partnering with nonbank fintech companies should also ensure that their nonbank partners do not violate the Texas Banking Act, §§ 31.004-31.005 of the Texas Finance Code, by falsely implying that the fintech itself is a bank or offering banking services. A nonbank cannot falsely "represent to the public that it is conducting the business of banking" in Texas and cannot use the term "bank" or a similar term or a character "in a manner that would imply to the public that the person is engaged in the business of banking" in Texas.

As the Department noted last year in Supervisory Memorandum 1043, under this law "there is no permissible way" for a nonbank fintech to partner with a bank to "offer a 'white-labeled bank account' or white-labeled banking services under circumstances where a nonbank holds itself out as the entity offering a 'bank' account or other banking services." Any fintech marketing materials using "banks", "banking," or related terms must "reasonably identify the banks providing the actual banking services" to ensure the nonbank fintech does not violate the Texas Banking Act by falsely holding itself out as a bank.

The Department and other state banking regulators have been working to address the ongoing problem of false advertising by nonbanks. The Department expects Texas banks to protect their own customer goodwill and brand loyalty as required by Texas law by ensuring their nonbank fintech partners adequately credit and acknowledge the bank itself as providing the banking services being advertised.

If you have any questions regarding fintech partnerships, please contact Dan Frasier, Director of Bank and Trust Supervision, at 512-475-1322 or via email at dan.frasier@dob.texas.gov.

Resources and References:

June 10, 2021

- Texas Department of Banking Industry Notice 2021-03: *Authority of Texas State-Chartered Banks to Provide Virtual Currency Custody Services to Customers*

- Referenced in Department Virtual Currency Industry Notice: Federal Financial Institutions Examination Council (FFIEC) IT booklet *Outsourcing Technology Services*

September 2021

- Federal Reserve System's *Community Bank Access to Innovation through Partnerships*

August 27, 2021

- Federal Deposit Insurance Corporation's FIL-59-2021: *Conducting Due Diligence on Financial Technology Companies – A Guide for Community Banks*

- Federal Reserve Bank's SR 21-15/CA 21-11: *Guide for Community Banking Organizations Conducting Due Diligence on Financial Technology Companies*

Financial Highlights

TABLE I
Quarterly Balance Sheet and Operating Performance Ratios
for Texas State-Chartered Commercial Banks 9/30/2021 Through 9/30/2020

ACCOUNT DESCRIPTIONS (IN MILLIONS OF $)	9/30/2021	6/30/2021	3/31/2021	12/31/2020	9/30/2020
Number of State-Chartered Banks	215	217	216	217	218
Total Assets of State-Chartered Banks	412,751	365,132	354,297	345,339	330,445
Number of Out-of-State, State-Chartered Banks Operating in Texas	48	48	45	45	45
Total Texas Assets of Out-of-State, State-Chartered Banks Operating in Texas	85,338	85,338	83,858	83,858	83,858
Subtotal	498,089	450,470	438,155	429,197	414,303
Less: Out-of-State Branch Assets/Deposits	-72,689	-72,689	-64,512	-64,512	-64,512
**Total State Banks Operating in Texas	425,400	377,781	373,643	364,685	349,791
BALANCE SHEET (Tx. State-Chartered Banks)					
Interest-Bearing Balances	71,432	52,631	47,826	48,445	31,727
Federal Funds Sold	895	692	1,188	1,165	998
Trading Accounts	1,477	1,222	856	857	931
Securities Held-To-Maturity	17,232	16,091	13,926	12,425	11,623
Securities Available-for-Sale	73,868	65,594	61,346	58,380	55,788
Total Securities	91,275	81,685	75,272	70,805	67,411
Total Loans	221,489	203,121	203,909	203,825	205,040
Total Earning Assets	385,091	338,129	328,195	324,240	305,176
Premises and Fixed Assets	5,244	5,168	5,153	5,148	5,082
Total Assets	412,751	365,132	354,297	345,339	330,445
Demand Deposits	66,746	51,592	44,296	44,171	39,007
MMDAs	205,003	179,590	174,771	164,165	157,982
Other Savings Deposits	29,349	30,477	35,707	33,778	32,601
Total Time Deposits	35,063	34,006	34,197	34,357	34,115
Brokered Deposits	7,971	4,959	5,595	5,627	5,568
Total Deposits	349,668	308,524	299,687	286,638	273,031
Federal Funds Purchased	3,403	3,446	3,052	3,839	3,036
Other Borrowed Funds	7,634	5,479	5,484	9,177	9,808
Total Liabilities	366,828	322,564	312,962	304,431	290,719
Total Equity Capital	45,922	42,568	41,335	40,908	39,727
Loan Valuation Reserves	2,793	2,653	2,833	2,937	2,965
Total Primary Capital	48,715	45,221	44,168	43,845	42,692
Past Due Loans > 90 Days	315	404	489	430	364
Total Nonaccrual Loans	1,076	1,039	1,101	1,175	1,113
Total Other Real Estate	159	165	174	188	197
Total Charge-Offs	174	90	48	572	433
Total Recoveries	102	61	29	96	71
Net Charge-Offs	72	29	19	476	362
INCOME STATEMENT					
Total Interest Income	8,431	5,175	2,538	10,499	7,880
Total Interest Expense	556	340	175	1,135	925
Net Interest Income	7,875	4,835	2,363	9,364	6,955
Total Noninterest Income	3,126	2,030	1,103	3,850	2,847
Loan Provisions	(407)	-354	-179	1,356	1,276
Salary and Employee Benefits	3,822	2,390	1,192	4,497	3,292
Premises and Fixed Assets Expenses (Net)	697	446	220	873	644
All Other Noninterest Expenses	1,870	1,154	552	2,345	1,745
Total Overhead Expenses	6,389	3,990	1,964	7,715	5,681
Securities Gains (Losses)	45	22	14	215	216
Net Extraordinary Items	0	0	0	0	0
Net Income	4,151	2,670	1,389	3,644	2,584
Cash Dividends	1,568	791	379	2,293	1,509
RATIO ANALYSIS					
Loan/Deposit	63.34%	65.84%	68.04%	71.11%	75.10%
Securities/Total Assets	22.11%	22.37%	21.25%	20.50%	20.40%
Total Loans/Total Assets	53.66%	55.63%	57.55%	59.02%	62.05%
Loan Provisions/Total Loans	-0.24%	-0.35%	-0.35%	0.67%	0.83%
LVR/Total Loans	1.26%	1.31%	1.39%	1.44%	1.45%
Net Charge-Offs/Total Loans	0.03%	0.01%	0.01%	0.23%	0.18%
Nonperforming+ORE/Total Assets	0.38%	0.44%	0.50%	0.52%	0.51%
Nonperforming+ORE/Primary Capital	3.18%	3.56%	3.99%	4.09%	3.92%
Net Interest Margin	2.72%	2.86%	2.88%	2.89%	3.03%
Gross Yield	3.72%	3.95%	4.11%	4.16%	4.32%
Return on Assets	1.34%	1.46%	1.57%	1.06%	1.04%
Return on Equity	12.02%	12.54%	13.44%	8.91%	8.65%
Overhead Exp/TA	2.06%	2.19%	2.22%	2.23%	2.29%
Equity/Total Assets	11.13%	11.66%	11.67%	11.85%	12.02%
Primary Capital/Total Assets+LVR	11.72%	12.30%	12.37%	12.59%	12.80%

*Unrealized gains/losses are already included in equity capital figures.
**Total State Banks Operating in Texas includes branches of out-of-state, state-chartered banks.
Data was derived from the FDIC website.

Financial Highlights

TABLE II
Comparative Statement of Condition
Commercial Banks Domiciled in Texas
September 30, 2021 and September 30, 2020

ACCOUNT DESCRIPTIONS (In Millions of $)	9/30/2021 STATE CHARTERED		9/30/2021 NATIONAL CHARTERED		9/30/2021 ALL BANKS		9/30/2020 ALL BANKS	
Number of Banks	215	% TA	157	% TA	372	% TA	387	% TA
BALANCE SHEET								
Interest-Bearing Balances	71,432	17.3%	19,367	13.6%	90,799	16.4%	60,985	12.2%
Federal Funds Sold	895	0.2%	2,409	1.7%	3,304	0.6%	2,051	0.4%
Trading Accounts	1,477	0.4%	16	0.0%	1,493	0.3%	1,052	0.2%
Securities Held-To-Maturity	17,232	4.2%	4,885	3.4%	22,117	4.0%	13,981	2.8%
Securities Available-For-Sale	73,868	17.9%	30,437	21.4%	104,305	18.8%	81,559	16.4%
Total Securities	91,275	22.1%	35,356	24.9%	126,631	22.8%	95,540	19.2%
Total Loans	221,489	53.7%	77,417	54.5%	298,906	53.9%	306,260	61.5%
Total Earning Assets	385,091	93.3%	134,549	94.8%	519,640	93.7%	464,836	93.3%
Premises & Equipment	5,244	1.3%	1,741	1.2%	6,985	1.3%	6,897	1.4%
TOTAL ASSETS	412,751	100.0%	141,991	100.0%	554,742	100.0%	498,320	100.0%
Demand Deposits	66,746	16.2%	34,980	24.6%	101,726	18.3%	41,741	8.4%
MMDAs	205,003	49.7%	38,968	27.4%	243,971	44.0%	222,558	44.7%
Other Savings Deposits	29,349	7.1%	21,014	14.8%	50,363	9.1%	54,312	10.9%
Total Time Deposits	35,063	8.5%	16,468	11.6%	51,531	9.3%	54,571	11.0%
Brokered Deposits	7,971	1.9%	858	0.6%	8,829	1.6%	11,759	2.4%
Total Deposits	349,668	84.7%	123,167	86.7%	472,835	85.2%	415,315	83.3%
Fed Funds Purchased	3,403	0.8%	1,567	1.1%	4,970	0.9%	4,503	0.9%
Other Borrowed Funds	7,634	1.8%	176	0.1%	7,810	1.4%	15,289	3.1%
TOTAL LIABILITIES	366,828	88.9%	127,042	89.5%	493,870	89.0%	441,572	88.6%
Equity Capital	45,922	11.1%	14,949	10.5%	60,871	11.0%	56,402	11.3%
Allowance for Loan/Lease Losses	2,793	0.7%	1,069	0.8%	3,862	0.7%	4,211	0.8%
Total Primary Capital	48,715	11.8%	16,018	11.3%	64,733	11.7%	60,613	12.2%
Past Due >90 Days	315		54		369		448	
Nonaccrual	1,076		496		1,572		1,784	
Total Other Real Estate	159		45		204		260	
Total Charge-Offs	174		81		255		721	
Total Recoveries	102		44		146		104	
INCOME STATEMENT	Y-T-D		Y-T-D		Y-T-D		Y-T-D	
Total Interest Income	8,431	100.0%	3,210	100.0%	11,641	100.0%	11,954	100.0%
Total Interest Expense	556	6.6%	212	6.6%	768	6.6%	1,464	12.2%
Net Interest Income	7,875	93.4%	2,998	93.4%	10,873	93.4%	10,490	87.8%
Total Noninterest Income	3,126	37.1%	1,442	44.9%	4,568	39.2%	4,200	35.1%
Loan Provisions	(407)	-4.8%	68	2.1%	(339)	-2.9%	1,825	15.3%
Salary & Employee Benefits	3,822	45.3%	1,545	48.1%	5,367	46.1%	5,029	42.1%
Premises & Fixed Assets (Net)	697	8.3%	296	9.2%	993	8.5%	960	8.0%
All Other Noninterest Expenses	1,870	22.2%	902	28.1%	2,772	23.8%	2,819	23.6%
Total Overhead Expenses	6,389	75.8%	2,743	85.5%	9,132	78.4%	8,808	73.7%
Securities Gains(Losses)	45	0.5%	16	0.5%	61	0.5%	260	2.2%
Net Extraordinary Items	0	0.0%	0	0.0%	0	0.0%	0	0.0%
NET INCOME	4,151	49.2%	1,460	45.5%	5,611	48.2%	3,701	31.0%
Cash Dividends	1,568		529		2,097		2,045	
Average ROA	1.34%		1.37%		1.35%		0.99%	
Average ROE	12.02%		12.99%		12.26%		8.73%	
Average TA ($ Millions)	1,920		904		1,491		1,288	
Average Leverage	11.13%		10.53%		10.97%		11.32%	
Dividends/Net Income	37.77%		36.23%		37.37%		55.26%	

*Unrealized gains/losses are already included in equity capital figures.
Table includes only banks domiciled in Texas. Branches of out-of-state banks are not included.
Data was derived from the FDIC website.