

Fintechs and Banks – A Journey Toward Meeting Customers Where They Are

The Transition to a Digital Bank

A Paper Presented to the Institute of International Economic Law
at Georgetown University Law Center
DC Fintech Week 2020

Eric J. Schuppenhauer, *President,*
Consumer Lending, Citizens Financial
Group

John R. Rosenfeld, *President, Direct*
Banking, Citizens Financial Group

Andrew Rostami, *Head of Consumer*
Unsecured Lending, Citizens Financial
Group

Matthew J. Greenberg, *Senior*
Cybersecurity and Privacy Counsel, Senior
Vice President, Citizens Financial Group

Jack P. Drogin, *Esq, Shareholder,*
Murphy & McGonigle, P.C.

Anna Lysyanskaya, *Professor of*
Computer Science, Brown University

9/30/2020

INTRODUCTION – WHAT DOES A SUCCESSFUL DIGITAL BANK LOOK LIKE?¹

The transition to digital banking from conventional banking was inevitable. Now, because of the COVID-19 pandemic, it is imminent. Given that the pace of this change is likely to be fluid, this paper is an attempt by the authors to establish a baseline and to discuss the current state of the fintech-banking relationship during one of the most challenging times in recent memory. We are confident, however, that this transition will be a successful one because its foundation is customer-centric. Nonetheless, success in this effort can be advanced or held back by the quality of the policies which impact this work. Hence, as this transition continues to gain momentum, the best policies will be crafted so as to promote customer centricity.

The Continuing Essential Nature of Traditional Banks.

It is self-evident that banks are essential in ensuring the continuity of functions critical to the economic and national security of the United States. During the COVID-19 Pandemic, the U.S. Department of Homeland Security, Cybersecurity & Infrastructure Security Agency (CISA) designated financial institutions as essential to the continued critical operational functions of the country and as a result, permitted employees working in branches, wire rooms and call centers, among others, to report to work every day during the COVID-19 response.² In addition, despite the restrictions contained in state executive orders related to face-to-face interactions with customers, banks made it a priority to look after their customers who had no choice but to visit an in-person location by setting up special hours for at-risk customers and implementing health and safety protocols to keep those locations safe for both employees and customers. Banks also implemented various relief programs to reduce the burden of the pandemic.³

¹ The authors note that the views expressed herein are solely their own and do not necessarily reflect the views of Citizens Financial Group or any of its subsidiaries or affiliates. The authors also acknowledge the insights and advice provided by members of the Citizens' Legal Department: Keith Woodman, Joel S. Barras and Stephen T. Gannon.

² Advisory "Memorandum on Ensuring Essential Critical Infrastructure Workers Ability to Work During the Covid-19 Response" (Aug. 18, 2020), https://www.cisa.gov/sites/default/files/publications/Version_4.0_CISA_Guidance_on_Essential_Critical_Infrastructure_Workers_FINAL%20AUG%2018v3.pdf.

³ American Bankers Association, "America's Banks are Here to Help," (survey of bank response to pandemic, last updated June 30, 2020), <https://www.aba.com/about-us/press-room/industry-response-coronavirus>.

For consumers, banks issued fee waivers, payment deferrals, and early CD withdrawals without penalty. For business customers, banks instituted fee waivers for Cash Management services, late fee and overdraft fee waivers, and were instrumental in the Paycheck Protection Program that helped Commercial and Business Banking customers keep workers employed amid the pandemic and economic downturn. Indeed, banks have never been stronger in terms of the capabilities they offer and the financial resources they can bring to bear on behalf of those they serve.⁴ And many customers, especially those who are not digital natives, as well as those who have been traditionally underserved, still value the certainty and convenience of a brick and mortar presence. Moreover, when it comes to business customers, technology can be crucial, but the most important factor in evaluating a banking partner remains the ability of the bank to support the business through its life cycle.⁵

Brick and Mortar Banks as Advice Centers for Digital Customers

Traditional banks are not going away, they are merely adapting to the new reality. The transition to an all-digital bank is underway and traditional banks are embracing the change to keep pace with peer banks and to provide customers with the banking experience that they demand. Resilient and reliable digital platforms are the key to the success of a digital bank along with the bank's customer-centric focus that concentrates on anticipating the customer's next financial need.⁶ However, traditional financial institutions are not likely to abandon what made them a customer's trusted bank to compete with the challenge presented by all-digital banks (Neobanks).⁷ National banking licenses, stable sources of liquidity, and customer trust are all highly sought after assets that digital banks do not yet possess. A fully digital bank with physical connections to local communities will have a significant advantage over pure Neobanks.

Maintaining connections to the communities which banks serve can be accomplished through moving in the direction of "Advice Centers" that will provide person-to-person advice in traditional locations, which

⁴ American Bankers Association, *supra* fn. 2.

⁵ "Real-Time Payments Gaining Traction Among Businesses" (Aug. 18, 2020), <https://www.businesswire.com/news/home/20200818005182/en/>.

⁶ John Rodgers and Rajeev Aggarwal, "Banks Must Rapidly Seize the New Digital Reality," Banking Exchange (June 1, 2020), <https://www.bankingexchange.com/mobile/item/8317-banks-must-rapidly-seize-the-new-digital-reality>.

⁷ Ben Gran, "Why do You Need a Brick-and-Mortar Bank?" Forbes (March 13, 2020), <https://www.forbes.com/advisor/banking/why-do-you-need-a-brick-and-mortar-bank/>; See also, "The Flywheel of Banking: Six Timeless Tenets of Extraordinary Banks", www.Bankdirector.com (May 14, 2020), "The temptation in banking right now is to focus on the technological changes underway. But ... success in the future isn't solely about mobilizing digital distribution channels, it's also about running a superb operation."

will complement digital products and services. Consumers and small businesses still value the convenience and personal interaction in the branch channel, and customers who desire person-to-person contact with their banking provider are more satisfied. This also applies to Millennials who are dealing with major financial decisions for the first time and value advice from proven, trustworthy partners.⁸ The key to the success of these advice centers will be talented professional staff who can serve as their client's go-to source for financial advice.

The Transition Picks Up Pace – Digital Banking Now Spans All Generations

As an example of the inevitability of the move to the Neobank model, prior to the pandemic, 76% of Baby Boomers banked online and 77% of Millennials preferred online banking.⁹ Currently, roughly one in three U.S. adults use a fintech product to meet their core financial needs, with more than 100 million U.S. consumers using digital financial services, including bank-offered services, to help them with things like payroll direct deposit, bill payments, investing, and savings.¹⁰ As the pandemic forced banks to close branches and limit in-person communication with customers, even more people embraced banking online. Real-time payments (RTPs), online mortgage applications, and Point of Sale (POS) products are quickly becoming a necessity instead of a novelty for the banking industry. RTP allows customers to make payments electronically and move funds instantaneously from one account to another. In a recent nationwide survey of 252 corporate decision-makers, results showed that only nine percent do not have plans to implement RTP, 81% expect RTP to dramatically transform the way business is done, 77% agree that digital currency will play a valuable role in the future, and 66% expect that they will stop making or accepting payments with cash or paper checks.¹¹ Removal of friction and enhancement of speed and security are the new imperatives.

⁸ David Kerstein and Nick Miller, "Transforming Branches into Advice Centers: The Long Road Ahead" (Sep. 16, 2019), <https://thefinancialbrand.com/88169/branch-advice-center-universal-teller/>

⁹ TJ McCue, "Is Your Mobile Banking App Secure – Three Tips To Stay Safe" (Aug. 30, 2019), <https://www.forbes.com/sites/tjmccue/2019/08/30/is-your-mobile-banking-app-secure-three-tips-to-stay-safe/#45aa7e4e16c2>.

¹⁰ Plaid Technologies, Written Statement for the Symposium on Consumer Access To Financial Records (Feb. 19, 2020), https://files.consumerfinance.gov/f/documents/cfpb_pitts-statement_symposium-consumer-access-financial-records.pdf.

¹¹ See fn 4, *supra*.

The Future of Customer-Centric Retail Banking

Customer-centric retail banking has been defined as “a way of banking based on trust and fairness that uses knowledge of customers to meet their needs and achieve sustainable, valuable, long-term relationships.”¹² Banks should see the future of banking as a customer-centric experience driven by application programming interfaces (APIs), allowing digital services to be tailored to the needs of the individual customer.¹³

As traditional brick and mortar banks rely less on physical branches and more on online and digital relationships, banks have an opportunity to reach more people, more efficiently, with increased customer interaction through digital communications. Increasingly, banks are offering products and services based on existing knowledge of the individual customer. This is compared to the current model where banks rely on customers to bring their individual needs to account managers who would then prescribe the optimal available products and services designed for large numbers of customers offered by their banking institutions. Banks will increasingly rely on data about individual customers to proactively offer products and services to meet the needs of those customers, and customers will increasingly expect their banks to do so. Interacting largely through user-friendly digital interfaces, banks will incentivize consumers to recognize the value added by the recommended banking services, providing the optimal experience for digitally native consumers looking for fast, efficient service they can access 24/7 through online and digital devices.

MEETING CUSTOMERS WHERE THEY ARE

As the “traditional” customer foot traffic into branches continues to fade, banks will have to go to their customers. The banks of the future will need to adapt their products and services to the expectations of their customers. For example, research has shown that today’s consumer – especially those under 30 – does not possess the same level of comfort with carrying credit card balances as their parents did. As a

¹² The Boston Consulting Group, “Customer-Centricity in Retail Banking” (2012), <https://mkt-bcg-com-public-images.s3.amazonaws.com/public-pdfs/legacy-documents/file98985.pdf>.

¹³ “Customers simply see no reason why they can’t enjoy the same functionality in managing their money as they enjoy ordering a product online or organizing a playlist on iTunes. Their belief – and rightfully so – is that they should be able to log on and ‘just have it work.’ Period. ... The imperative today is for a seamless customer experience across channels that taps the very best digital technologies and business models to offer customers exactly the products, solutions and advice they want – when, where and how they want them.” *Banking 2025 – Laying the Foundation for the Next Era in Financial Services*; Remarks of Bruce Van Saun, Chairman and CEO, Citizens Financial Group, to the Wharton Leadership Conference (June 6, 2018).

result, lines of credit can be more appealing than using credit cards, and products will need to target this customer base with the intent of meeting these new opinions on banking products.¹⁴

Point of Sale Products as a Customer-Centric Solution

Likewise, the POS “buy now, pay later” financing model capitalizes on new technology that enables compelling and innovative products that young people are looking for. This population prefers online self-service tools, expects transparency, and has very high expectations around digital offerings. Evidence of these expectations is the rapid advancement of POS financing products over the last several years.¹⁵

Many merchants have offered POS financing on large purchases for many years, such as furniture companies or electronics retailers, etc. While these programs are typically backed by select banks, they are presented by the merchant as the sole option to the consumer, aside from paying in full. POS financing has evolved such that banks and credit card companies are now offering POS financing on a much broader scale, not limited to select merchants. Additionally, by using a bank to finance a purchase, there are no new applications to complete or additional credit checks to be completed for each subsequent purchase.

Even in cases in which customers may not have thought in advance about how to finance their purchase, they have been proven to be savvy and receptive to attractive options and product simplicity. Examples of sought after products include products that offer attractive terms such as 0% APR financing, no fees, fixed payments, and fixed terms. Customers are looking for simple, clear, and understandable products and a superior customer experience which includes limited steps, speed of result, and ease of process. To achieve a superior cutting edge banking experience, innovative products and services will be essential. Providing attractive financing options for the customers will require flexibility and the ability to scale as needed.

¹⁴ Bloomberg, “Why Millennials are Ditching Credit Cards,” Fortune (February 27, 2018), <https://fortune.com/2018/02/27/why-millennials-are-ditching-credit-cards/>

¹⁵ “Point of Sale Financing – the New Frontier of Payments,” Charge After (October 28, 2018), <https://chargeafter.com/point-of-sale-financing-the-new-frontier-of-payments/>.

A Necessary Element – The Supply Chain

Program flexibility and scalability will result directly from a well-constructed and managed supply chain that covers the entire system of producing and delivering a product or service to the end user. For financial institutions, a good portion of the supply chain consists of leverageable in-house capability, such as underwriting and servicing, which is attractive to potential merchants. External portions of the supply chain must be built in advance, invested in, and closely managed and supervised. The customer experience in POS programs can suffer dramatically from just one weak link in the process flow.

A strong supply chain enables the starting point for any successful customer application experience. This will be especially important when competing to attract prime customers. Financial institutions that invest in an end-to-end POS program – leveraging existing operational, sales, systems and servicing infrastructure – will be well positioned to compete in this space. Managing partnerships with the third party technology providers who build, operate and maintain the POS platform will be equally important to the success of the supply chain. Absent a robust vendor oversight program built on well-vetted vendor relationships, firm Service Level Agreements (SLA) commitments and strict bank operational and performance oversight, the reliance on third parties' delivery partners can throw a kink in the supply chain – a kink that can be detrimental to that frictionless customer experience.

A strong supply chain also enables flexibility. Retail partners will expect bank programs to be tailored to their products and revenue drivers. This can mean a single-product program where the product and the company are synonymous; or a product-family program, such as an electronics retailer aiming to sell a new upgraded version of the product; or a subscription service to the customer on a regular cadence; or a product-agnostic program where the retailer is trying to give the customer financing flexibility at checkout, but with a longer-term appeal, like a fixed monthly payment on a line of credit product.¹⁶

Lastly, as banks better understand and collaborate with consumers, merchants, and Original Equipment Manufacturers (OEM), other consumer-oriented brands are likely to be added to the supply chain in new ways. This will raise new issues to consider regarding joint customers, customer experience, branding, and oversight over marketing and sales practices. Omni-channel capabilities that enable seamless shopping and delivery options remain a priority for consumers, and thus must be a priority for banks.

¹⁶ Accenture, "2019 Accenture Global Financial Services Consumer Study," https://www.accenture.com/_acnmedia/pdf-95/accenture-2019-global-financial-services-consumer-study.pdf.

With a rising number of fintech companies and banks providing POS financing, the importance of differentiation cannot be understated. If a financial institution wants to build and maintain a deeper relationship with the customer, it will be necessary to move beyond a business model built solely on originations, which offers only abbreviated, indirect access to the customer. The goal will be a holistic, well-managed financing solution.

Offering Superior Products and Services – Full Service Digital Banking (the Rise of the Neobank)

A bank's balance sheet and in-house financing flexibility, combined with a much larger suite of consumer lending products than any fintech can currently offer, will provide banks with a powerful competitive advantage. A customer's needs and preferences change and grow with the customer's financial lifecycle, and when informed by the insights of big data, the customer's bank will be best-positioned to meet those needs and preferences with tailored, timely offerings.

When competing against fintech companies, a bank's in-house financing capabilities will offer a major advantage. Creation of a full-service National Digital Bank to meet the needs of the digitally native customer will require personalized experience, a cutting edge platform to deliver compelling and innovative new products, and brand recognition based on a national presence and reputation. Notwithstanding the clear advantage that traditional banks transitioning to digital banks have over fintechs, the Office of the Comptroller of the Currency recently issued a national bank charter to Varo, a Neobank representing a low cost, digital banking organization aimed at providing digital services to consumers seeking solely digital interactions, causing many traditional banks to take notice.¹⁷

Neobanks are 100% digital and reach customers on mobile apps and personal computer platforms. They are technology-driven and may adopt machine learning and artificial intelligence technologies to assist in providing better services to their customers. Generally, apps offered by financial institutions to support digital banking should provide the basic services such as mobile check deposit, money transfers, bill pay, transaction history, and ATM locations. The apps should offer a clean and user-friendly interface and allow password storage.

¹⁷ John Cabell, "FinTechs vs. Traditional Banks: Who Has the Bigger Advantage," The Financial Newsletter <https://thefinancialbrand.com/84106/fintech-bank-credit-union-competition-advantages/>; see also, Alex Graham, CFA, FinTech and Banks: How Can the Banking Industry Respond to the Threat of Disruption? <https://www.toptal.com/finance/investment-banking-freelancer/fintech-and-banks>

Digital customers will expect to have access to fintech services that allow the customer to transfer funds to other individuals (P2P) using only email addresses and phone numbers, receive push notifications that allow a customer to track purchases, set travel notifications to avoid lack of access to funds while traveling, and have the ability to track and view all customer accounts at one time and on one platform.¹⁸

As the transition accelerates, digital banks will need to leverage their experience as leaders in POS financing to develop consumer centric solutions to address *unmet* needs in the marketplace. In particular, banks must focus on delivering next generation payments products that allow customers to pay for larger ticket items responsibly – without getting into burdensome, or even unsustainable, debt. Products could be designed to help customers better manage their existing debt and reinforce responsible spending habits by offering a regular, predictable repayment schedule to help budget spend.

Success in Digital Banking

Building and operating best in class digital product offerings will require balancing the need to create the frictionless experience that consumers expect with the legal and compliance requirements implicit in any regulated financial service activity. But there is a challenge – the crafting of strong, accurate and complete disclosures which are easily available and understandable.

For example, given the POS focus on simplicity, speed and convenience, the placement and manner in which required disclosures are delivered will be critical to the customer experience. Satisfying these requirements, while staying true to the POS hallmarks of speed and simplicity can be achieved with creative techniques such as hyperlinks to disclosures sent via email or SMS authentication codes delivered via email/SMS to validate user’s ability to access e-docs. This will require a change in how disclosures are used and viewed by both financial institutions and customers. The goal should be to move away from the standard disclosure buried on a webpage that customers don’t read. Consumers should be educated by the disclosure, which will be drafted in a way that conveys to the customer that it is for their protection and not just a speedbump in the customer experience.

The interdependencies with third party technology providers that are incumbent in many bank-delivered POS financing programs will necessitate an additional layer of consumer disclosures centered around the consumer’s interaction with the third party. Here, it will be incumbent on the bank to disclose to its

¹⁸ Accenture, “Beyond Digital: How Can Banks Meet Customer Demands?” (2017), https://www.accenture.com/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-Banking-Global-Distribution-Marketing-Consumer-Study.pdf?_en

customer what data the third party will see and what the third party can do with that data. These disclosures should be simple, prominently displayed, and easily accessible within the POS experience.

ADVANCING INSIGHTS, SPEED AND SECURITY – BIG DATA, CRYPTO AND CBDCs

Using Data to Drive Decisions

Responsible use of “Big Data” defined generally by the FTC as a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions, will also be required and undoubtedly, a focus of regulators.¹⁹ Using advanced analytics, Big Data is being used by financial institutions to inform investment decisions, assess credit or risk management activities, identify marketing opportunities with clients, help customers understand their own transactions, and improve products and services by targeting the needs of the customer. Predictive data-driven decisions improves the customer experience by providing personalized products, assists financial institutions with fraud prevention by analyzing suspicious spending patterns, and helps obtain new customers through target optimization.²⁰

Notwithstanding that promise, careful thought and consideration must be given to whether certain uses of Big Data may harm consumers that are in lower income brackets or underserved populations by biased datasets or flawed Artificial Intelligence algorithms. Algorithmic transparency is an important concept for banks to consider as data-driven algorithmic decision-making can lead to discriminatory outcomes despite the best intentions of the financial institution.²¹

Cryptocurrency/Banking Crypto Services

The payment services industry is going through a revolution, brought upon by technological changes led, in large part, by blockchain and cryptocurrency. Instead of reliance on credit cards or paper checks, the

¹⁹ Federal Trade Commission, “Big Data: A Tool for Inclusion or Exclusion” (January 2016), <https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf>

²⁰ Pankaj Upadhyaya, “Advanced Analytics in Banking World” (October 1, 2019), <https://www.finextra.com/blogposting/17951/advanced-analytics-in-banking-world>

²¹ Bruno Lepri et al. “Fair, Transparent, and Accountable Algorithmic Decision-Making Processes.” *Philosophy & Technology* 31, 4 (December 2018): 611–627 © 2017 Springer Science+Business Media https://dspace.mit.edu/bitstream/handle/1721.1/122933/13347_2017_279_ReferencePDF.pdf?sequence=2

future of e-commerce payments will be through mobile devices, and international payments will be increasingly done using cryptocurrency. In fact, by 2021, an estimated 72 percent of all e-commerce payments are expected to be effected through mobile devices. Anticipating the need for faster, more efficient payment systems, merchants and consumers are increasingly turning to cryptocurrency.²²

As consumers become more comfortable with cryptocurrency, and technologies relying on cryptocurrency and blockchain continue to improve, banks will increasingly offer consumer cryptocurrency services, while relying on cryptocurrency technology to offer improved services to consumers. Products and policy are evolving rapidly to meet those needs.

In particular, banks are relying on cryptocurrency for faster, more efficient cross-border payment services. Some banks are creating their own blockchain-based systems, including digital currencies, to enable business to business payments between their customers.²³ Often, these bank products are proprietary products pegged to national currencies, or “stablecoins.” This makes the coins less volatile in price than traditional virtual currencies, allowing them to be used as a digital form of cash. In other cases, banks rely on convertible cryptocurrencies for fast, efficient, foreign exchange services. In parallel with the development of cryptocurrency payment systems, banks have been upgrading the speed and times of availability of conventional bank-account-based payment systems. The global standard for a fast payment system is near real-time availability of the funds by payees on a 24/7 basis.²⁴

Central Bank Digital Currencies

The use of cryptocurrency in banking may be accelerated by the development of central bank digital currencies (CBDCs). To take a recent example, the U.S. Federal Reserve Board is working with researchers at the Massachusetts Institute of Technology to test and build a possible U.S.-based CBDC.²⁵

²² Ilker Koksak, “The Rise of Crypto as Payment Currency,” *Forbes* August 23, 2019), <https://www.forbes.com/sites/ilkerkoksak/2019/08/23/the-rise-of-crypto-as-payment-currency/#38e9bcfa26e9>

²³ [https://www.americanexpress.com/us/foreign-exchange/articles/us-banks-support-cryptocurrency-payments/.](https://www.americanexpress.com/us/foreign-exchange/articles/us-banks-support-cryptocurrency-payments/)

²⁴ Darrell Duffie, “Digital Currencies and Fast Payment Systems: Disruption is Coming” (Preliminary Draft), Stanford University, For Presentation to the Asian Monetary Policy Forum (May 2019), <https://www.darrellduffie.com/uploads/policy/DuffieDigitalPaymentsMay2019.pdf>. This need has not been lost on global regulators. For example, on July 13, 2020, the Bank for International Settlements (“BIS”), Committee on Payment and Market Infrastructures (“CPMI”), released its Step Two report on enhancing cross border payments which, BIS believes, will form the building blocks for a global roadmap for international payments.

²⁵ Lael Brainard, “An Update on Digital Currencies,” Remarks by Lael Brainard, Member, Board of Governors of the Federal Reserve System” (August 2020), <https://www.federalreserve.gov/newsevents/speech/brainard20200813a.htm>.

A general purpose CBDC is designed for payments efficiency, offers potentially significant technical improvements over conventional bank deposits, and would likely be simpler to transfer than bank deposits. The learning in this space is advancing rapidly. For example, the “Digital Dollar Project” (sponsored by the Digital Dollar Foundation and Accenture) seeks to encourage the next major innovation in U.S. currency: a tokenized digital dollar that has the same legal status as physical bank notes.²⁶ The fundamental benefit of this concept is that there is no better, riskless settlement medium than U.S. central bank money.

The development of fast and efficient bank-account-based or cryptocurrency payment systems, including CBDCs could place pressure on existing banking franchises to upgrade their technology to meet the needs of their customers. New payment technologies will force banks to compete more aggressively for deposits. Fintech entrant banks could trigger changes in depositor behavior, such as the use of APIs to monitor and transfer funds.

Additional blockchain-based banking services likely will include custody and ATM services. Until recently, national banks have been reluctant to provide banking services for cryptocurrencies, but recent guidance from the OCC is likely to soften that reluctance.²⁷ As discussed more fully below, from a policy perspective the OCC is becoming increasingly proactive in permitting digital banking, which should lead to larger banking institutions being more willing to invest in new technologies to better serve their customers.

Of course, digital banking carries risks as well as rewards. Mobile banking carries security risks that are different than those resulting from traditional paper-based banking through brick and mortar branches. Passwords can be lost or stolen, and accounts can be hacked, though advances in protection are being made (*See infra* pp. 18-22). Similarly, cryptographic keys can be misplaced, causing the currencies to be lost forever, unless the key is later located. Also, as convenient as Bitcoin ATMs may be for consumers, they also provide additional opportunities for money laundering and facilitate anonymous payments by individuals seeking to avoid detection by tax or criminal authorities, frustrating a bank’s ability to perform the required customer identification programs and sanctions due diligence. Realizing the increasing concerns over money laundering, industry groups such as the Bank Policy Institute have

²⁶ Digital Dollar Project, “Exploring a US CBDC” (May 2020), https://static1.squarespace.com/static/5e16627eb901b656f2c174ca/t/5ecfc542da96fb2d2d5b5f15/1590674759958/Digital-Dollar-Project-Whitepaper_vF.pdf

²⁷ Office of the Comptroller of the Currency, Interpretive Letter 1170 (July 22, 2020), <https://www.occ.gov/topics/charters-and-licensing/interpretations-and-actions/2020/int1170.pdf>.

vigorously supported new anti-money laundering legislation aimed to improve the effectiveness of financial institution anti-money laundering efforts.²⁸

Social Equality – Serving the Underbanked Through Technology

The progression from reliance on primarily brick and mortar branches to digital banking also may offer the opportunity for banks to provide products and services to a greater number of consumers, including those living in geographic areas that traditionally have been underserved. Already, the presence of ATMs in retail stores enables consumers to access cash at more locations, including those without traditional bank branches. Along these lines, it has been recently reported that at least one major bank has been in discussions with the U.S. Postal Service about placing ATMs in post office branches to better serve some historically underserved communities.²⁹

The transformation to digital banking could accelerate this process, as consumers may soon be able to access a whole array of banking services, from establishing and transacting in checking accounts to obtaining mortgage loans, all through applications on their mobile phones. Access to banking services through mobile devices could help level the playing field in lower income communities. Moreover, the combination of digital banking with more finely tailored banking products accompanied by innovative designs could make accessible for the first time access to credit, deposit and savings, lending products, and payment and safekeeping services previously unavailable in underserved locations. The presence of Bitcoin ATMs may allow local residents to deposit, store and retrieve currency safely, both locally, and globally wherever such ATMs may be located. Cryptocurrencies may also allow for fast, efficient and inexpensive payments, regardless of an individual's geographic location.

One additional area in which digital banking may help the traditionally underserved is in access to Community Reinvestment Act (CRA) qualifying banking services. In May 2020, the OCC adopted a rule intended to increase bank CRA lending, investment and services in low-moderate income communities where there is a significant need for credit, more responsible lending, and greater access to banking service.³⁰ The final rulemaking included examples for digital CRA-qualifying activities, including : (1)

²⁸ Angelena Bradfield, "Congress Should Pass Anti-Money Laundering Reform Legislation Now," Bank Policy Institute (July 23, 2020), <https://bpi.com/congress-should-pass-anti-money-laundering-reform-legislation-now/>

²⁹ Hugh Son, "JPMorgan Chase Held Talks with U.S. Postal Service About Installing ATMs in Post Offices," (August 19, 2020), <https://www.cnbc.com/2020/08/19/jpmorgan-chase-held-talks-with-us-postal-service-about-installing-atms-in-post-offices.html>.

³⁰ Department of the Treasury, Office of the Comptroller of the Currency, CC-2018-0008 (May 20, 2020), <https://www.occ.gov/news-issuances/federal-register/2020/nr-occ-2020-63a.pdf>

a grant to a nonprofit community program which assists low-moderate income individuals to find and enroll in a free or low cost home broadband internet services for which they are eligible; (2) a grant in support of a nonprofit program which refurbishes used computers in order to provide them to low-moderate income individuals at no cost or a very low cost; and (3) financial support of a nonprofit community program that provides digital literacy training to residents of a low-moderate income neighborhood, in order to increase their ability to use online banking services. The OCC thereby supported bank digital services as a central part of CRA compliance programs.³¹ Along similar lines, there also have been calls for the Federal Reserve Board to expand its policy mandates to include addressing the phenomenon of income inequality.³²

As an example, on August 5, 2020, Congresswoman Maxine Waters, Senator Elizabeth Warren, and Senator Kristen Gillibrand introduced legislation to require the Federal Reserve to use its existing authorities to attempt to close racial employment and wage gaps and report on how the gaps change over time.³³ Moreover, the Federal Reserve Bank of New York has begun a new and extensive research series to better understand what contributes to economic inequality in the New York region and across the nation.³⁴

FINTECH AND NATIONAL BANK CHARTERS – POLICY AND REGULATORY CONSIDERATIONS

Fintech companies are increasingly providing payment services relying, for the moment, on state money transmitter licenses. Recent developments in technology have permitted companies such as PayPal and Stripe to take increasing amounts of market share in payments from federally regulated banks. As discussed below, this has led the OCC to propose Special Purpose National Bank Charters to companies engaging in certain core banking activities, other than deposit taking.

³¹ Bill Callahan, “New Rules from OCC: Banks can now get CRA Credit for Funding Digital Inclusion, (May 20, 2020), <https://www.digitalinclusion.org/blog/2020/05/20/new-rules-from-occ-banks-can-now-get-cra-credit-for-funding-digital-inclusion/>

³² Somin Park, “Economic Inequality Matters for Federal Reserve Monetary Policymaking” (September 17, 2019), <https://equitablegrowth.org/economic-inequality-matters-for-federal-reserve-monetary-policymaking/>

³³ U.S. House Committees on Financial Services, “Waters, Warren and Gillibrand Introduce Legislation Requiring the Fed to Close Racial Employment and Wage Gaps” (August 5, 2020), <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=406829>

³⁴ Federal Reserve Bank of New York, “Heterogeneity: A Multi-Part Research Series”, <https://www.newyorkfed.org/research/heterogeneity-series>; also known as the “Economic Inequality and Equitable Growth” project (nyfed.org/inequality).

Moreover, until recently, national banks have been reluctant to adopt cryptocurrency and blockchain technology, particularly in consumer services, due to regulatory uncertainty. This has resulted in a small number of state chartered banks and myriad fintech companies offering traditional banking services using this technology. For example, Silvergate Bank, a California-chartered bank and member of the Federal Reserve System, has offered traditional banking services to fintech companies, including offering cryptocurrency services for a number of years, and currently offers cryptocurrency backed loans.³⁵

State-chartered trust companies, such as BitGo and Gemini, have also been offering custody services for cryptocurrency. Other fintech companies, such as BitPay and Coinbase offer cryptocurrency payment services, regulated by states as money transmitters. The emergence of so many fintechs into the payment services arena has created the possibility of significant advancement in digital banking by pushing the envelope of what is possible. However, patchwork regulatory frameworks surrounding fintechs in this space coupled with the sheer amount of companies trying to obtain customers could create “white noise” for consumers and send them back to their financial institution as a known and secure environment. Traditional banks making the transition to digital banking could use the current landscape to their advantage.

Regulatory Developments in Digital Banking

Under the leadership of its new Acting Comptroller, Brian Brooks, the OCC has taken the lead in driving increased awareness of the technological developments in banking, and recently has become proactive in providing guidance on national banks offering digital banking services. For example, in June 2020, the OCC issued an advanced notice of proposed rulemaking, inviting public comment on national bank and federal savings association digital activities. The notice stated that national banks and federal savings associations must have a regulatory and supervisory framework that enables banks to adapt to rapidly changing trends while continuing to operate in a safe and sound manner.³⁶ In addition to the advanced notice of proposed rulemaking, the OCC has also taken steps recently to enable national banks to offer traditional banking services through digital means.

The OCC recently issued an interpretive letter, clarifying that national banks and federal savings associations may act as custodians for cryptocurrency. Services may range from holding copies of the

³⁵ Lubomir Tassev, “Big Banks Won’t Touch Crypto Clients – But These Smaller Banks Will” (September 13, 2019), <https://news.bitcoin.com/big-banks-wont-touch-crypto-clients-but-these-smaller-banks-will/>.

³⁶ Office of the Comptroller of the Currency, OCC Bulletin 2020-59 (June 4, 2020), <https://www.occ.treas.gov/news-issuances/bulletins/2020/bulletin-2020-59.html>.

cryptographic keys enabling transfer of the customer’s cryptocurrency to related services such as those currently provided by cryptocurrency exchanges – facilitating the customer’s cryptocurrency and fiat currency exchange transactions, transaction settlement, trade execution, recording keeping, valuation, tax services, reporting and other appropriate services. Banks holding custody of crypto assets must address the risks associated with the account and customer to include compliance with anti-money laundering rules and may include developing additional controls such as specialized audit procedures to ensure the bank’s controls are effective for digital custody activities.³⁷

OCC Policy Statement on Fintech National Bank Charters

In 2018, the OCC issued a Policy Statement that it has the authority to grant national bank charters to fintech companies engaging in solely one or more core banking activities, such as receiving deposits, making payments or sending money. The statement provided a framework of uniform standards and robust supervision with the intention of leveling the playing field between regulated institutions and fintech companies providing such services, particularly to digital assets.³⁸

Current Fintech Regulatory Landscape

States currently regulate the traditional banking activities provided by many of the fintech companies, including money transmission and custody of cryptocurrency assets. Perhaps because the OCC charter may arguably preempt the ability of the states to regulate this activity, the New York Department of Financial Services (NYDFS) challenged in court the ability of the OCC to issue such charters.³⁹

In its Complaint, the NYDFS asserts three counts seeking declaratory and injunctive relief. Count I asks the Court to find that the Fintech Charter Decision was unlawful because it exceeded the OCC’s authority under the National Bank Act. Count II asks the Court to find 12 C.F.R. § 5.20(e)(1) null and void because the OCC exceeded its statutory authority in promulgating the Regulation (OCC’s authority to issue special bank national charters). Count III asks the Court to find that the Fintech Charter Decision violates the Tenth Amendment of the Constitution because it creates a conflict with state law. The Court

³⁷ See fn 26, *supra*.

³⁸ Office of the Comptroller of the Currency, Policy Statement on Financial Technology Companies’ Eligibility to Apply for National Bank Charters (July 31, 2018), <https://www.occ.gov/news-issuances/news-releases/2018/another-occ-policy-statement-fintech.pdf>.

³⁹ *Maria T. Vullo v. Office of the Comptroller of the Currency and Joseph M. Otting*, 18-cv-08377 (SDNY May 2, 2019), https://www.consumerfinance.com/wp-content/uploads/sites/14/2019/05/2019.05.02-Division_NYDFS-v.-OCC_fintech-charter.pdf.

ordered that the OCC's motion to dismiss the complaint was denied as to Counts I and II, but granted as to Count III.

Despite the current litigation, on June 25, 2020, Acting Comptroller Brooks announced that the OCC intends to introduce a new Payments Charter "Version 1.0" this fall, which would serve as a federal alternative to obtaining state money transmitter licenses. After approximately eighteen months, the OCC hopes to introduce "Version 2.0," which would allow specially-chartered organizations to obtain access to the Federal Reserve's payment system. Such a charter would arguably preempt the need for state licenses, permitting the recipient to operate nationally in all fifty states with a single federal primary regulator, the OCC, rather than fifty individual state regulators.⁴⁰

This summer, as noted on p. 7, the OCC advanced its "pro-digital" position by issuing a national bank charter to Varo, a digital bank, operating through mobile apps. Acting Comptroller Brooks stated that, "Varo Bank's opening on August 1, 2020, represents the evolution of banking and a new generation of banks that are born from innovation and built on technology intended to empower consumers and business."⁴¹

Special Purpose Charters and State Regulators

As stated above, fintech companies offering core banking services are currently supervised by the state regulators. The OCC's limited-purpose charter was theoretically designed to help fintechs that do not seek to take deposits but that want to operate under a single national regulator. Press reports indicate that Google, PayPal and dozens of other technology and fintech companies have visited with officials at the OCC during the past year to explore whether to obtain the agency's new special-purpose national bank charter. The reports are that both Google and PayPal, as well as several others, have since backed off over fears that they could harm existing relationships with state regulators and concerns about whether the OCC will prevail in a legal challenge to its authority to create the fintech charter (discussed above).⁴²

⁴⁰ Amanda Averch, "OCC's Brooks Plans to Unveil "Payments Charter 1.0 by This Fall," The Colorado Bankers Association (June 25, 2020), <https://www.coloradobankers.org/news/514451/OCCs-Brooks-Plans-to-Unveil-Payments-Charter-1.0-This-Fall.htm>

⁴¹ OCC News Release 2020-99 (July 31, 2020), "Acting Comptroller of the Currency Presents Varo Bank, N.A. It's Charter," <https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-99.html>

⁴² Rachel Witkowski, "Google and PayPal Explored OCC's FinTech Charter, Then Walked Away, American Banker" (June 16, 2020), <https://www.americanbanker.com/news/google-and-paypal-explored-occs-fintech-charter-then-walked-away>.

For their part, the states have not been idle in responding to that challenge. Understanding the difficulty of being regulated by fifty different regulators, the states have been working to streamline multistate regulations for nonbanks largely through the Conference of State Bank Supervisors, which launched a major effort in 2017 to get states to harmonize the licensing process by next year, called “Vision 2020.” Nearly half the states in the country have now agreed to form a joint licensing process. It also is worth noting that trade groups, such as the Money Services Business Association, are also working to drive consistency and uniformity, as well as development and innovation in the payments space. However, despite these efforts, it remains cumbersome and expensive to obtain and operate under the many state licenses currently required to provide core banking services under state licensing regimes. Accordingly, the tension between the benefits of nationwide uniformity and the well-known matrix of state regulation is not likely to disappear anytime soon.

Relationship of High-Tech Companies Providing Operational Services to Banks

In remarks at a recent Brookings Institute event, Acting Comptroller Brooks discussed his idea that the three main components of banking – deposit taking, loan making, and payment services – could be “unbundled,” justifying national bank charters for fintechs that just provide payment services. However, he stressed that the challenge isn’t unbundling the components, but rather it is keeping them unbundled. He stated that, while it may be possible to unbundle payments services from deposit-taking and loan-making, those different functions will inevitably recombine.⁴³

A recent article published by the Bank Policy Institute, discussed those arguments and replied that although fintech companies currently enjoy many of the same benefits as bankers of centuries ago, such as interest free deposits from customers and no capital and deposit insurance requirements, Brooks’ proposal won’t lead to greater stability in the financial system. If the OCC’s proposal is to offer special bank charters that are less stringent than those required of full service national banks, this would lead to unnecessary risk taking by those fintech companies, with greater short-term profits, and greater risks to their customers and the financial system. For example, if the fintech companies accept deposits, this would put the customer deposits at risk, potentially leading to a run on the bank scenario.⁴⁴ Moreover, the article continued, the OCC must make sure the special charter banks don’t become the weakest link in the

⁴³ The Brookings Institution, “Fixing America’s Payment System: The Role of Banks and Fintech; a Conversation with Acting Comptroller of the Currency Brian Brooks (July 29, 2020), https://www.brookings.edu/wp-content/uploads/2020/08/es_20200729_payment_systems_transcript.pdf.

⁴⁴ Bill Nelson, *Executive Vice President and Chief Economist*, Bank Policy Institute, “Medieval Money Changers, FinTechs, and the Risk of Unbundling, Bank Policy Institute” (August 12, 2020), <https://bpi.com/medieval-money-changers-fintechs-and-the-risk-of-unbundling/>.

intermediation chain of the financial system. They should be subject to the same prudential regulatory and supervisory requirements as all other banks, their holding companies must be subject to Federal Reserve supervision and they must not combine banking and commerce.⁴⁵

Under the OCC proposed model, however, fintech companies may offer vendor services such as payments to banks, relying on bank national licenses, while offering technological efficiencies.⁴⁶ This approach should allow banks to integrate technological improvements more quickly, while helping to satisfy regulatory concerns about the impact of fintech on the financial system.

PROTECTION OF CUSTOMER DATA IN A DIGITAL WORLD

Customer-Centric Platforms Driven by APIs

Digitally native customers expect their banks to offer digital banking based on a Banking as a Platform (BaaP) model. Specifically, customers are looking for a flat structure that facilitates the exchange of financial information between businesses, customers, and other third parties. The platform structure is based on connection and requires an advanced infrastructure built around APIs. To a customer, a frictionless mobile banking experience is a positive customer experience. Smartphones, broadband internet, the 24/7 availability of commerce and data, and social networks have made us organize ourselves very differently than in the past and the Millennial generation now have completely different expectations than their parents or grandparents of communication and commerce.⁴⁷

Within the BaaP model, customers are increasingly seeking new ways to manage their finances or move money in a seamless way leveraging different financial tools to meet their specific needs. Financial Data Aggregators (FDAs) play an important role in this by accessing customer data to provide a consolidated view of customer financials, transaction activity, or to move money from one account to another.

⁴⁵ See fn 43, *supra*.

⁴⁶ Igor Tomych, "Top Six Banking as a Service Providers to Lead the Next Banking Revolution," Finextra (January 28, 2020), <https://www.finextra.com/blogposting/18379/top-six-banking-as-a-service-providers-to-lead-the-next-banking-revolution>.

⁴⁷ David Brear and Pascal Bouvier, "Exploring Banking as a Platform (BaaP) Model" (2020), <https://thefinancialbrand.com/57619/banking-as-a-platform-baap-structure/>.

Understanding FDAs

Customers must understand what it means to provide a third-party FDA access to their financial accounts. A customer new to using FDAs may not be aware of the potential risks that accompany opening their complete financial history to a third party. To ensure that customers are providing informed consent to the FDAs, they must be made aware that their data is subject to the FDA's privacy policy and terms of use and that these terms could differ significantly from those of their trusted financial institution. Customers must acknowledge that the FDA's privacy policy and terms of use will dictate how the customer data is used, stored, analyzed, and potentially sold. Recent class action litigation against FDAs provides a stark reminder of the issues FDAs face and of the expectations of consumers.⁴⁸

It is worth noting that there may be a silver lining to recently filed class actions against FDAs and that is that fintechs are being put on notice that customers expect that their privacy will be protected and their data will remain secure. As discussed below, FDAs have begun to provide consumers with more transparency and control of the information that the consumer has shared with the FDA and has provided the consumer with the ability to "disconnect" from the FDA when desired.

Screen Scraping and APIs

Currently FDAs obtain customer data in two ways. The first is by using customer provisioned credentials to screen scrape information from customer bank accounts. The second method is through a more secure Application Programming Interface (API) platform.

Screen scraping allows access to a wide range of data as the customer deals directly with the FDA and provides the aggregation service with account login credentials to the customer's accounts. Once the login credentials are provided, the customer must either change their username and password or formally request the FDA to stop accessing their accounts. Through the use of screen scraping, FDAs may also be

⁴⁸ *Cottle et al. v. Plaid, Inc.*, 3:20-cv-03056 (D. N. Cal, May 4, 2020). Plaintiffs contend that when a consumer enters her bank login credentials on one of the apps that partners with Plaid, she does so believing that the credentials would be used for the ostensible limited purpose of verifying and linking her financial account to the chosen app. However, plaintiffs allege that users are never informed that third-party Plaid will receive and retain access to their bank account credentials, and use them to an extent beyond what is understood and authorized by the consumer.
<https://www.bloomberglaw.com/public/desktop/document/CottleetalvPlaidIncDocketNo320cv03056NDCalMay042020CourtDocket?1597159618>. See also *Wesch v. Yodlee, Inc., et al*, 3:20-cv-05991 (D.N. Cal, August 25, 2020) (plaintiffs allege Yodlee collects and sells customer information without consent and fails to maintain adequate security measures to protect customer data),
https://www.pacermonitor.com/public/case/35982309/Wesch_v_Yodlee,_Inc_et_al

able to store large amounts of customer data which they can use to analyze and market products to customers or sell said data to additional parties.

It is important for customers to understand that when their data is in the custody of an FDA, the protection of that data is reliant upon that FDA's data security policies. Also, banks must be aware that as part of their obligations under the Gramm-Leach-Bliley Act (GLBA), banks are responsible for conducting due diligence of data security practices of third parties with whom they share personal information. Screen scraping may also make security more difficult for financial institutions and hamper fraud detection efforts. Having internal procedures to limit the effects of screen scraping such as an enterprise API platform where aggregators are required to register to use a bank's API is one way of mitigating these risks.⁴⁹

APIs support new product development, customer enabled preferences, protection of customer passwords, and provide a significant reduction of the load on the bank's systems by removing the strain caused by screen scraping. APIs are designed to give customers more control through the ability to manage and direct what information they share with an FDA and to provide a secure data transfer environment using one-time passwords to access customer data. APIs are considered to be faster, more stable, secure, and accurate than screen scraping and provide financial institutions the ability to provide customer data in a predictable manner. This allows FDAs and other fintechs to know in advance the data they are authorized to collect and the rules for collecting the data. The customer is confident that the data being collected by the FDA is accurate, current, and complete.

Educating Consumers about FDAs

As noted above, to remain competitive, banks must strive to create a secure, frictionless experience for customers choosing to use FDAs. This will allow the financial institution to keep pace with customer behavior, maximize the customer's control over their data, and minimize risk to the bank. Partnerships with FDAs provide desirable services to consumers. To benefit from the services provided by FDAs, consumers must feel confident in disclosing personal and financial information to the FDAs. For years, banks have cautioned their customers not to share their login credentials. With the introduction of FDAs, however, customers are now sharing login credentials with FDAs and other third parties and need to understand what this sharing entails. Educating consumers ensures that they realize the scope of the

⁴⁹ Office of the Comptroller of the Currency, OCC Bulletin 2005-35 (Oct. 12, 2005), https://bsaaml.ffiec.gov/docs/resources/new_5_2007/OCC/BL_2005_35.pdf

access to personal information that they are providing to a third party and disclosures inform the consumer when that access is taking place.

Informed customer consent is the key to using FDAs. The lack of disclosures and notifications could hamper the customer's ability to make informed decisions about what data they share with FDAs and potentially expose banks to liability. While FDAs provide unmatched convenience and connectivity, customers may not be aware that when using an FDA, they are entering into a relationship with a third-party service provider where their bank may no longer be able to secure their financial information. Creating a communication plan that updates customers on their linked accounts whenever there is FDA activity is an additional way to educate and protect customers.

As customers become better educated and aware of the issues involved in using an FDA, they will seek a safer option by choosing a bank that can offer a secure method of data transfer as well as customer control over data sharing and usage. Banks that continue to rely solely on the screen scraping technique will almost certainly lag the market

Protecting Customers with Authentication

One way for banks to offer security to customers is through authentication methods that go beyond password-based authentications. Passwords present issues for customers such as: (1) customers often forget their usernames and passwords; (2) resetting forgotten usernames and passwords is either insecure if done over email or telephone or cumbersome if done in person; and (3) usernames and passwords can be guessed because customers often reuse them. Two-factor or multi-factor authentication is often thought of as a good alternative to passwords but can be prohibitive for customers who only have one device.

One approach would be to have a customer register a trusted device with the bank. The trusted device would create a cryptographic key pair, a public key (PK) that it will send to the bank, and a secret key (SK) that it would store on the device in a way that would be very difficult for a hacker to retrieve. Each transaction between the customer and the bank will be authenticated using the customer's SK. A digital signature scheme is an attractive tool to use here: any information or document that the customer wants to send to the bank from its registered trusted device (for example, a digital check) can be authenticated by using a digital signature scheme. To sign a document, the trusted device will need the SK, and to verify it, the bank will need the PK.

Consumer devices, such as smartphones and laptops, are increasingly able to securely authenticate the end user. One such authentication method is the use of Biometrics. Many banks are currently using fingerprint scanning, voiceprinting, and facial recognition as authentication tools to provide additional security for its customers in addition to other security features -- such as secure enclaves -- that make consumer devices hard to break into. Taking advantage of these security features is attractive for banking because they allow the bank to authenticate the customer without invading his or her privacy. Moreover, an application running on a consumer device can serve as a platform that provides all banking services to the consumer in one spot, without ever requiring that the consumer provide his or her valuable private banking data to any external entity.

Expertise in Continual Evolution – The Strength of Cross-Functional Teams

Another way a financial institution could look to protect customers is to create a cross functional team to address issues surrounding the use of FDAs at an enterprise level and to work with third party aggregators on rules related to customer data. The team could work with the financial industry to identify, define, and adopt a common standard for secure consumer and business access to personal information and financial records. The team could also focus on the education of customers regarding issues related to the use of FDAs using clear and concise disclosures, educational sites, and interstitial pages that notify customers before they leave their bank's site and before they provide personal information to a third-party FDA.

To further limit the risk to banks from engagements with FDAs, banks should also look to create a customer facing online educational page detailing what a customer should know about third-party financial apps and how to safeguard their accounts. The page should be designed to inform customers of what happens when they grant an FDA access to their financial information, how FDAs use customer data, how the customers can protect themselves, and what actions the bank is taking to protect the customer.

Consumption and Provider Models

When creating a strategy around FDA engagement, banks may want to consider two different models. The Consumption Model involves cases where the customer is applying for a product or service and the bank uses an FDA to enhance the product or service for a better customer experience (e.g., linking accounts to assist in filing a loan application or for income verification). The second model is the Provider Model wherein the consumer deals directly with the FDA and grants the FDA access to consumer's accounts. In the Provider Model, the bank's strategy will require a platform to share data

securely with vetted FDAs and move from the method of screen scraping to the use of APIs. APIs will provide consumers with control of the data they share with FDAs and will lessen the load on a bank's infrastructure related to FDA's current practice of screen scraping.

Risks Associated with the Consumption and Provider Model

Banks still have a responsibility to manage FDA relationships in a safe and sound manner wherein the level of due diligence and ongoing monitoring is commensurate with the risk to the bank. In the Provider Model, banks may not receive a direct service or benefit from the FDA and the risk level would be lower than in the Consumption Model wherein a bank has a third-party relationship with the FDA. With the introduction of APIs to replace screen scraping, both the Consumption Model and the Production Model have the ability to create a business arrangement with an FDA and therefore, a third-party relationship pursuant to OCC Bulletin 2013-29.⁵⁰ Banks should also be aware that as part of their obligations under the Gramm-Leach-Bliley Act (GLBA), they are responsible for safeguarding customer information and exercising appropriate due diligence over service providers with whom they share personal information to ensure that those service providers also have safeguards in place to protect said information.⁵¹

Regulatory Considerations

As described above, customers are becoming increasingly reliant on fintech apps to track spending, set budgets, apply for loans, make payments, and manage investments. Section 1033 of the Dodd-Frank Act requires financial institutions to make consumers' financial data available in an easily useable format and grants authority to the CFPB to create rules to govern the interactions.⁵² In 2017, the CFPB issued non-binding principles for "Consumer Authorized Financial Data Sharing and Aggregation". The 2017 CFPB Consumer Protection Principles reiterated the importance of consumer interest related to the consumer-authorized use of financial data to promote a "robust, safe, and workable data aggregation market that

⁵⁰ OCC Bulletin 2020-10 (Mar. 5, 2020) "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," <https://www.occ.gov/news-issuances/bulletins/2020/bulletin-2020-10.html>.

⁵¹ 12 C.F.R. 30, Appendix B "Interagency Guidelines Establishing Information Security Standards," https://ithandbook.ffiec.gov/media/resources/3530/occ-12cfr30_ap_b_inter_guid_estab_stand_safe_info.pdf

⁵² American Bar (Dec. 5, 2019) "The Future of Interconnected Banking is Now, and It's Brought to You by APIs," https://www.americanbar.org/groups/business_law/publications/committee_newsletters/consumer/2019/201911/banking/

gives consumers protection, usefulness, and value”.⁵³ The non-binding CFPB principles emphasized consumer control over their data as well as the need for privacy and data security protections.

Other legal considerations applicable to data aggregation include the avoidance of deceptive practices under the Federal Trade Commission Act, data sharing restrictions under the GLBA, and state laws such as the California Consumer Protection Act. Increased regulatory oversight over the use of data aggregation combined with the ongoing class actions against data aggregation companies will require more guidance from financial regulators to navigate these issues and will be critical to the success of digital banking.

CONCLUSION

As the digital transition advances, superior customer experiences and relationships will be at the center of how any successful bank operates. Indeed, consultants lately have begun to say that leading companies now understand themselves to be in the customer experience business. Evolving into that business will necessarily require customer-centric policies.

As we noted at the outset, we believe the transition to digital banking is inevitable, and that ultimately it will lead to the Banking as a Platform model. This suggests a natural sequence. Banking as a Platform requires connectivity. Connectivity is driven by customer demand and supported by the use of APIs. FDAs play a huge role in fostering the connections to which customers are quickly becoming accustomed. Innovative products, data security, and anticipating the needs of customers will go a long way for banks making the transition from traditional banking to a digital-first environment. But, along with the significant benefits of digital banking comes new and increased risk. Financial institutions will need to ensure that they have policies and procedures in place to address the legal, regulatory, and reputational risk associated with digital banking. On balance, however, we believe that all these pragmatic and policy considerations are flowing in the same direction – toward digital banking that is safe, secure, real-time, and rich in products and services. In short, a bank that meets customers where they are.

⁵³ “Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation” (Oct. 18, 2017) available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf