Center of Regulatory Intelligence

August 31, 2017

Regulatory Intelligence Briefing:
Offering a Special Purpose National Bank Charter to FinTech Companies

CAPCO

Table of Contents

A. Editorial Note from the Managing Director, Center of Regulatory Intelligence

In March of this year, the Office of the Comptroller of the Currency (OCC) announced a new special purpose national bank (SPNB) charter the agency will be offering to financial technology (FinTech) companies. The announcement followed more than two years of research including multiple opportunities for public comment. Even so, the proposed charter met harsh criticism from a variety of firms, government agencies and professionals in the field. This included two different lawsuit filings against the OCC regarding the proposed FinTech charter.

In this month's Regulatory Intelligence Briefing (RIB), we take a look at the FinTech charter's history and proposed requirements to better understand the implications of the proposal. We outline many of the contributing events in the long history of OCC research and legislative action to better understand where the charter proposal stands now. We also look at what the chartering and supervision process will look like for a FinTech firm that wants to apply for the SPNB charter. Finally, we consider the impact this OCC offering might have on both FinTech firms and the financial industry as a whole.

In addition to the primary article on the OCC's SPNB charter for FinTech companies, we explore recent trends in Bank Secrecy Act/Anti-money laundering (BSA/AML) regulations and enforcement actions. We will outline developments regarding BSA/AML in real estate, virtual currency and the gaming industry.

We also provide a review of two recent congressional hearings on BSA/AML. The first hearing covered BSA/AML regulatory compliance and the second explored how to manage terrorism financing risk in money transfers and remittances. In the hearings, witnesses discussed major issues in the BSA/AML field and provided suggestions on how to mitigate problems for financial institutions while ensuring safety against money laundering and terrorism financing.

As always, we will continue to monitor changes in these areas and provide updates with any new developments.

Peter D. Dugas

Managing Director, Center of Regulatory Intelligence

Peter has more than 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. government and in the implementation of enterprise risk management programs. He is a thought leader in government affairs and regulatory strategies in support of banks and financial institutions compliance with the Dodd-Frank Act and Basel Accords. Prior to joining Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

B. Washington, D.C. Regulatory Roundup

Regulatory and Compliance Alerts

OCC Requests Comment on Volcker Rule Revisions

On August 2, 2017, the Office of the Comptroller of the Currency (OCC) announced a request for comment related to revisions to the Volcker Rule. Specifically, the OCC is looking to tailor the rule's requirements and clarify key provisions that define prohibited and permissible activities. **Comments are due by September 21, 2017**.

FRB Proposes Supervisory Guidance regarding Role of Board of Directors

On August 3, 2017, the Federal Reserve Board (FRB) requested comment on a corporate governance proposal to enhance the effectiveness of boards of directors. The proposal would refocus the FRB's supervisory expectations for the largest firms' boards of directors on their core responsibilities, to promote the safety and soundness of their respective firms. The proposal would also help distinguish between the roles of the board and senior management. **Comments are due by October 10, 2017**.

SEC Releases Risk Alert on Cybersecurity

On August 7, 2017, the Securities and Exchange Commission (SEC) issued a risk alert entitled "Observations from Cybersecurity Examinations." The alert provides findings and observations concerning industry practices and legal and compliance issues related to cybersecurity preparedness, stemming from examinations the Office of Compliance Inspections and Examinations conducted as part of its Cybersecurity 2 Initiative.

NCUA Requests Comment on Regulatory Reform Plan

On August 16, 2017, the National Credit Union Administration (NCUA) requested comment on a package of regulatory reforms that an internal agency task force recommended. The task force recommended changes that NCUA would adopt in the coming four years to clarify, improve, revise or eliminate regulations. **Comments are due by November 20, 2017**.

Agencies Release HMDA Examiner Transaction Testing Guidelines

On August 22, 2017, the Federal Financial Institutions Examination Council (FFIEC) members announced new FFIEC Home Mortgage Disclosure Act (HMDA) Examiner Transaction Testing Guidelines for all financial institutions that report HMDA data. The guidelines will apply to the examination of HMDA data collected beginning in 2018 and reported beginning in 2019. These guidelines were a joint effort of the Consumer Financial Protection Bureau (CFPB), the Federal Deposit Insurance Corporation (FDIC), the FRB, the NCUA and the OCC to provide—for the first time—uniform guidelines across all federal HMDA supervisory agencies.

FRB Issues Policy Statement on Payment System Risk

On August 25, 2017, the FRB revised part II of the Federal Reserve Policy on Payment System Risk (PSR policy) related to the transaction posting times used for measuring balances intraday in institutions' accounts at the Federal Reserve Banks. This policy statement update conforms to enhancements to the Reserve Banks' same-day ACH service, **and goes into effect on September 15, 2017**.

C. Congressional Hearing Summary: BSA/AML

Before Congress adjourned for summer recess, reforms to Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regulations were a topic of interest. The House Financial Services Committee held two hearings addressing the issue. The first hearing focused mainly on traditional BSA/AML programs at financial institutions, while the second hearing honed in on some more unique challenges related to international remittances. The participants were as follows:

Examining the BSA/AML Regulatory Compliance Regime (June 28, 2017)

House Financial Services Committee,
Subcommitte on Financial Institutions and Consumer Credit

- **Faith Lleva Anderson**, Senior Vice President and General Counsel, American Airlines Credit Union, on behalf of the Credit Union National Association
- **Greg Baer**, President, The Clearing House Association, Executive Vice President and General Counsel, The Clearing House Payments Company
- **Lloyd DeVaux**, President and Chief Executive Officer, Sunstate Bank, on behalf of the Florida Bankers Association
- **Heather A. Lowe**, Legal Counsel and Director of Government Affairs, Global Financial Integrity

Managing Terrorism Financing Risk in Remittances and Money Transfers (July 18, 2018)

House Financial Services Committee,
Subcommitte on Terrorism and Illicit Finance

- **Duncan DeVille**, Senior Vice President, Global Head of Financial Crimes Compliance, Western Union
- **Matthew B. Oppenheimer**, President and Chief Executive Officer, Remitly, Inc.
- **John Cassara**, Member, Board of Advisors, Center on Sanctions and Illicit Finance, Foundation for the Defense of Democracies
- **Scott Paul**, Chief Humanitarian Policy Advisor, Oxfam America

Traditional Compliance Burdens

Since the passage of Dodd-Frank, compliance burdens have grown for financial institutions of all sizes. Witnesses' testimonies during both hearings stressed this point. DeVaux cited a Florida Bankers Association survey that found 91 percent of responding banks felt "BSA/AML regulation has caused them to avoid certain industries, decrease business development, and lower customer retention." DeVaux presented additional figures, stating that in 2007, 86 percent of Florida banks had five or fewer BSA/AML employees, whereas now only 62 percent have five or fewer. While DeVaux accepted that acquisitions account for a portion of this increase, he believes regulatory pressure, regulatory risk and concern regarding potential law enforcement were the main driving factors.

Building on this point about law enforcement action, Baer stated in his testimony that while there have been some egregious BSA/AML cases in which enforcement action was warranted, "many enforcement actions taken involve no actual money laundering."

Training is another substantial undertaking for financial institutions. Anderson described how her institution is required to conduct BSA/AML training for 600 employees annually. She also outlined how regular training must be supplemented with one-on-one and board training to help establish a strong culture of compliance. Additionally, she pointed out, some federal regulatory agencies require institutions conduct OFAC training.

The burden of ensuring full compliance can be daunting for banks and credit unions and is not any easier for Money Services Businesses (MSBs), particularly those operating internationally. Deville addressed how Western Union "has increased its compliance funding by more than 200 percent over the past five years, and now spends more than $200 million annually on compliance." As a result, Western Union has approximately 2,400 full-time employees, over 20 percent of its workforce, dedicated to compliance functions.

Suspicious Activity and Currency Transaction Reports

The witnesses identified opportunity for reform in two areas concerning core processes for a compliance program: suspicious activity reports (SARs) and currency transaction reports (CTRs).

	SARs	CTRs
Problems	• SARs are filed defensively for protection. • There is no dollar threshold for insider abuse. • The four largest banks file approximately half of the SARs filed annually. • Law enforcement's utilization of SARs leads to unnecessary filing. • Takes some depository institutions three to five days to process an average SAR.	• There is a $10,000 threshold set in 1970 (adjusted for inflation, this would be around $64,000 currently). • To identify additional suspects, accounts or assets during an investigation, law enforcement has only used 65 percent of CTRs filed.
Potential Solutions	• At least double the $5,000 threshold. • Impose a deadline to file SARs from 30 days to 40 days. • Issue more meaningful feedback from regulators so financial institutions can better utilize new technology like artificial intelligence and machine learning.	• Increase threshold to at least $20,000. • Potentially evaluate whether a common trend or basis is associated with unused CTRs. • Better utilize the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT) Section 314(a) on Information Sharing.

Regarding regulator feedback on SARs and the use of artificial intelligence and machine learning to improve financial institutions' compliance systems, Baer highlighted one concern:

> "[S]everal AML executives have reported that efforts to construct novel approaches to detecting illegal behavior have resulted in examiner criticism because such innovative approaches were deemed to lack sufficient documentation, and therefore were not auditable by bank examiners. Banks will be reluctant to invest in systems unless someone in the government can tell them that such systems will meet the banking examiners' expectations. Thus, we have a database created for one purpose and being utilized for another. Innovation awaits regulatory reorganization and leadership."

International High-Risk Areas

The witnesses also spent time discussing problems with some of the higher-risk areas of BSA/AML compliance. Financial institutions face potentially severe liability, both institutional and personal, when issues arise with lines of business that regulators identify as "high-risk." As a result, financial institutions have begun to "de-risk," defined by former U.S. Secretary of the Treasury Adam Szubin as "instances in which a financial institution seeks to avoid

perceived regulatory risk by indiscriminately terminating, restricting, or denying services to broad classes of clients, without case-by-case analysis or consideration of mitigation options."

In his testimony, Paul stated that customers affected by de-risking are "all viewed widely in the financial sector as inherently 'high-risk.'" However, the level of risk associated with a customer does not correlate with that customer's likelihood of law violation, but rather the likelihood of exploitation for terrorist financing, money laundering and other financial crimes.

Baer pointed out that de-risking can also lead to other major problems like:

- Forcing money into shadow markets or foreign banks
- A loss of political influence for the nation's diplomats
- A loss of allies for national defense
- Human suffering in countries cut off from correspondent banking, remittances and other access points to the global financial system

When looking at issues with the international remittance system, Cassara pointed to unofficial estimates placing remittances as high as $850 billion per year. Things like virtual currencies, mobile payments and other forms of new person-to-person (P2P) money transfers could potentially change and complicate traditional remittance networks like hawala. These new payment products and services will require attention, and financial institutions involved in international remittances will have to devote more resources to remaining compliant and preventing terrorism financing.

For this reason, many of the witnesses during the July hearing opposed the Border Wall Funding Act of 2017, introduced by Rep. Mike Rogers (R-AL). The bill would place a two percent tax on remittances to fund a border wall in the U.S. In opposition, Oppenheimer explained through his testimony that the two percent tax would effectively raise fees associated with remittance transfers to 10 percent. This would cause prices to double for consumers. "A pricing increase of this magnitude would lead customers to abandon licensed, regulator service options like Remitly, and engage in black market alternatives. By pushing this money underground, we would be funding the very illicit activities that we want to stop."

Conclusion

When Congress returns after Labor Day, it is expected BSA/AML discussions will continue. While difficult to predict whether changes will be made, the complexities and burdens associated with BSA/AML compliance are not likely to ramp down moving into 2018, with the beneficial ownership rule set to go into effect May 2018. As the number one use of compliance resources, BSA/AML will remain a chief focus for financial institutions.

D. Offering a Special Purpose National Bank Charter to FinTech Companies

Financial technology (FinTech) companies are not new, but with technology advancing as rapidly as it is, FinTech has been at the forefront of many conversations about the future of the world's financial systems. The Financial Stability Board (FSB) defines "FinTech" as: "technologically enabled financial innovation that could result in new business models, applications, processes, products, or services with an associated material effect on financial markets and institutions and the provision of financial services."

The current focus on FinTech firms has included recent official and intensive reports on the industry: FSB published for the G20 leaders in June 2017 a report on FinTech's potential financial stability implications and identified regulatory and supervisory issues for these types of institutions. And on August 10, 2017, the Federal Reserve Board (FRB) published a paper titled *FinTech and Financial Innovation: Drivers and Depth*, which covers FinTech origins, growth and potential to affect financial stability. Both reports address how FinTech will affect the future stability of financial systems, and the FSB report specifically addresses concerns many industry participants have voiced: while FinTech companies engage in banking activities, they are not held to the same standards and supervision as other banking entities, which creates risks and can potentially compromise financial stability.

In response to some of these concerns and after two years of research into the matter, earlier this year, the Office of the Comptroller of the Currency (OCC) announced its intentions to provide an option for certain FinTech companies to apply for a Special Purpose National Bank (SPNB) charter. While there are other types of special purpose national banks to which the OCC's existing policies refer, this "SPNB" would be chartered as a national bank that does not take deposits within the Federal Deposit Insurance Act (FDIA) definition, but be approved to engage in a limited range of banking activities, including one of the core banking functions: taking deposits, paying checks or lending money. Because a FinTech company applying for this charter cannot be insured by the Federal Deposit Insurance Corporation (FDIC), it is likely the institution would satisfy one of the latter two functions.

The OCC believes the National Bank Act is broad enough to permit new banking activities or new approaches for traditional banking activity participation.

Discounting notes, purchasing bank-permissible debt securities, engaging in lease-financing transactions and making loans are forms of ***lending money***.

Issuing debit cards or engaging in other means of facilitating payments electronically may be considered the modern equivalent of ***paying checks***.

Since the OCC began researching the matter over two years ago, there has been significant activity regarding the proposal of an SPNB charter for FinTech companies. This includes changes in leadership at the OCC, legal battles with different federal and state agencies, opposition and support from those in the field and the general public, major developments within the planning process and other factors contributing to where the OCC stands today on the charter. The following is a timeline of the activity surrounding the SPNB proposal from its inception.

A Timeline of FinTech Charter Activity

August 2015	The OCC begins researching the implications of financial services industry innovation to develop a framework for ensuring innovation is responsible. Research includes, but is not limited to, discussions with FinTech companies, banks, community and consumer groups, academics and other regulators.

March 2016	The OCC publishes a white paper, *Supporting Responsible Innovation in the Federal Banking System: An OCC Perspective*, that outlines principles for the development of a framework supporting responsible innovation in the federal banking system.
October 2016	The OCC announces plans to execute its responsible innovation framework, and establishes an Office of Innovation serving as the central contact and clearing house for requests and information related to novel advancements. The office conducts outreach and provides resources for banks and nonbanks to understand regulatory expectations and principles.
December 2016	Comptroller of the Currency (at the time) Thomas Curry, a President Barack Obama-appointee announces the OCC's plans to consider SPNB charter applications from FinTech companies. The OCC publishes and requests public comment on a paper titled *Exploring Special Purpose National Bank Charters for FinTech Companies*, which describes the OCC's legal granting authority and articulates the OCC's charter requirements. The paper clarifies that the OCC will hold any SPNB chartered FinTech company to the same standards of safety and soundness, fair access and fair treatment of customers required of all federally chartered institutions.
January 2017	The OCC receives over 100 comment letters on the SPNB paper. After reviewing all comments, the OCC states that it will be guided by certain threshold principles in evaluating applications from FinTech companies for an SPNB charter. These principles also inform the creation of the draft Supplement and are as follows: • The OCC will not allow the inappropriate commingling of banking and commerce. • The OCC will not allow products with predatory features nor will it allow unfair or deceptive acts or practices. • There will be no "light-touch" supervision of companies that have an SPNB charter. Any FinTech companies granted such charters will be held to the same high standards that all federally chartered banks must meet. Aligned with those principles, the OCC believes that making SPNB charters available to qualified FinTech companies would be in the public interest because applying a uniform regulatory framework, process and supervision to the entire FinTech industry will, in the opinion of the OCC: 1. Help ensure that these companies operate in a safe and sound manner so that they can effectively serve the needs of customers, businesses and communities, just as banks that operate under full-service charters 2. Promote consistency in the application of law and regulation across the country and ensure that consumers are treated fairly 3. Make the federal banking system stronger by not only helping to ensure that these companies operate in a safe and sound manner, but also encouraging them to explore new ways to promote fair access and financial inclusion and innovate responsibly One of the comment letters submitted in strong opposition to the OCC charter was that of New York Department of Financial Services (NYDFS) Superintendent Maria Vullo. In her letter, she outlined that: • The OCC proposal ignores decades of experienced state-based regulatory authority for nonbank financial services companies, including "FinTech," never before regulated by the OCC. • State regulators are best equipped to guard against predatory and abusive practices targeting consumers in their borders. • The proposal lacks legal authority and threatens the growth of small businesses while potentially creating more "too big to fail" companies with lax oversight.

March 2017	The OCC issues a draft licensing manual supplement for evaluating SPNB charter applications from FinTech companies, titled *Comptroller's Licensing Manual Draft Supplement: Evaluating Charter Applications From Financial Technology Companies*. Additionally, the OCC also issues guidance to explain the review process for comments on the December 2016 paper, titled *OCC Summary of Comments and Explanatory Statement: Special Purpose National Bank Charters for Financial Technology Companies*. Though not required, the OCC held a comment period on their March 2016 Draft Supplement through April 2017.
April 2017	**April 26**: The Conference of State Bank Supervisors (CSBS) announces it has filed a complaint against the OCC in the U.S. District Court for the District of Columbia, seeking an injunction to stop the agency from moving forward with the SPNB charter. **April 28**: Curry gives a speech at the "FinTech and the Future of Finance" conference Kellogg School of Management, Northwestern University, in which he acknowledges opposition to the OCC's intent to offer SPNB charters to FinTech companies and discusses the OCC's thorough review of public comments before taking next steps. He also outlines the activities of the Office of Innovation since its inception and moving forward.
May 2017	**May 5**: Curry steps down from office after a one-month extension of his five-year term. President Donald Trump appoints Keith Noreika as Acting Comptroller of the Currency. **May 12**: NYDFS files a complaint against the OCC in the U.S. District Court for the Southern District of New York, based on the idea that granting an SPNB charter for FinTech companies is out of the OCC's jurisdiction, based on the definition of the "business of banking."
June 2017	CSBS launches a FinTech advisory panel with hopes of modernizing state regulation of FinTech companies and aims to: "discuss existing pain points in multi-state licensing and supervision, brainstorm possible solutions, and provide feedback to ongoing state initiatives"
July 2017	Noreika gives a speech before The Exchequer Club, in which he mentions that the NYDFS named him as a defendant in a lawsuit challenging the OCC's authority to grant SPNB charters to FinTech companies. He nonetheless argues the potential positive contributions such a charter would make and refutes the idea that it would be detrimental to banks. In response, Vullo said in a press statement, "New York continues to stand by its position that the OCC lacks the authority to charter nonbank financial services firms and only state regulators like DFS have the extensive experience, knowledge, and skills to supervise these cash-intensive companies."

The lawsuits ask: Does the OCC have the authority to grant this type of charter?

The OCC's proposed FinTech charter has been a hot topic in recent months in part due to the legal battles surrounding the proposal. The OCC claims that it's chartering authority includes the authority to charter special purpose national banks, with trust banks and credit card banks as examples of special purpose national banks for which it has already granted operational permissions. Under 12 CFP 5.20 (e)(1):

> "The OCC charters a national bank under the authority of the National Bank Act of 1864, as amended, 12 U.S.C. 1 *et seq.* The bank may be a special purpose bank that limits its activities to fiduciary activities or to any other activities within the business of banking. A special purpose bank that conducts activities other than fiduciary activities must conduct at least one of the following three core banking functions: Receiving deposits; paying checks; or lending money..."

Opposition to the charter specifically questions whether or not the OCC has the statutory authority to grant a FinTech charter. In response to the second white paper which the OCC published on FinTech charters, U.S. Senators Sherrod Brown (D-OH) and Jeffrey Merkley (D-OR) wrote:

> "Because many of these [FinTech] firms evidently do not intend to accept deposits, it is far from clear whether the OCC has the authority to grant national bank charters to them. Congress has given the OCC a very narrowly-defined authority to charter only three special-purpose national banks (bankers' banks, credit card banks, and trust banks) that do not accept deposits .... An alternatively chartered firm that does not take deposits by offering transactions or savings accounts, and therefore does not encourage the fundamental banking act of building wealth by encouraging savings, should not be able to refer to itself as a "bank."

Applicants

In addition to whether or not a proposed bank can reasonably achieve and maintain profitability and contribute to "healthy" market competition, the OCC's governing statutes and regulations outline the following principles for national bank evaluation:

- Maintaining a safe and sound banking system
- Encouraging a national bank to provide fair access to financial services by helping to meet the credit needs of its entire community
- Ensuring compliance with laws and regulations
- Promoting fair treatment of customers, including efficiency and better service

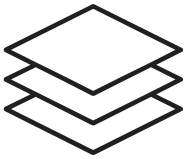
This means the OCC is committed to only considering applications for SPNB charters from FinTech companies that will avoid predatory, unfair or deceptive acts or practices and the inappropriate merging of bank and commerce. To ensure it meets these standards, the OCC requires proposed SPNBs to show they have experienced and appropriate organizers and management; adequate finances to support the risk profile and business activities; a clear and compelling business plan; and, if applicable, a Financial Inclusion Plan (FIP) that outlines full inclusion of and service to the target market.

The OCC makes it clear they will not allow companies, through an SPNB charter application, to avoid the consequences of an investigation or enforcement action of another regulator. Further, the OCC can deny a charter

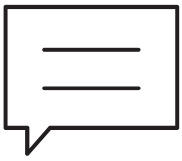
application due to a pending regulatory investigation or enforcement action, but at a minimum, the OCC will consult with the other regulator to ensure remediation is sufficient to consider the application.

The OCC plans to assess any activities not previously considered to be a "core banking activity." Organizers of a charter application must be able to discuss the permissibility of such activities and legal analysis may be required. In such a case, the OCC will conduct an independent legal analysis.

Tips Before Applying for the FinTech SPNB Charter



Applicant should familiarize themselves with applicable licensing procedures, including a variety of OCC publications with relevant information.



Applicant can contact the OCC's Office of Innovation regarding any preliminary questions and inquiries.

The Chartering Process for FinTech SPNBs

Chartering Process	
1	The Office of Innovation will schedule an exploratory meeting with the applicant and OCC staff and Licensing Division to review to applicant's business model and alignment with charter application requirements (as discussed later in this article) and the OCC's expectations.
2	The OCC will assign a licensing contact, who will form a group of OCC staff to informally review the applicant's proposal. This group might include examiners, subject matter experts, legal staff and others who will be able to provide assistance through the chartering process and ensure the applicant is aware of all application requirements.
3	The applicant must provide the following to its assigned OCC staff committee: • An overview of the FinTech charter proposal, including a discussion of the business plan and the relevant market, including an FIP, as well as any novel policy or legal issues and any unique aspects of the proposal • Information about the qualifications of the applicants and proposed senior management • Any informational submissions the OCC requests prior to the submission of an application, such as a draft business plan
4	Depending on complexity and novelty of application, there may be one or more formal prefiling meetings with the applicant and its assigned committee.
5	Applicant files the charter application according the procedures set forth in the "Charters" booklet of the *Comptroller's Licensing Manual*. The application will include a business plan (detailed later in this article) and the appropriate Interagency Biographical Report on all identified insiders.

6	As soon as possible before or after the filing, the applicant must publish a notice of charter in the community in which the proposed bank will be located and allow a 30-day comment period following publication. The OCC can provide a public file of the application to any requester and, in addition, makes a public file available on the OCC website. A "public file" has portions of the business plan, such as FIP section, but applicants may request certain sections be redacted.
7	Upon review of the application and any comments received during the public comment period, the OCC may grant preliminary conditional approval or deny the application. Under a preliminary conditional approval, the OCC will impose a number of standard requirements that apply to all de novo institutions and a set of special requirements tailored to the applicant. These requirements may apply only for the preliminary period, or may carry over into the OCC's permanent requirements for a chartered SPNB's official operation.
8	If granted a preliminary conditional approval, the proposed charter now enters the "Organization Phase"—the company must raise capital, fill necessary employee positions, adhere to all rules and regulations set forth by the OCC's preliminary conditional approval and begin business activity within 18 months (or apply for an extension). The OCC may additionally require the applicant to enter into an operating agreement.
9	If the applicant meets all requirements and conditions of approval, the OCC may grant final approval of the application and issue a charter for the SPNB, meaning the SPNB may begin conducting its banking business as an OCC-chartered bank. Until the OCC's official modification or removal of approval conditions, the SPNB will retain all conditions that the OCC set forth prior to approval. The conditions include compliance examinations, along with other supervisory activities outlined later in this article.

Elements of an Application's Business Plan

The OCC expects FinTech charter applicants to submit as part of their application a business plan in line with the Interagency Business Plan Guidelines, which require including a description of the business; marketing plan; management plan; records, systems, and controls; the financial management plan; monitoring and revising the plan; alternative business strategies; and financial projections. There is also information in the *Comptroller's Handbook*, specifically in the "Charters" booklet including sections on operations such as audit requirements, information technology (IT) and corporate risk and governance.

Because applicants for an SPNB charter will likely have business models that differ from those of traditional, full-service banks, the OCC has provided additional guidance to supplement the interagency guidelines:

Topic	Questions to Ask
Risk Assessment	□ Does the plan examine potential risk areas (such as concentration risk, compliance risk, reputation risk, strategic risk and operational risk)? □ Does the plan discuss risks related to cybersecurity? □ What is the institution's risk appetite? □ What is the institution's risk management plan, and does it consider the economic and competitive conditions of the target markets? □ Does the plan consider Bank Secrecy Act/Anti-Money Laundering (BSA/AML), consumer protection and fair lending laws? □ Does the plan describe the risk-mitigating system and internal controls?

Records, Systems and Controls	Does this section contain descriptions of the institution's: □ IT program, including what internal controls are in place to ensure data security; overviews of operational, security and resiliency structures; and cybersecurity risk governance frameworks? □ compliance management program, which guarantees an institution-wide adherence to all applicable laws and regulations? □ outsourcing and third-party risk management, with each potential engagement outlined and appropriately detailed based on the risk level and complexity of the engagement?
Financial Management	□ In addition to the minimum leverage and risk-based capital requirements that apply to all national banks, as outlined in the Capital Adequacy Standards of 12 CFR 3, does the institution consider other metrics that would be more appropriate in considering the unique operations of the institution? □ Does this section of the business plan outline both initial and ongoing minimum capital requirements, especially for operation in adverse markets? □ Does the section outline funds management models that reflect changing liquidity thresholds as the institution evolves?
Monitoring and Revising the Plan	□ Do the applicants show that their institution's board of directors has a system to monitor business plan adherence? □ Is the business plan able to accommodate technology's rapid changes?
Alternative Business Strategy; Contingency Plans; Recovery and Exit Strategies	□ Did the applicants identify critical assumptions in the business plan and develop contingency plans for disparities in expectation and possible reality; plans for recovery and viability under stress; and exit strategies for organized disentanglement from the market?
Financial Inclusion Plan	□ Does the FIP identify and define: • the products and services the SPNB will offer, highlighting those that will promote financial inclusion of underserved populations; • the institution's market and community, recognizing underserved populations or geographies; • the identified community's financial services needs and how the SPNB's products may serve some of these needs; • milestones and measurable goals for meeting FIP objectives; and • the terms and conditions under which the SPNB will lend or provide financial services to small businesses or consumers? □ Does the application show commitment to financial inclusion, if the institution's business plan includes consumer or small business lending or financial services? □ Does the application show whether the SPNB, if approved, might participate in governmentally insured, guaranteed or subsidized loan programs; how the institution's operations will ensure fair and non-discriminatory services; and the institution's ability to modify its FIP, both through public input and changing circumstances?

Supervision After Approval

Approved FinTech charters will have a supervisory framework that is similar to the framework for all OCC-supervised banks, with the core elements of this being:

- A dedicated portfolio manager who will have the subject matter expertise appropriate for the SPNB business model to serve as the primary point of contact and examiner-in-charge for the institution
- A specifically-dedicated Assistant Deputy Comptroller (ADC) for SPNB supervision who will report to the Deputy Comptroller for Thrift Supervision and Special Supervision
- A custom supervision plan that considers the bank's business model and a variety of supervisory activities which a tailored expert examination team will conduct both on-site and off-site

The younger the institution and the larger or more complex it is, the more frequent and intensive the supervision is likely to be, including regular communication with the bank's board of directors and management team. This supervision will be supplementary to statutory examination requirements and comparable to the supervision already outlined for de novo institutions.

The same ratings framework that applies to other OCC-supervised banks will also apply to SPNBs, as outlined in Appendixes A-G of the OCC's "Bank Supervision Process" booklet and in accordance with the Federal Financial Institutions Examination Council (FFIEC) Uniform Financial Institutions Rating System (UFIRS). This uniform and comprehensive system, commonly referred to as the CAMELS/ITCC, assesses components of a bank's performance as well as specialty areas that include: capital adequacy, asset quality, management, earnings, liquidity, sensitivity to market risk, information technology, trust, consumer compliance, and performance under the Community Reinvestment Act, if applicable.

Each SPNB must also have risk management frameworks in place that are appropriate for the institution's risk volume and complexity. A sound risk management system will identify risk at the transaction and portfolio levels, based on new business initiatives, changing regulations, third-party engagements and the external market; measure risk quickly and effectively; monitor risk presently to ensure immediate risk position review and risk limit exceptions, swift corrections and appropriate notifications if necessary; and control risk by clearly delineating responsibilities and authorities through established policies, standards and procedures. As is the case for other national banks, the OCC expects SPNBs to have corporate governance frameworks that actively engage an institution's board of directors and comprises the "three lines of defense" model.

The OCC will communicate with each SPNB on a case-by-case basis, through formal and informal meetings, conversations, examinations, etc. At least once per supervisory cycle, the OCC will provide a bank's board of directors with a report of examination (ROE) outlining the bank's overall condition, ratings and risk assessment summary.

The Pros and Cons of SPNB Chartering for FinTech Firms

While the research and planning for this SPNB charter has been in the process for over two years, it is still difficult to forecast the effects this chartering option will have on the financial services industry. Notably, there has been significant pushback from many in the financial services industry, particularly from traditionally-chartered banks. Additionally, this matter is receiving attention not only from those within the industry and those involved on a legal level, but also individuals from a variety of fields, including academia.

As discussed earlier in this article, much of the legal action assumes the charter option would make FinTech firms, in Vullo's words, "too powerful." On the other hand, some people question whether the charter option is a positive move for FinTech firms themselves: as Brian Knight, a professor at the Mercatus Center at George Mason University, states in his paper *Federalism and Federalization on the FinTech Frontier*,

> "If the OCC's charter simply applies regulations built for universal banks to much more limited companies or if it otherwise imposes significant costs, it may be of little value to new entrants that lack the resources to manage the associated regulatory burden. Likewise, if the OCC regulates FinTech firms, which rely on speed and nimbleness to survive, in the same way that it regulates banks, the FinTech firms—especially newer, smaller firms that are still finding their way—may not remain viable."

While the OCC has made clear their intentions of tailoring each application process, approval and subsequent supervision to each SPNB, it is interesting to note that the banks the OCC supervises fund the agency through assessments and fees. It has supplemented the assessments for other limited purpose national banks (e.g., credit card companies and trust banks) to account for the banks' activities and asset types and it seems likely the OCC will similarly require supplementary supervisory activities for SPNBs, which may create serious financial burden and stress on such institutions.

Some people feel, however, that these types of charters will be too advantageous for FinTech firms, and cause unfair market imbalances. These critics point out that while other banks must comply with state standards, SPNBs might be preempted from these regulations and therefore benefit from fewer restrictions than their non-SPNB competitors.

The OCC has attempted to refute this, and additionally recognizes that becoming an SPNB will remain one option of many for FinTech firms' operation in the regulated space. Some states offer the option for FinTech firms to operate under state banks or state trust bank charters and FinTech firms in these states may elect this form of operation. Other FinTech firms might adjust their business plans and services so as to qualify and apply for a full-service national bank charter or another type of limited purpose national bank.

Some FinTech firms have already partnered with banks to provide services and expertise, and this operating model continues to be available. For example, many banks have begun to roll out their own versions of people-to-people payment options through mobile applications. There are also cases of bank partnerships with online lending companies, and some banks now offer their clients small-dollar amount "one-click" loans through their mobile platform. Further examples of these partnerships include services like mobile financial advising, real-time receipts from credit and debit card purchases and a tool that uses artificial intelligence to predict borrower payment delinquency.

While the financial services industry awaits further and more concrete developments about the OCC's proposed SPNB charter for FinTech firms, it remains clear that the cutting-edge technologies these FinTech firms provide will continue to change the market and the way the world's citizens interact with money.

E. BSA/AML Trends

This summer has marked multiple developments related to anti-money laundering (AML) compliance, including the Financial Crimes Enforcement Network's (FinCEN) enforcement of the Bank Secrecy Act (BSA)/AML regulations in two "hot-topic" areas: money laundering through real estate transactions and through virtual currency. In this article, we discuss current trends in AML in the U.S. and provide an overview of AML-related changes to the EU gaming industry.

BSA/AML Trends in the US

FinCEN publicly states its mission "is to safeguard the financial system from illicit use and combat money laundering and promote national security through the collection, analysis, and dissemination of financial intelligence and strategic use of financial authorities." In the U.S., BSA/AML regulations make money laundering itself a crime and establish requirements for financial services firms to detect, deter and disrupt money laundering, terrorist financing and other criminal activities.

In the past, FinCEN acted mostly as a data-gathering agency, but in more recent years, the agency has taken a significantly more aggressive enforcement agenda to combat money laundering and terrorist financing.

***TRENDING* Proceeds from Criminal Activity go Unnoticed in Real Estate Market**

According to FinCEN estimates, suspicious activity report (SAR) requirements for the mortgage lending industry make 78 percent of residential purchases in the U.S. subject to BSA/AML compliance. The remaining transactions are almost entirely "all-cash" deals. In these types of transactions, since there is no involvement from a regulated financial institution (i.e., the purchaser does not require a loan to complete the acquisition), firms and professionals that are involved (e.g., settlement/closing attorneys and agents, appraisers and title search and insurance companies) are under no legal obligation to identify or report any suspicious activity.

A Background on GTOs

The BSA authorizes GTOs, which originally could only last for 60 days; the USA PATRIOT Act extended this to 180 days. Historically, FinCEN did not publicize GTOs, but since 2014 has given multiple press releases and speeches on these initiatives. Among its first publicly-announced GTOs were those seeking to investigate funnel accounts and trade-based money laundering (TBML) activities. This included:

- Armored car services and other common carriers of currency along the U.S.-Mexico border
- The Los Angeles Fashion District
- Electronics exporters in South Florida

FinCEN noted that this gap leaves significant risk for money laundering and terrorist financing in the high-end real estate market when individuals attempting to hide their identities and assets can do so through non-transparent methods (e.g., shell companies). A notice from the New York Department of Financial Services (NYDFS) said, "Terrorists, drug traffickers, human traffickers and other criminals, by using U.S. shell companies, are able to access cash in New York and other states through a variety of transactions, including purchasing real estate and then selling it, to finance criminal activities." And in an investigation of 2015 home sales, the New York Times found shell companies purchased almost half of residential homes over $5 million.

In an attempt to combat this threat, FinCEN issued real estate-focused Geographic Targeting Orders (GTOs) in 2016, which temporarily required certain title insurance companies to perform customer due diligence (CDD) and identify the people behind high-end real estate all-cash purchases in Manhattan and Florida's Miami-Dade county. The same NYDFS notice showed approval of this action: "Requiring full transparency and disclosure of beneficial ownership when a company is established or incorporated in the U.S. would enhance the ability of state and federal enforcement and regulatory authorities to combat financial crime, terrorist financing and money laundering."

FinCEN expanded the list of areas in July 2016 to include of all the boroughs of New York City; the counties of Broward and Palm Beach in Florida; the counties of Los Angeles, San Diego, San Francisco, San Mateo, and Santa Clara in California; and the county of Bexar (San Antonio) in Texas. The agency renewed the GTOs in February 2017, ending August 2017, after finding that about 30 percent of GTO-covered transactions involved a beneficial owner or purchaser representative that had also been the subject of a previous SAR. This evidence corroborated FinCEN's expectations.

Most recently, on August 22, 2017, FinCEN announced the issuance of revised real estate-related GTOs which included adding the City and County of Honolulu, HI. Following the recent enactment of the Countering America's Adversaries through Sanctions Act, FinCEN revised the GTOs to capture a broader range of transactions and include transactions involving wire transfers. FinCEN simultaneously issued an advisory to financial institutions and the real estate industry on the money laundering risks associated with real estate transactions.

***TRENDING* AML Enforcement for Virtual Currency**

FinCEN issued guidance in 2013 classifying virtual currency exchangers as "money transmitters" under the BSA and requiring these businesses to register with FinCEN and follow certain AML measures. Specifically, the guidance stated, "an administrator or exchanger is an MSB under FinCEN's regulations, specifically, a money transmitter, unless a limitation to or exemption from the definition applies to the person."

FinCEN's first-ever civil enforcement action against a virtual currency exchanger occurred in May 2015, in conjunction with the U.S. Attorney's Office for the Northern District of California. The action was a $700,000 civil money penalty the second largest cryptocurrency by market capitalization after Bitcoin at the time. By acting as a money services business (MSB) and selling its virtual currency, the company willfully violated multiple provisions of the BSA. The firm did not register with FinCEN as an MSB and did not implement and maintain an AML program to adequately disallow money launderers or terrorist financers from using the products.

Following this action, in May 2015 FinCEN Director at the time Jennifer Shasky Calvery announced the agency would be instigating a series of supervisory examinations of virtual currency businesses with the help of BSA examiners at the Internal Revenue Service (IRS).

On July 27, 2017, FinCEN issued its second supervisory enforcement action against a virtual currency exchanger and the first against a foreign-located MSB. In coordination with the U.S. Attorney's Office for the Northern District of California, FinCEN assessed civil money penalties of over $110 million against a Bulgaria-based virtual currency exchanger and $12 million against one of their operators for willfully violating U.S. AML laws.

The company operates as an exchanger of convertible currency, which according to FinCEN's assessment, would make it an "MSB" and a "financial institution" under the BSA, and particularly a "money transmitter." However, the company did not register with FinCEN as an MSB. Among other things, the FinCEN civil money penalty assessment identified that the company:

1. Failed to implement policies, procedures and internal controls reasonably designed to prevent the MSB from facilitating money laundering
2. Failed to collect and verify basic customer information needed to comply with the BSA and even after implementing policies for customer identification, stated compliance with the policies was "optional"
3. Processed transactions with digital currency features that restricted the company's ability to verify customer identification or monitor for suspicious activity, allowing users to transfer over $40 million on its platform from bitcoin mixers

4. Lacked adequate procedures for conducting due diligence, monitoring transactions and refusing to consummate transactions that facilitated money laundering or other illicit activity; for example, the users "openly and explicitly" discussed conducting criminal activity through internal messaging systems, public postings and user chats

5. Failed to file a single SAR, including on transactions involving funds stolen from the Mt. Gox exchange even after the thefts were publicly reported in the media

6. Failed to meet the most basic recordkeeping requirements

TRENDING *AML Changes in Gaming for EU Member States*

This summer is also an important time for European AML developments, with a June 26, 2017 compliance date for the European Union Fourth Anti-Money Laundering Directive (Fourth Directive). Member states had two years to adapt their national laws to adhere to the Fourth Directive.

The Fourth Directive makes important changes to AML regulations for the gaming industry, particularly by amending enhanced CDD requirements. Under the directive, gaming operators must apply CDD measures for single transactions amounting to €2,000 or more, including the collection of winnings and purchasing or exchanging of gambling chips. Also, brick-and-mortar gaming sites should ensure that CDD, if taken at the point of entry to the premises, can be linked to the transactions the customer conducts on those premises.

But, the Fourth Directive does allow for EU member states to exempt certain low-risk gambling services from some or all of the requirements. Member states should only use the exemption in limited and justified circumstances, subject to specific risk assessments which consider the degree of vulnerability of the applicable transactions. The Fourth Directive also requires that authorities ensure the business executives and beneficial owners of gaming operators are fit and proper.

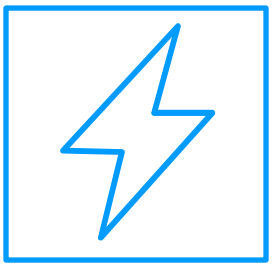
In July, the Malta Gaming Authority, in coordination with the Financial Intelligence Analysis Unit of Malta, released a consultation document for the application of anti-money laundering and countering the funding of terrorism (AML/CFT) obligations to its remote gaming sector (internet gaming). The consultation enters the Fourth Directive into Maltese law. While the island country is very densely populated, it remains the smallest member of the EU. However, it does have a thriving remote gaming sector. For this reason, the application of CDD requirements for Malta's remote gaming sector are important.

Malta's remote gaming sector is also important for another reason: in crafting their internet gaming regulations, the New Jersey Division of Gaming Enforcement (DGE) hired a former Maltese gaming regulator to serve as an official consultant. New Jersey's internet gaming market dwarfs that of Nevada and Delaware, the other two states operating internet gaming. If more states decide to offer regulated internet gaming in the coming years, looking to Europe and Malta as models may also be an option. This could also apply for internet gaming AML regulations.

Other Notable Elements from Malta's Consultation Document

For syndicated gaming, where funds are collected from multiple persons who will share in any winnings, both the customer and other persons providing the funding are subject to due diligence requirements. The persons providing funding are to be considered "beneficial owners." In the U.S., the beneficial ownership rule set to take effect in 2018 generally doesn't apply to the gaming industry.

When a customer is identified as "low-risk," a gaming operator may apply lower CDD requirements. However, the gaming operator is required to carry out verification and collect any other information necessary to build a better profile of the customer, including source of wealth when the customer deposits €150 or more into their gaming account, whether through a single transaction or a series of transactions.



It is possible that a business relationship will present a low risk of money laundering or financing of terrorism even though the customer's activity is no longer considered "low value." In those instances, gaming operators may apply lower CDD requirements but are not permitted to delay verification of the customer's identity and the collection of required information like source of wealth.

Conclusion

Recent developments concerning BSA/AML are far-reaching and varied, affecting multiple industries in terms of new regulations, enforcement actions and other changes. With all the new developments, it is important for financial institutions to evaluate their existing and new business units, products, services and customer relationships to determine the applicability of BSA/AML regulatory requirements and as part of the BSA/AML risk assessment process.

F. Did You Know?

Third-party Relationship Management Services

Financial institutions are expected to have a comprehensive risk management process in place to govern their service provider relationships. The FIS third-party risk management assessment will determine the efficacy of controls implemented to minimize and adequately manage third-party risk.

An effective third-party risk management process incorporates the following activities, at a minimum:

- Risk assessment and requirements definitions
- Due diligence in selecting a service provider
- Contract negotiation and implementation
- Ongoing monitoring.

Working with your management team, our domain experts will develop an understanding of your institution's third-party management infrastructure, gathering information related to overall third-party management responsibility and managing the day-to-day activities with critical third parties, including periodic third-party oversight activities.

Using regulatory guidance and industry best practices, we will review:

- Third-party management policies and procedures
- Third-party risk assessments and assignment of third-party risk categories
- Documentation of due diligence conducted for new third parties
- Critical third-party contracts for standard content based on your institution's policies
- Third-party oversight efforts, including evaluation of third parties' financial condition, compliance with service-level agreements, evaluation of the third party's SSAE 16 or similar security audit and evidence of third parties' business continuity plans testing
- Documentation of senior management's reporting to the board of significant third-party issues, including new and terminated contracts, outsourcing risk assessments and critical third-party oversight

Capco will work with your risk management team to deliver a comprehensive third-party risk management assessment that provides a foundation for developing and executing plans to effectively mitigate third-party service provider-related risks.

G. About Capco's Center of Regulatory Intelligence

Capco is a global management consultancy with a focus in financial services including banking and payments, capital markets, and wealth and asset management. The Center of Regulatory Intelligence (CRI) opened in Washington, D.C. on June 16, 2015. The primary goal of CRI is to translate policy, legislative and regulatory developments into actionable intelligence for Capco clients to enable knowledge advantage. The unique perspective gained by monitoring regulatory change in such close proximity to the policymakers and regulators enables CRI to empower Capco clients to stay one step ahead, identify impact precisely, make smart business decisions and succeed. Capco clients receive insights from CRI through regularly published regulatory intelligence briefings and thought leadership insights intended to give client institutions deep intelligence into regulatory initiatives coming out of the legislature, administration and regulatory agencies. Input from CRI also helps drive Capco consulting services aimed at helping address regulatory changes prior to implementation.

CRI provides the latest intelligence, thought leadership and cutting-edge regulatory insights into risk, information security and compliance issues facing the financial services industry. This FIS thought leadership center provides early insight on regulatory changes, helping financial services clients stay compliant with new regulations. Through CRI, Capco interfaces with key policymakers to provide industry perspectives on the potential impacts of regulatory mandates to financial institutions.

Contact Us

Capco Center of Regulatory Intelligence
1101 Pennsylvania Ave.,
NW Suite 300 Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

Register your colleagues to receive regular updates from Capco's Center of Regulatory Intelligence.