# VACB: FinTech Forum 2019

## *Contracting for FinTech Services*

troutman sanders

October 15, 2019

**Presented by: Mark W. Jones**
Troutman Sanders LLP
mark.jones@troutman.com
(804) 697-1294

## Overview of Presentation

- **The buck stops with *you***
- **FDIC framework for effectively managing third party relationships**
  - Risk assessment
  - Due diligence in selecting a third party
  - Contract structuring
  - Oversight

---- FDIC FIL-44-2008, Third-Party Risk: Guidance for Managing Third-Party Risk, June 6, 2008

## The Buck Stops with *You*


- Desk plaque of President Harry S. Truman, 33rd President of the United States
- *Idiom; informal*: **the ultimate responsibility rests here**. [Short for "*buckhorn knife*" (from its use as a marker in poker)].
  *--The American Heritage Dictionary of the English Language, 5th Ed.*



troutman sanders

## The Buck Stops with *You* (cont.).

**Outsourcing does not relieve a bank or its management from their obligations to conduct business in a safe and sound manner and in compliance with applicable law**

- **"When service are outsourced, a financial institution's *board of directors and senior management are responsible* for managing the risks posed by those services as if they were performed within the institution."**

  ***----FDIC FIL-19-2019, Technology Service Provider Contracts, April 2, 2019***

- **"Institutions and their customers can achieve benefits through outsourcing of products and services. However, *responsibility* for managing the risks associated with those products *cannot be outsourced*."**

  ***----FDIC FIL-81-2000, Risk Management of Technology Outsourcing, November 29, 2000***



troutman sanders

## Risk Assessment

### Risk assessment is fundamental to the initial decision of whether to enter into a third-party relationship

- Consistency with strategic planning and business strategy
- Cost / benefit analysis
- Initial requirements for business goals and regulatory compliance
- Ability to provide long-term oversight and management of the proposed third-party relationship
- Likely long-term financial effect of the proposed third-party relationship.



troutman sanders

## Due Diligence in Selecting a Third Party

### Quantitative and qualitative due diligence should be performed on third-party vendors both before selecting a counterparty and periodically during the relationship

- Business reputation and experience of the counterparty and its principals
- Litigation and regulatory history of the counterparty and its principals
- Specific experience with particular service or product, including familiarity with applicable laws and regulations
- Adequacy of audit, internal control, IT systems, and data / cybersecurity
- Financial condition and results of operations, including pro forma for the effect of the proposed relationship



troutman sanders

## Contract Structuring

### FDIC has re-emphasized the importance of contract structuring and review in managing third-party vendor risk

> **"Undefined and unclear contract terms could contribute to ambiguity in financial institution rights and service provider responsibilities, and could increase the risk that technology service provider business disruptions or security incidents will impair financial institution operations or compromise customer information."**
>
> **----FDIC FIL-19-2019**



troutman sanders

## Contract Structuring – Key Terms (cont.)

**FDIC FIL-44-2008, Third-Party Risk: Guidance for Managing Third-Party Risk, June 6, 2008**

- **Scope –** clearly identify the rights and responsibilities of each party
- **Costs / Compensation**
  - Describe all applicable fees and compensation, including variable or contingent items
  - Allocate responsibility for expenses associated with the contract (e.g., equipment, software, etc.)
  - Compensation should not improperly incentivize the third party to take imprudent risks on behalf of the bank or push the regulatory envelope
- **Performance Standards** – if possible given the nature of the contract, measurable performance standards and consequences for failure to meet them
- **Reports / Audit Rights**
  - Nature and frequency of reports from third-party, including exception-based reports
  - Access to audit reports; right of bank to audit third-party's performance directly
  - Internal controls



troutman sanders

## Contract Structuring – Key Terms (cont.)

- **Confidentiality and Security**
  - Terms should ensure that bank can comply with its obligations under Gramm Leach Bliley and other applicable law
  - Handling of customer information should be consistent with bank's privacy policy
  - Breaches and potential breaches should be promptly disclosed to the bank
- **Business Resumption and Contingency Plans** – detail third party's responsibilities in event of an operational failure of any kind, including data and systems back-ups
- **Default and Termination**
  - Identify defaults, remedies, grace periods and termination events
  - Bank should have right to terminate the agreement if serious bank regulatory compliance issues arise
  - Address handling of shared data post-termination
- **Subcontracting** – if subcontracting is allowed, allocate responsibility for subcontractor's actions to third-party and address selection and monitoring of subcontractors



troutman sanders

## Contract Structuring – Key Terms (cont.)

- **Ownership and Licenses** – ownership and use of bank property, including data, equipment, software, records and intellectual property (e.g., bank's name, logo, slogans, etc.)
- **Insurance** – where appropriate, specify insurance coverage and require notice of changes in same
- **Indemnification**
  - Provisions requiring a party to hold the other harmless from liability in specified circumstances, usually stemming from negligence or gross negligence
  - Typically bilateral
  - Often heavily negotiated
  - Indemnification is not a magic cure-all: reputational harm, monetary limits, etc.



troutman sanders

# Oversight

- **The board should ensure that the third-party relationship furthers the strategic goals of the bank without undue business or regulatory risk**
  - While actual contract negotiation is the responsibility of management, the board should understand the terms of a proposed relationship well enough to judge whether it would further the strategic goals of the bank in a risk-appropriate and legally compliant fashion
  - On an ongoing basis, the board should receive reports of sufficient detail to allow it to determine if the relationship is continuing to further the strategic goals of the bank without undue business or regulatory risk
  - The level of board involvement will depend on the materiality of the relationship to the bank
- **Management is responsible for the ongoing oversight of the third party's performance and risk management**
  - Confirm compliance of third-party with contractual terms
  - Document and address non-performance by the third party or customer complaints related to the outsourced service
  - Keep the board regularly updated with a frequency and level of detail appropriate for the materiality of the contract
  - Update initial risk assessment and conduct "bring-down" due diligence at regular intervals, making adjustments to the relationship as necessary



troutman sanders