STARLING

info@starlingtrust.com

January 4, 2020

via email: regs.comments@occ.treas.gov
Office of the Comptroller of the Currency
Chief Counsel's Office
Attn: Comment Processing
400 7th Street, SW.
Suite 3E-218
Washington, DC 20219
Agency Name: OCC
Docket ID OCC-2020-0005

via email: regs.comments@federalreserve.gov
Board of Governors of the Federal Reserve System
Attn: Ann Misback, Secretary
20th Street and Constitution Ave, NW
Washington, DC 20551
Docket No. R-1725
RIN No. 7100-AF96

via email: regscomments@fdic.gov
Federal Deposit Insurance Corporation
Robert E. Feldman, Executive Secretary
Attn: Comments
550 17th St, NW
Washington, DC 20429
RIN 3064-AF32

via email: OGCMail@ncua.gov
National Credit Union Administration
Attn: Melane Conyers-Ausbrooks, Secretary of the Board
1775 Duke Street
Alexandria, VA 22314
Agency Name: NCUA
Docket ID NCUA-[2020-0098]

via email: 2020-NPRM-SupervisoryGuidance@cfpb.gov
Bureau of Consumer Financial Protection
Attn: Comment Intake
1700 G St, NW
Washington, DC 20552
Docket No. CFPB-2020-0033
RIN 3170-AB02

RE: Notice of Proposed Rulemaking on the *Role of Supervisory Guidance*

INTRODUCTION

Thank you for the opportunity to provide comments to the Notice of Proposed Rulemaking (NPR) regarding the Role of Supervisory Guidance. Starling (https://starlingtrust.com) is an innovative US-based RegTech startup that delivers analytics using internal bank data to improve non-financial risk ("NFR") governance, particularly with regard to risks that stem from firm culture.

Through our thought leadership and industry engagement, Starling has become recognized as an expert in our industry. Our annual white-paper, *Culture and Conduct Risk Management in the Banking Industry*[1], (aka the Starling '*Compendium*'), has become a must-read reference on the latest trends and strategies taken by bank supervisors globally to address these non-financial operational risks.

[1] https://starlingtrust.com/compendium/

Starling also offers an AI-driven technology platform that applies advances in behavioral science and network theory to the challenge of identifying and mitigating NFR in banks – proactively.

Supervisory guidance is particularly relevant in the area of NFR governance where the management of culture and conduct risk has been viewed as something that cannot be easily measured and, therefore, does not fall easily under traditional regulatory supervision. Despite this, regulators and banks alike have begun to recognize that proactive management of a firm's culture can lead to better outcomes by addressing potential misconduct issues before they lead to customer harm.

By clarifying that supervisory guidance lacks the power of regulatory enforcement, this may lead to agencies having fewer levers to intervene when firms fail to deploy their systems, processes, and people to properly embed an effective NFR management framework. Instead, management must bear responsibility for identifying and addressing the behavioral proclivities that lead to increased culture and conduct risk.

To that end, we strongly support the principle that the agencies should continue, and perhaps increase, their use of supervisory guidance in order to "provide examples of safe and sound conduct, appropriate consumer protection and risk management practices, and other actions for addressing compliance with laws or regulations." Furthermore, such guidance should focus on management tools, metrics, and frameworks that permit firms to manage NFR proactively and to address problems before they lead to customer harm.

BACKGROUND

Over the past two decades, spending on systems and processes, as well as the associated personnel, to manage NFR has exploded. Yet it is important to note that the Basel Committee on Bank Supervision ("BCBS") defines Operational Risk as the "risk of loss resulting from inadequate or failed internal processes, *people* and systems or from external events."[2] (emphasis added)

Even as investment has exploded in systems and processes for managing NFR, investment in the *people* element, namely tools for managing behavioral propensities and culture, has significantly lagged. Without this emphasis on people, interventions based on systems and processes tend to be heavily rules-based, primarily targeting visible activities and processes, and therefore risk becoming simple tick-box exercises. The motivating desire has been to manage risk through documentation, restrictive processes, and by removing people from decision-making loops.

To the extent that behavior is recognized as a source of risk, firms have implemented complex reporting systems and detailed processes to manage culture and conduct risk. Yet the success of such efforts is entirely dependent upon a complex web of interactions and critical behaviors among senior executives and risk management specialists across all "three lines" within a firm (i.e. front office, risk functions, and audit.) For instance, systems must be configured and operated effectively by well-trained analysts, identified issues must be escalated appropriately and in timely manner, and risks – even when identified and reported – must be monitored properly and may require manual follow-up.

[2] Sound Practices for the Management and Supervision of Operational Risk, BIS, February 2003

As a result, in the global aggregate, firms spend billions of dollars annually to implement and maintain NFR management frameworks, only to realize they must spend billions more to effectively *embed* appropriate behaviors into the culture of their organizations for this risk to be sufficiently mitigated.

Tools like online surveys and townhall meetings are inadequate to such complex management responsibilities. Often HR-led, such undertakings may represent 'good hygiene,' but they are not "fit for purpose" in the NFR management context, as is evidenced by continual bank misconduct scandals.

With respect to compliance with a broad range of other regulatory requirements, the "three lines of defense" model has become an accepted global implementation standard over the past two decades. In simplified form, the framework recognizes that the first line of defense (management and the business areas) has primary responsibility for managing the risks posed by their operations; the second line of defense (risk & compliance) helps in assessing and establishing frameworks and monitoring efforts; and the third line (internal audit) conducts periodic independent reviews of NFR-relevant activities and outcomes. Boards of directors, outside audit and accounting firms, and supervisory bodies are all occasionally referenced as representing additional lines of defense.

An effective approach to mitigating NFR, will incorporate all material financial and operational factors that represent a bank's risk management practices, which in turn span across the three lines of defense. Whereas financial-related and other quantitative risk controls are supported by robust metrics and models, to date, non-financial and qualitative risk factors have lacked similarly robust means of measurement. This leaves those with governance responsibilities largely reliant upon measurement methods that are subjective and imprecise. As a result, firms have difficulty knowing whether the systems and processes they have implemented are operating sufficiently well, in real-time, and levels of success are defined in the negative, only after failures have become evident.

Notably, this metrics challenge also makes it difficult for supervisors to benchmark performance on a horizontal peer-review basis, adding to the likelihood of public and political rebuke when regulatory or supervisory assessments prove inconsistent with after-the-fact realities. For firms and supervisors alike, the challenge is to move from a past reliance on *ex post* learnings and to develop credible *ex ante* options.

WHAT'S MISSING

Regulatory guidance strongly influences the decisions banks make in choosing the systems and processes they implement. Heretofore, regulators and firms have prioritized processes and systems for internal risk governance (and guarding against external threats such as those in cybersecurity) and far less inclined to try and address the people element in NFR with equal rigor.

This is understandable because, for a long time, the tools available for measuring and managing behavior have not lent themselves to such supervision. Like management, supervisors have also had to rely on HR-delivered tools such as staff surveys, townhall meetings, self-reported behavior journals, and online ethics training. These tools lack objectivity, specificity, and real-time responsiveness. And – when these measures fail – the fallback is reliance upon robust surveillance and monitoring systems that promise to detect risk events after the fact or in the making. Such instruments produce enormous 'false-positive' signals which result in added expense as risk examiners are required to run each to ground. And, when successful in identifying an actual risk management failure, awareness of such is too little / too late.

These challenges are all the more relevant given the COVID-19 pandemic. Controls and surveillance systems that were established at a time when everyone worked together have been upended by work-from-home protocols. Further, the most effective protection against misconduct risk is a culture that encourages challenge and speak-up behavior, encouraging and enabling staff to push back when risk behaviors threaten to take hold. These cultural safeguards are broadly undone in the current operating climate, along with much in the way of standard first line risk management capabilities.

During a recent interview with *Bloomberg*, Gary Cohn, past-COO of Goldman Sachs and advisor to Starling, was quoted as saying: "Banks need people to be working together in a cooperative fashion and watching and listening to each other," adding, "That is what the Fed would call a first line of defense: overhearing conversations, looking at presentations, or looking at the way you talk to a client. […] When people are sitting in their bedrooms, there is no one there to look over their shoulder."[3]

With traditional tools for managing behavior and culture proving inadequate, and given the added pressures stemming from the COVID-19 pandemic, we would urge the agencies to embrace supervisory guidance as a means to encourage innovation and investment into better tools for measuring and managing culture and conduct risk.

THE SOLUTION

Like Starling, some firms in the so-called "regtech" space (regulatory technology) are today seeking to address the NFR metrics challenge. Predictive behavioral analytics capabilities have the potential to provide *ex ante* insights into the real-time efficacy of operational risk management programs. This would permit for far more robust assurance to supervisors, investors, management and other key stakeholders**.**

Advances in machine learning have made it possible to process vast troves of internal bank data at scale. By applying novel approaches in the field of "computational social science," it is now possible to detect signals within those massive data sets that tie to particular behaviors of interest to management and supervisors. This may be behaviors that represent a predilection for misconduct or, equally, behaviors that are necessary to enable critical non-financial risk management systems and processes. And by incorporating network science, it becomes possible to determine the key influencers of such behavior.

Analyzing these signals leads to metrics that update continuously and reveal where specific behavioral propensities are likely to appear. Further, such tools can illuminate the pathways by which certain behaviors are most likely to spread – contagion-like – throughout an organization. Such 'behavioral epidemiology' positions management to operate from the front-foot. It also allows precision targeting of audit activities and risk management interventions, enabling firms and supervisors to scale their risk oversight and to act in a more timely, effective, and efficient manner.

A significant additional benefit is to be had once such technologies are established as industry-standard best practice: standardized risk metrics such as those we describe here may permit for horizontal reviews on an apples-to-apples basis, system-wide, across any given jurisdictional space. And the adoption of

[3] https://www.bloomberg.com/opinion/articles/2020-07-08/covid-19-pandemic-is-a-great-incubator-for-financial-fraud?sref=GNTXiFne

such metrics among regulators in other financial markets may permit for more efficient collaborative oversight of firms with an extensive global footprint. (e.g., the G-SIBs)

RECOMMENDATION

Advances in behavioral science and advanced data analytics enable new tools and methods for obtaining real-time assessment of management and board oversight activity, effectiveness of audit and compliance functions, and the identification and mitigation of non-financial risk – all on a proactive basis.

With new clarity provided through codifying the 2018 Statement, Starling recommends that the agencies embrace supervisory guidance as a means to encourage the adoption of these promising technologies by the firms they oversee – particularly among the more operationally complex large and regional firms – and to collaborate in the further evolution of such capabilities to enhance system-wide integrity.