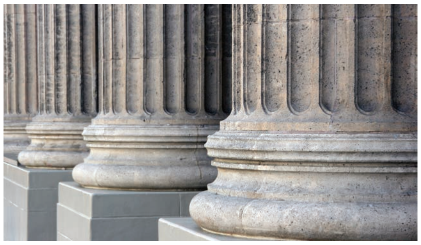
Chief Compliance Officers Beware—New York DFS Proposed Legislation Calls for Unprecedented Individual Accountability



Introduction

Seemingly fueled by historic lapses in senior management oversight and accountability, the New York State Department of Financial Services (NYDFS) has proposed new regulations, modeled on the Sarbanes-Oxley Act certification requirements. The proposed regulations are intended to further the cause of detecting and mitigating illicit financial transactions. See full press release here. Interestingly, most of the key requirements appear to be codification of previously published AML/Sanctions and model risk management guidance.[1]

Following several high profile cases, which fueled the proposed regulation and evolution of model risk management programs, most financial institutions are probably already satisfying many of the proposed requirements. So, if the new rules look a lot like the old rules, what is the point of the new legislation—and more importantly—how will it affect financial institutions?

> Each financial institution's Chief Compliance Officer will be held accountable for executing and submitting official compliance certifications to the NYDFS each year by April 15.

The key takeaway: accountability

At the core of the newly proposed anti-terrorism and anti-money laundering regulations is a requirement that senior-level Compliance Officers within regulated financial institutions certify the integrity of their AML and sanctions compliance programs. One new aspect of these requirements is an emphasis on the tracking and continued validation of data as it moves through the system. Each institution's Chief Compliance Officer (or organizational equivalent) will be held accountable for executing and submitting official compliance certifications to the NYDFS each year by April 15. Essentially, the NYDFS announcement has less to do with changing the rules than it has to do with giving the existing guidance the force of law and increasing the level of accountability aimed at specific individuals.

Heavy investing in compliance

Leaders in the financial services industry have already expressed concerns about the significant investments required to keep pace with existing compliance mandates. These same leaders' concerns extend to the growth and size of future investment required to keep pace with expanding mandates like the recently proposed regulations by the NYDFS. A compliance program may be designed with all the controls included in the proposed regulations and still fail at the operational level due to data quality. AML/Sanctions compliance programs may conform to the regulations, and may even temporarily avoid major problems, but poor data quality will eventually be exposed and compliance failures realized. Making major investments in AML/Sanctions compliance programs that don't actually perform well is a worst-case scenario that more than a few financial institutions experience.

This is a particularly worrisome scenario for Chief Compliance Officers at New York institutions because of the heightened personal accountability for failures due to poor quality data.

A tough spot for Chief Compliance Officers

While the specific penalties levied against Chief Compliance Officers (CCO) for non-compliance and other program failures may vary greatly depending on the nature and scale of the offense, heavy fines, dismissal and permanent career damage are possibilities. The situation gets more complicated when the Chief Compliance Officer needs to remediate poor data quality. The data, funding, resources and the decision to remediate poor data quality often belong to the business line. Business line executives and C-Suite leaders may not fully appreciate the impact data quality has on compliance programs or have significantly different risk appetites than the CCO. In other words, a heavy onus is being placed on individuals that may not have the means or full authority to make changes, satisfy mandates and protect themselves and their careers.

Never before have individuals, rather than whole organizations, been held so accountable for the integrity and effectiveness of AML/Sanctions compliance programs.

What makes AML/Sanctions compliance programs ineffective?

The most challenging issue compliance programs experience can be accurately described with the simple cliché, "garbage in... garbage out." Low quality gasoline inhibits engine performance. Low quality food results in low energy and unhealthy bodies. And low quality data inevitably produces ineffective AML/Sanctions compliance programs particularly in the context of strict liability Sanctions laws.

Today, all kinds of data are gathered at unprecedented speeds from many disparate locations. Whether from fraud, unintentional errors, acquisition or changing regulatory requirements over time, there are constant inconsistencies and issues that can make managing data quality a difficult task—especially as that data is being moved from point A to points B, C and D for use in various operational areas with disparate purposes.

Quality data is more critical than ever —and here's why

One key requirement in the validation section of the proposed NYDFS regulation says AML/Sanctions compliance programs must validate, pre-implementation and post-implementation, the integrity, accuracy and completeness of the data. An AML/Sanctions compliance program can do everything that's prescribed within the proposed NYDFS regulations, but ultimately, if you're starting with poor quality data, it's possible to validate that your poor quality data is being accurately and completely transferred and used within your program. Stated another way, institutions can validate the integrity, accuracy and completeness of bad data, and transfer that bad data, accurately and completely, from beginning to end. The problem is still bad data (garbage in) and your program breaks down (garbage out). The point is, many validation and certification processes don't identify and solve the underlying weakness of your program caused by poor quality data.

The Solution: Include the right tests in your validation processes and fix the data

Model validation is a set of processes and activities implemented to verify that models are achieving their intended objectives. Model validation also identifies model assumptions and limitations, malfunctions and gaps, and assesses their potential negative impact. In addition to the bevy of other validation tests, Compliance Officers should evaluate model validation plans to ensure they include:

- Thorough sensitivity and stress testing based on the design of specific watchlist filtering systems (testing a few hundred names is rarely sufficient);
- Robust data quality assessment to identify data quality weaknesses in internal data based on sensitivity/stress test results; and,
- Benchmarking watchlist filtering configurations against industry performance.

Model validation requires strong collaboration between business line data owners, technology, compliance and the model developer. In the case of third-party developed models, this may include involving the watchlist filtering vendor in the validation process. Including model developers helps ensure testing personnel have access to the knowledge necessary to design effective test plans without impairing the independence of the tests and drive effective remediation plans.

In the case of the NYDFS legislation, solutions can be applied to identify where watchlist filtering systems may not be performing correctly. More often than not, problems found in model performance can be traced directly to poor data quality that's not "fit for purpose." A truly comprehensive model validation solution will include data quality management tools that expose data weaknesses and make corrections, enhancements and updates to ensure optimum data quality suitable for the watchlist filtering, and transaction monitoring systems. Model validation and data remediation activities can be set up as automated processes and should continue on an ongoing basis in order to spot any new issues and maintain optimum data quality and compliance program effectiveness while managing costs.

Fortunately for Chief Compliance Officers, there are simple, affordable data quality management, sensitivity/stress testing and benchmarking solutions available today that simplify the discussion with and reduce the dependence on technology resources to solve the problem.

Attention Chief Compliance Officers: If you're not looking at the underlying quality of your data, and its fit for purpose (watchlist filtering, transaction monitoring, etc.), you can validate and certify a program that, because of poor data quality, isn't working properly. Data management and validation that doesn't assess data quality issues which impact watchlist filtering and transaction monitoring programs will inevitably fail to catch prohibited transactions and/or suspicious activities. This means you individually, and your organization as a whole, will be at increased risk.

About the Author

Chris Siddons is Senior Director, Regulatory and Compliance Solutions. In this role, Chris is responsible for identifying legal and regulatory developments in the financial services sector and driving the strategic direction of LexisNexis Risk Solutions compliance solutions. Prior to LexisNexis, both as a Compliance Officer and Consultant, Chris was responsible for the development, implementation, audit, validation and remediation of AML/Sanctions compliance programs and monitoring systems at financial institutions.

For more information:

Call 561.212.3671 or email
chris.siddons@lexisnexis.com

About LexisNexis Risk Solutions
LexisNexis Risk Solutions (www.lexisnexis.com/risk) is a leader in providing essential information that helps customers across all industries and government assess, predict and manage risk. Combining cutting-edge technology, unique data and advanced analytics, LexisNexis Risk Solutions provides products and services that address evolving client needs in the risk sector while upholding the highest standards of security and privacy. LexisNexis Risk Solutions is part of RELX Group plc, a world-leading provider of information solutions for professional customers across industries.

Our financial services solutions assist organizations with preventing financial crime, achieving regulatory compliance, mitigating business risk, improving operational efficiencies and enhancing profitability.

LexisNexis®
RISK SOLUTIONS

[1] *Supervisory Guidance on Model Risk Management* jointly issued by the Board of Governors of the Federal Reserve System and the Office of the Comptroller of Currency in April 2011