

The Rise of New York: Groundbreaking Laws Enhance AML, Sanctions, and Cybersecurity Program Requirements and the First Virtual Currency Dedicated License

New York's Transformation to an Outsized Financial Regulator Post-USA PATRIOT Act and Setting the Standard for AML, Sanctions, and Digital Finance

Installment Six of a Six-Part Series

October 2026

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

Welcome to New York, It's Been Waiting For You

Overview

In the aftermath of 9/11, the USA PATRIOT Act of 2001 reshaped the financial regulatory landscape, embedding Anti-Money Laundering (AML) and sanctions compliance into the very core of US financial oversight. What began as a national security imperative soon evolved into a broader framework that demanded vigilance across banks, money services businesses, and emerging financial intermediaries. Against this backdrop, New York, home to Wall Street and the world's largest international financial institutions, carved out its own identity as a regulatory powerhouse.

New York's Bold Steps to Program Standards

After the BNP Paribas AML and sanctions penalty in 2014, New York implemented a series of unique AML and sanctions compliance certification requirements. Shortly thereafter, in the early days of virtual currency, New York introduced the BitLicense in 2015, the first dedicated virtual currency license in the world. Concurrently, NY implemented cybersecurity compliance certification requirements. Initially, the certifications were targeted at traditional financial intuitions, however, a new market of virtual currency-based financial institutions emerged, and the requirements applied to a broader marketplace.

Future Trajectory

As financial services continue to digitize and threats grow more complex, New York's trajectory raises intriguing possibilities. Will its model become the blueprint for national and international regulation, harmonizing AML, sanctions, and cybersecurity across borders? Or will the rise of decentralized finance and global competition challenge New York's dominance?

> *"Financial institutions doing business in New York must do everything they can to help stem the tide of illegal financial transactions that fund terrorist activity. It is time to close the compliance gaps in our financial regulatory framework to shut down money laundering operations and eliminate potential channels that can be exploited by global terrorist networks and other criminal enterprises."*
>
> *- Maria T. Vullo, NY Financial Services Superintendent Director of FinCEN (June 30, 2016), DFS issues Final Anti-Terrorism Transaction Monitoring and Filtering Program Regulation (Part 504)*

The Starting Point

On October 3, 2011, the New York State Department of Financial Services (NYS DFS) was officially established, consolidating the state's banking and insurance oversight into a single, powerful regulator. This marked the beginning of New York's transformation from a financial hub into an even stronger regulatory powerhouse, uniquely positioned to oversee Wall Street and the nation's largest financial institutions. But long before the establishment of NYS DFS, the 9/11 attacks reshaped the financial regulatory landscape with the birth of the USA PATRIOT Act.

USA PATRIOT Act

The terrorist attacks of September 11, 2001 exposed vulnerabilities in the US financial system which led to the USA PATRIOT Act.

Compliance shifted from a simple function into a national security mandate, embedding AML and sanctions screening into US financial system and downstream into foreign markets doing business with US financial institutions.

NYS DFS Established

The State of New York consolidated its banking and insurance departments which then created a single regulator with jurisdiction over Wall Street and the nation's largest financial epicenter.

NYS DFS became the architect of New York's regulatory identity which uniquely positioned AML, sanctions, and cybersecurity frameworks at state-level.

BNP Paribas Case

In June 2014, BNP Paribas pled guilty in New York to sanctions violations and paid a record of $8.9B for concealing transactions tied to Sudan, Iran, and Cuba.

The case positioned New York as a significant regulator due to its standing with many foreign banks holding NY banking licenses. The enforcement kicks off a series of AML-based enforcement of compliance failures for domestic and international banks with NY banking licenses.



New York and Building the Foundation of Enforcement

Between 2015 and 2017, NY's regulatory landscape evolved that reshaped its financial oversight. These foundational years signaled that New York was not simply filling gaps left by federal enforcement. Rather, NY tacked onto the Bank Secrecy Act (BSA) AML compliance requirements with an annual compliance certification, created a new regulatory regime on virtual currency state-based licensing, and, separately, followed on AML certification with annual cybersecurity program compliance certifications.

BitLicense

New York introduced the Virtual Currency Business Activity License or BitLicense, the first framework for crypto firms, requiring AML/KYC, cybersecurity, consumer protection, and capital standards.

This positioned New York as a global pioneer, and proved innovation must operate under regulated accountability, which set the tone for future state-level leadership in fintech governance.

Part 504

Requires *regulated institutions with transaction monitoring and sanctions screening programs, which included certification annually, and embedded accountability directly into executive governance.

Part 504 elevated AML and sanctions programs from procedural to strategic risk management pillars and strengthened rigorous oversight at state-level.

Part 500

One of the most comprehensive cybersecurity frameworks in the US. Part 500 mandated risk-based cybersecurity programs, designated CISOs, multi-factor authentication, encryption, vendor oversight, and breach reporting within 72 hours, and annual certification requirements.

NY rolled up guidance from Federal Financial Institutions Examination Council (FFIEC) and National Institute of Standards and Technology (NIST) into a programmatic requirement.



*Under 23 NYCRR § 504.2, "Regulated Entities" include: (b) Bank Regulated Institutions : banks, trust companies, private bankers, savings banks, savings and loan associations chartered under the New York Banking Law, and branches or agencies of foreign banking corporations licensed to operate in New York; and (d) Nonbank Regulated Institutions: check cashers and money transmitters licensed under the Banking Law. Pursuant to § 504.2(e), "Regulated Entities" means all Bank Regulated Institutions and all Nonbank Regulated Institutions.

New York and Expanding Scope of AML Oversight

Continuing 2017, New Y was not only pioneering virtual currency regulation and cybersecurity standards, it also expanded the AML framework to cover MSBs and check cashers. Through 23 NYCRR Parts 416 and 417, New York embedded AML obligations at two critical stages: Part 416 at the entry point and Part 417 at the operational level. These two rules reinforce New York's identity as a regulator that demanded bank-level scrutiny across all financial institutions.

Part 416

Part 416 is treated as entry-level AML readiness that requires applicants for new licenses, branches, or acquisitions in the MSB and check-cashing sectors to demonstrate AML program readiness consistent with federal laws.

This meant showing clear policies for customer identification, suspicious activity reporting, and recordkeeping, as well as designating compliance officers.

Part 417

Part 417 is the ongoing governance cycle. This applies to existing licensees, requiring them to maintain and continuously update AML programs aligned with federal standards and OFAC sanctions obligations.

Institutions had to implement policies, procedures, internal controls, training programs, and designate compliance officers to oversee effectiveness. This made compliance continuous obligation rather than one-time certification.



From Federal Baselines to New York Mandates

The establishment of US financial compliance starts with the BSA and OFAC Sanctions Programs, which required "effective" AML and sanctions frameworks but left broad discretion in design and oversight. NYS DFS pinpointed critical gaps such as weak monitoring systems exposed in enforcement cases and escalating cyberattacks against financial institutions. In response, NYS DFS issued Parts 500 and 504 to establish cybersecurity standards and board-level accountability, and mandate documented transaction monitoring with annual executive certifications.

High and Mighty New York

Recognizing that below baselines were insufficient for modern and evolving risk, NYS DFS introduced landmark rules that reshaped compliance.

Part 500. Cybersecurity guardrails for covered entities to implement multifactor authentication, breach reporting, and annual certifications for executive leadership.

Part 504. Requirements such as transaction monitoring and sanctions screening programs, as well as annual certifications signed by CEOs and boards, highlighting executive liability.

OFAC Sanctions Rules

Mandates blocking and reporting of transactions tied to sanctioned individuals, entities, or countries, enforced through list-based screening.

Compliance Highlights:

1. Block prohibited transactions.
2. Report blocked property and rejected transactions to OFAC.
3. Maintain records of compliance.
4. Implement sanctions screening programs across all customer transactions.

Bank Secrecy Act

Requires covered financial institutions to maintain effective programs at institutional level. Responsibility is rested with the institution and not its executives.

Federal Baseline:

1. Effective AML programs;
2. Current Transaction Reporting for transactions over $10,000;
3. Suspicious Activity Reporting related to financial crimes; and
4. Retain transaction records and customer identification.

New York State of Mind: Oversized Global Regulatory Presence

New York's regulatory reach extends far beyond its borders. Being the epicenter of US and global finance, any institution holding a New York banking license or operating a New York branch is subject to NYS DFS oversight. This jurisdictional hook has allowed New York to impose record fines on foreign banks for AML and OFAC violations: The following identify New York's position:



Global Reach

Foreign banks with NY branches are fined for AML/OFAC violations, even if misconduct occurred abroad.

Bespoke Authority

No other state has such outward enforcement power, rooted in New York's position as the global financial center.

Cultural Continuum

Enforcement against foreign banks reinforced New York's identity as the epicenter of financial oversight.

Elevated Accountability of NYSDFS

The NYS DFS's regulatory standards transform passive, corporate compliance into mandatory, personal executive liability. The BSA requires institutions to maintain "effective" programs but needs aggressive personal operational mandates for executive leadership.



Part 504 (Transaction Monitoring)

The NYS DFS's regulatory framework demands a comprehensive documented back-testing, data lineage verification, and mandatory system validation.

Dual Signature Mandate

Requires explicit annual certifications signed personally by the CEO and/or Board of Directors, attesting to material compliance of financial institution.





Executive Liability

Knowingly or recklessly filing a false or immature annual certification exposes individual corporate officers to civil and criminal liability.

The Compliance Hurdle in IPOs

Over the past two (2) decades, enforcement actions in New York have consistently reshaped the expectations placed on New York regulated financial institutions. “Serious deficiencies” warnings in AML and sanctions programs brought sharper scrutiny to risk management practices as companies aim seek public listings through an initial public offering (IPO). Post-IPO, New York has delivered a sharper message: When companies grow fast, especially on the road to an IPO, their risk profile grows even faster and failing to scale compliance alongside such growth is a compliance and governance failure.

Hyper-Growth Problems

When companies grow too fast, their risk profile can shift dramatically. Old manual systems can’t keep up, and regulators see that as an immediate red flag.



Governance Failure

Regulators now treat the failure to match user growth with strong, automated controls as a basic failure of leadership and corporate responsibility.



Embedding Compliance

Recent enforcement actions have shown that regulators penalize firms that do not invest in compliance infrastructure during rapid onboarding surges. Waiting until after the IPO to fix compliance issues leads to expensive settlements, outside monitors, huge backlogs, and a loss of investor confidence right when the market spotlight is brightest.



Today, enforcement language emphasizes the necessity of scaling controls in tandem with business expansion, embedding governance and a culture of compliance as non-negotiable components. This progression illustrates how enforcement has moved from identifying gaps to demanding structural accountability, setting the tone for how regulated financial institutions must prepare for an IPO.

From Hurdles to Stringent Governance Accountability

As covered entities transition from hyper-growth to IPO, compliance shifts from an internal challenge to regulatory scrutiny. Enforcement actions by NYS DFS not only shape operational risk but also appear in mandatory Securities and Exchange Commission (SEC) filings as material disclosures. Between 2021 and 2023, corporate filings evolved from treating NYS DFS as a licensing risk, to recognizing it as a governance benchmark and supervisory authority.

Evolving Disclosures To Adapt to NYS DFS Governance

2021

NYS DFS is referenced as a licensing and oversight risk, with language stressing "extensive regulatory requirements" and possibilities of penalties and restrictions. Compliance theme is defensive, treating NYS DFS as a risk factor to be managed.

2022

Disclosures expanded to note being "subject to examinations and supervisory reviews" with enforcement actions described as material to operations and reputation. Language recognized NYS DFS as an impactful regulatory authority to covered entities.

2023

NYS DFS is considered in disclosures as governance benchmark, with language around "ongoing regulatory inquiries," "remediation mandates," and "investor-relevant risk." The compliance culture highlights NYS DFS oversight into board-level obligation and governance-anchored framework.

Since then, this stringent state oversight reflects a mature compliance culture and show how New York's regulatory posture and corporate obligations have converged.

On September 10, 2026, NYS DFS published an industry letter on cyber risk assessments that reinforces Part 500's risk-based governance framework and emphasizes on the below:

Risk Assessments as Core of Part 500
NYSDFS stressed that risk assessments are not optional checklists but mandatory framework of cybersecurity program.

Annual Review and Event-Driven Updates
Risk assessments are reviewed annually and when material changes occur such as migrations, acquisitions, adoption of AI, or third-party involvement or dependencies.

Governance Emphasis
The newsletter highlights recurring weaknesses such as outdated asset inventories, inconsistent methodologies, failure to identify or foresee emerging risks, and governance gaps.

Threat Landscape in New York's Eyes

New York has redefined the compliance narrative by shifting from identifying programmatic "deficiencies" to treating lapses as governance failures. Early enforcement built the foundation with Parts 500 and 504, targeting weak monitoring systems and rising cyberattacks. Over the years, the language of enforcement has sharpened. Regulators frame compliance breakdowns as leadership failures, penalize firms for inadequate cyber resilience, and demand board-level accountability. Likewise, enforcements are recognized in regulatory disclosures, treating NYS DFS as one of the most consequential state regulators and penalties are described as significant operational and reputational risks. For regulated financial institutions, NYS DFS is seen as an authority at a governance level, not just a compliance reviewer.

NYS DFS's Point of View to Threats

Structural Accountability over Procedural Compliance. NYS DFS' posture shifted from identifying "deficiencies" to treating breakdowns as failures of leadership. Annual certifications anchor modern enforcement themes.

Elevating Cyber and Operational Threats. Ransomware, third-party breaches, MFA vulnerabilities, and incident-response failures now dominate enforcement. Part 500 amendments include real-time detection, universal MFA, and board-level oversight.

Rapid Growth Risk = System Threat. NYS DFS increasingly penalizes firms whose onboarding surges outpace compliance infrastructure. Scaling without controls is treated as a structural risk to the financial system.

How Companies See NYSDFS

High-Impact Regulatory Authority Public companies identify NYS DFS as one of the strictest state regulators with supervisory actions capable of affecting operations and financial conditions.

Licensing Obligation and Operational Dependency. Covered entities acknowledge NYS DFS licensing as vital to their business model, and noncompliance could jeopardize market access, putting the company at risk.

Examination and Enforcement Exposure. NYS DFS bespoke oversight can lead to remediation mandates, operational restrictions, and penalties that paves NYS DFS role as core compliance risk.

The Cybersecurity Shield: Absolute Zero-Tolerance

New York's regulatory evolution did not halt at financial oversight. Rather, it extended into the digital core of financial operations. With 23 NYCRR Part 500, the NYS DFS established the nation's first comprehensive cybersecurity regulation, transforming data protection from a best practice into a legal mandate. The Second Amendment to Part 500 further elevated this framework, closing gaps that federal guidance like the FFIEC IT Manual left open.



Area	Federal Baseline	2023 Changes
Governance	Institutional in nature	Board-level accountability; CISO reporting and responsibility
Incident Reporting	Suspicious Activity Reporting and sanctions violations	72-hour breach reporting; ransomware and extortion reporting
Multi factor authentication (MFA)	Not mandated federally	Universal MFA; phishing-resistant methods
Certifications	No executive sign-off	Annual certifications signed by CEO or board of directors
Large institutions	No distinction	"Class A" companies with strengthened obligations

This model positions New York as the benchmark for cybersecurity governance worldwide. Where other frameworks gives flexibility, NYS DFS demands proof such as annual certifications, board-level involvement to accountability, and demonstrable protection against any credentials compromise.

New York's Way of Doing Business

The rise of New York's regulatory presence pose stricter requirements to financial institutions operating in or through the state. The heightened obligations, while burdensome, offer areas of opportunity. Financial institutions that embrace the standards gain reputational credibility, access to New York's financial markets and significant customer population, and a competitive edge in jurisdictions adopting similar rules.

The same regulatory presence reshaped the global compliance landscape. New York's cybersecurity rules became a model for other states and countries. The BitLicense sparked international debate and inspired regulatory frameworks abroad. Sanctions enforcement demonstrated that state-level regulators could impose penalties rivaling federal actions. For financial institutions, this meant that operating in New York was not just about meeting local requirements but also falling into alignment with a global standard of statutory framework and oversight.

25 years after the USA PATRIOT Act, New York has established a significant presence in AML, sanctions, and cybersecurity requirements of regulated financial institutions operating in New York that compliment, supplement, or go beyond federal requirements.





LAUNCH | SCALE | OPTIMIZE

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com