NY Banking Brief: All The Notable Legal Updates In Q4

By **Chris Bonner** (January 14, 2026)

*In this **Expert Analysis series**, attorneys provide quarterly recaps discussing the biggest developments in New York banking regulation and policymaking.*

Chris Bonner

The fourth quarter of 2025 contained several items of interest to New York financial institutions. One item expressly affects financial service regulation, and two statutes signed into law during the fourth quarter directly affect the financial services business.

Cybersecurity at Third-Party Service Providers

The only definite development during the fourth quarter is the cybersecurity industry guidance published by the New York State Department of Financial Services on Oct. 21.[1] The guidance accentuates the need for financial institutions to oversee cybersecurity at their third-party vendors.

The guidance states that it contains no new requirements. However, it does recommend industry best practices and is intended to clarify regulatory requirements,[2] including the NYDFS' Cybersecurity Regulation at Title 23 of the New York Code of Rules and Regulations, Part 500.

The guidance points out that banks, insurance companies and other entities required to be licensed by the NYDFS rely on third-party service providers for cloud computing, file transfer systems, artificial intelligence and the like.[3] The NYDFS states that, in general, covered entities need to improve the cybersecurity risk at their service providers.[4]

Much of the guidance addresses points previously covered in Part 500, with which covered entities should already be familiar. New in the guidance are lists of recommended criteria for selecting service providers and provisions to include in a contract with a service provider.[5]

While emphasizing that each covered entity's risk plan should be tailored for each service provider,[6] the guidance provides a "non-exhaustive list of considerations that Covered

Entities should assess when performing due diligence on [service providers]."[7]

A particularly thorny item on the list is "[w]hether the [service provider], its affiliates, or vendors are located, or operate from, a country or territory jurisdictions that is considered high-risk based on geopolitical, legal, socio-economic, operational or other regulatory risks."[8]

Because so many service providers operate with employees and contractors who might be anywhere in the world, the covered entity's due diligence might not find fully satisfactory results. However, the guidance recognizes that a service provider may have to deal with limited vendor options.[9]

Attention to the location of where service providers store data is accentuated in the section of the guidance about contracting,[10] where the NYDFS recommends incorporating into a service provider contract "[r]equirements for the [service provider] to disclose where data may be stored, processed, or accessed; obtain prior written approval for cross-border transfers (or full prohibitions of this practice); and comply with applicable data residency or localization laws."[11]

This recommendation could interfere with data storage in the cloud, since cloud storage can be located in data centers anywhere in the world.

Among the NYDFS' recommended provisions are:

- Immediate or timely notice by the service provider when a cybersecurity event directly affects the covered entity's information system or nonpublic information;
- Disclosure of the service provider's use of subcontractors that may have access to the covered entity's information system or nonpublic information, with the right of the covered entity to reject the use of one or more subcontractors; and
- Whether the covered entity's data may be used to train artificial intelligence.[12]

Several additional recommended contract provisions are listed in the contracting section.[13]

The NYDFS stops just short of mandating these provisions, but says that covered entities should consider them.[14] The guidance states that the list is not exhaustive, because the

terms might not be viable or appropriate in all situations.[15]

On the other hand, the guidance refers on occasion to contract provisions that the service provider contract should include, such as "remedies in the event the Covered Entity reasonably determines that the service provider has breached any material terms of the agreement related to cybersecurity."[16]

The guidance further notes that additional contractual terms should be evaluated, "based on the nature of the engagement, market conditions, and the sensitivity of data."[17]

Because the recommendations in the guidance are not exhaustive, in practice the recommendations may become, over time, part of the core of a covered entity's process of engaging a service provider, with essential additions to that process based upon the specific facts and circumstances of the contracting parties.

Some common service providers are large nationwide entities, which have bargaining power that is greater than, or at least equal to, many New York state-chartered banks and other covered entities.

It is not immediately apparent how covered entities will be able, in their contracts with these larger service providers, to include one or more provisions that are recommended — in some cases arguably mandated — by the NYDFS. The guidance can be expected to assist covered entities toward including the recommended provisions.

Multifactor Authentication and Inventory of Information Systems

On Nov. 1, two small but important amendments of the NYDFS' Cybersecurity Regulations, originally adopted on Oct. 16, 2023,[18] went into effect.[19]

One amendment, at Section 500.12 of the regulations, states that a covered entity,[20] with certain limited exceptions, must require multifactor authentication for any individual to access the institution's information systems.[21]

If the institution has a chief information security officer, which means "a qualified individual responsible for overseeing and implementing a covered entity's cybersecurity program and enforcing its cybersecurity policy,"[22] then the CISO may give written approval to reasonably equivalent or more secure compensating controls that shall be reviewed periodically, but at a minimum annually.[23]

The other amendment that became effective on Nov. 1, at Section 500.13 of the NYDFS regulations, specifies two additional housekeeping requirements at a covered entity's cybersecurity program.

The cybersecurity program shall have written policies and procedures to make an inventory of each asset in the covered entity's information systems, and to keep the asset inventory updated and validated frequently.[24] Section 500.13(a)(1) lists some of the items of key information to be tracked for each asset.

Although the term "asset" is not defined in the NYDFS regulations, a covered institution should include in its asset inventory those contracts with third-party vendors which pertain to cybersecurity.

The second housekeeping requirement is for the cybersecurity policies and procedures toprovide for the secure disposal on a periodic basis of nonpublic information that becomes unnecessary.[25]

Cash Acceptance Law

On March 21, New York state's cash acceptance law will require practically every retail store in the state of New York to have some kind of bank account or other cash management system.[26]

If a retail store does not accept cash, but requires payment by credit card, debit card or other electronic means, customers without access to an electronic payment system will not be able to make purchases at that store.

New York state, following an ordinance adopted by New York City, enacted a law applicable to every food store and retail establishment, as defined in the statute, stating that "[i]t shall be unlawful for a food store or a retail establishment to refuse to accept payment in cash from consumers."[27] However, a food store or retail establishment may:

- Refuse payment in bills denominated above $20; and
- Refuse any cash payment for telephone, mail or internet-based transaction, unless the payment takes place on the premises of the food store or retail establishment.[28]

Further, no food store or retail establishment is allowed to charge a higher price for the same item in the case of a cash, rather than a cashless, transaction.[29]

However, a food store or retail establishment may have a so-called reverse ATM that turns cash, at a minimum of $1, into a prepaid card that allows the customer to pay for the transaction. The reverse ATM cannot charge a fee, and the prepaid card must not have an expiration date or have a limit on the number of transactions that may be charged on it.[30]

At present, almost all retail stores in New York state allow for payment in cash. Commencing March 21, those stores that do not will need to have some kind of agreement with a financial intermediary that will permit a customer to pay with cash.

Uniform Commercial Code Article 12

Effective June 3, New York will join the majority of states in the U.S. that have adopted Uniform Commercial Code Article 12.

How does one take a security interest in cryptocurrency?

Cryptocurrencies and nonfungible tokens are **general intangibles** under the Uniform Commercial Code. New Article 12 defines a controllable electronic record, or CER, as:

a record stored in an electronic medium that can be subjected to control under Section 12-105. The term does not include a controllable account, a controllable payment intangible, a deposit account, an electronic copy of a record evidencing chattel paper, an electronic document of title, electronic money, investment property, or a transferable record.[31]

A security interest in a CER may be taken by possession, defined in Section 12-105(a) as:

(a) General rule: control of controllable electronic record. A person has control of a controllable electronic record if the electronic record, a record attached to or logically associated with the electronic record, or a system in which the electronic record is recorded:

(1) gives the person:

(A) power to avail itself of substantially all the benefit from the electronic record; and

(B) exclusive power, subject to subsection (b), to:

(i) prevent others from availing themselves of substantially all the benefit from the electronic record; and

(ii) transfer control of the electronic record to another person or cause another person to obtain control of another controllable electronic record as a result of the transfer of the electronic record; and

(2) enables the person readily to identify itself in any way, including by name, identifying number, cryptographic key, office, or account number, as having the powers specified in paragraph (1).[32]

Control of a CER under Section 12-105 is in effect a kind of possession. Section 12-104(h) provides that "[f]iling of a financing statement under Article 9 is not notice of a claim of a property right in a controllable electronic record,"[33] and as a result taking control of a CER under a security agreement would take priority over a financing statement filed under Uniform Commercial Code Article 9.

For transactions involving security interests taken before the effective date of Article 12 on June 3, one should be careful to check what effect, if any, the transitional rules of Uniform Commercial Code Article 12-A may have.

Conclusion

Compliance departments at New York state financial institutions will need to attend to the cybersecurity guidance because the guidance lists several planning and contracting recommendations that the NYDFS thinks regulated financial institutions should follow.

Financial institutions with small business customers might find the cash acceptance law relevant to their operations. Any financial institution that takes cryptocurrency as collateral should take control under Uniform Commercial Code Article 12 in order to perfect its security interest.

Chris Bonner is special counsel at Barclay Damon LLP.

[1] https://www.dfs.ny.gov/industry-guidance/industry-letters/il20251021-guidance-managing-risks-third-party ("Guidance") (accessed December 16, 2025).

[2] Guidance at ¶4.

[3] Guidance at ¶2.

[4] Guidance at ¶3.

[5] See, e.g., Guidance at ¶¶7 and 10.

[6] Guidance at ¶¶6 and 7.

[7] Guidance at ¶7.

[8] Id.

[9] Guidance at ¶9.

[10] Guidance at ¶¶10-12.

[11] Guidance at ¶10.

[12] Guidance at ¶¶10-11.

[13] Guidance at ¶¶10-12, including footnotes [21], [24], [26] and [27].

[14] Guidance at ¶10.

[15] Guidance at ¶12.

[16] Guidance at ¶11.

[17] Guidance at ¶12.

[18] https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf (accessed January 2, 2026).

[19] See Cybersecurity Implementation Timeline for Covered Entities, at https://www.dfs.ny.gov/system/files/documents/2023/11/cybersecurity_implementation_timeline_covered_entities.pdf (accessed January 2, 2026).

[20] Defined as "any person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law, regardless of whether the covered entity is also regulated by other government agencies." 22 NYCRR § 500.1(e).

[21] 22 NYCRR § 500.12(a).

[22] 22 NYCRR § 500.1(c).

[23] 22 NYCRR § 500.12(b).

[24] 22 NYCRR § 500.13(a).

[25] 22 NYCRR § 500.13(b).

[26] General Business Law, §396-ii.

[27] General Business Law, §396-ii.b.

[28] Id.

[29] General Business Law, § 396-ii.b.

[30] General Business Law, § 396-ii.e.(i).

[31] New York Uniform Commercial Code, § 12-102(a)(1).

[32] New York Uniform Commercial Code, § 12-105(a).

[33] New York Uniform Commercial Code, § 12-104(h).