BRIDGHAM TECHNOLOGY INSTITUTE
BTI WORKING PAPER 325-26

Access Controls and Cybersecurity Enforcement: Evidence From New York Part 500 Consent Orders, 2021 to 2026

Bridgham Technology Institute

This work is made available under the rights statement In Copyright - Educational Use Permitted
https://rightsstatements.org/page/InC-EDU/1.0/
Raleigh, NC: Bridgham Technology Institute, November 2026.

Electronic copy available at: https://bridghaminstitute.com/research/working-papers/325-26

Access Controls and Cybersecurity Enforcement: Evidence From New York Part 500 Consent Orders, 2021 to 2026

Bridgham Technology Institute*

November 2026

Abstract: Each firm covered by the New York Cybersecurity Regulation, 23 NYCRR Part 500, files an annual statement on its compliance, signed by its highest-ranking executive and its chief information security officer. We examine which requirements the New York State Department of Financial Services (NYDFS) has cited when it penalized a firm under the regulation, using all 31 consent orders with a Part 500 finding from March 2021 to November 2026. The orders carry $153,225,000 in penalties. Seventeen orders (54.8%) find a violation of section 500.12, which covers multi-factor authentication (MFA) and, in its earlier form, access controls that may include MFA; nine orders (29.0%) name MFA itself. The 17 orders account for $43,575,000 (66.8%) of the $65,225,000 in penalties under the 28 orders whose findings concern cybersecurity alone. The annual certification is cited in 12 orders (38.7%), risk assessment in 10 (32.3%) and late notice to NYDFS in 10 (32.3%). A cybersecurity event preceded 27 orders (87.1%), including all 17 that cite section 500.12. The share of orders citing section 500.12 rose from 41.2% in 2021 to 2024 to 71.4% in 2025 and 2026. These results suggest that access controls are the part of a cybersecurity program most exposed to enforcement after an event.

Keywords: 23 NYCRR Part 500, New York State Department of Financial Services, multi-factor authentication, consent orders, cybersecurity enforcement, annual certification, insurance regulation
JEL codes: G28, G22, K23

* Bridgham Technology Institute is a division of Bridgham Cyber, LLC, Raleigh, NC. Contact: headofresearch@bridghamcyber.com.

1. Introduction

Each year, by April 15, a firm covered by New York's Cybersecurity Regulation, 23 NYCRR Part 500, must tell its regulator whether it complied with the regulation in the prior calendar year.[1] The filing is either a certification of material compliance or an acknowledgment of noncompliance, and it is signed by the firm's highest-ranking executive and its chief information security officer (CISO).[1] The regulator, the New York State Department of Financial Services (NYDFS), has penalized insurers, insurance agencies, mortgage lenders and servicers, money transmitters and virtual currency firms under the regulation since 2021.[2–23]

The executive who signs that filing faces a practical question: when NYDFS has penalized a firm under Part 500, which requirements did it cite? The record that answers the question is public. NYDFS publishes its consent orders, and each order lists its findings section by section.

In this paper, we examine all 31 consent orders from March 2021 to November 2026 in which NYDFS found a violation of Part 500. For each order we record the penalty and whether the order cites four requirements: multi-factor authentication (MFA) and access controls under section 500.12, risk assessment, notice to NYDFS within 72 hours of a cybersecurity event, and the annual certification.

We document three main findings. First, section 500.12 is the requirement cited most often. Seventeen of the 31 orders (54.8%) find a violation of it, and those orders carry $43,575,000 of the $65,225,000 (66.8%) in penalties under the 28 orders whose findings concern cybersecurity alone. Second, enforcement follows events. A breach, phishing compromise or other cybersecurity event preceded 27 of the 31 orders (87.1%) and all 17 that cite section 500.12. Third, the pattern has strengthened over time. The share of orders citing section 500.12 rose from 7 of 17 (41.2%) in 2021 to 2024 to 10 of 14 (71.4%) in 2025 and 2026.

These findings are counts of negotiated enforcement findings, not rates of control failure among covered firms. Almost every order followed a reported event, so the orders show what NYDFS cites after an event. The headline share also depends on how section 500.12 is read. Nine of the 17 orders name MFA itself; the other eight rest on an earlier form of the section, which required effective access controls that "may include" MFA.[20] We report both counts throughout.

The question is timely. Since November 1, 2025, Part 500 has required MFA for any individual who accesses a covered entity's information systems, with limited exceptions.[1,24] The submission due April 15, 2027 is the first to cover a full calendar year under that wider requirement.

The paper proceeds as follows. Section 2 describes the regulation and the four requirements we track. Section 3 describes the consent orders and how the list was built. Section 4 defines the measures and states the assumptions behind them. Section 5 presents the results. Section 6 discusses what the results mean for a covered firm. Section 7 states the limitations, and Section 8 concludes.

2. The Regulation

Part 500 sets cybersecurity requirements for the firms it defines as covered entities. Its second amendment took effect on November 1, 2023, with later compliance dates for some sections.[1] Four requirements matter for this paper.

Section 500.12 governs authentication. Before the second amendment, section 500.12(a) required "effective controls, which may include Multi-Factor Authentication or Risk-Based Authentication," and section 500.12(b) required MFA for access to internal networks from an external network.[20,23] Since November 1, 2025, the section requires MFA for any individual who accesses the covered entity's information systems.[1,24] At least 27 of the 31 orders, those announced before that date, concern conduct under the earlier text.

Section 500.9 requires a covered entity to conduct periodic risk assessments of its information systems.[11] Section 500.17(a) requires notice to NYDFS within 72 hours of a cybersecurity event.[2] Section 500.17(b) requires the annual submission. Since the second amendment, a covered entity that did not materially comply may file an acknowledgment of noncompliance in place of a certification, naming the sections, the nature and extent of the noncompliance, and a remediation timeline or confirmation that remediation is complete.[1]

3. Data

Our data are the NYDFS press releases and consent orders for each action, read on dfs.ny.gov.[2–23] We built the list of actions from three NYDFS sources: the cybersecurity enforcement listing on the NYDFS site, the NYDFS newsroom, and the annual reports of the NYDFS Consumer Protection and Financial Enforcement Division for 2021 to 2025.[25] The cybersecurity listing proved incomplete (it leaves out the two November 2024 orders), so we opened and checked every action named in the annual reports or the newsroom. Actions for 2026 rest on the newsroom alone, because no 2026 annual report was available.

We include an action when NYDFS entered a consent order that finds a violation of Part 500, alone or alongside other regulations. Four kinds of matter were found and left out: settlements by the New York Attorney General without an NYDFS order; NYDFS orders that mention Part 500 only in background; NYDFS orders under other laws, such as motor vehicle reporting; and one multistate settlement for which no NYDFS consent order was found.[25] Thirty-one orders remain. Two of them each name two related companies, and each is counted once.

Each order was read twice, by separate readers, against seven facts: the date, the penalty, the sector, whether the order cites each of the four requirements, and whether a cybersecurity event preceded it. Every entry in Appendix B was confirmed on the second reading. We use no client data, survey or proprietary dataset, and every number in Section 5 can be rebuilt from Appendix B.

4. Measures and Assumptions

4.1. The Measures

Our main measure is the share of orders that cite section 500.12, M:

M = (orders citing section 500.12) / (all Part 500 consent orders)

We report three companion measures. The penalty share, D, is the total penalty in orders that cite section 500.12 divided by the total penalty in all orders whose findings concern cybersecurity alone. The core-control share, C, is the share of orders that cite at least one of section 500.12, risk assessment (section 500.9) or late notice (section 500.17(a)). We give the same counts for the annual certification (section 500.17(b)) and for a prior cybersecurity event.

Every order has the same weight in M and C, whatever its size. D weights each order by its penalty. Penalties range from $150,000 to $5,000,000 among the 28 orders whose findings concern cybersecurity alone, with a median of $2,000,000, so no single order carries more than 7.7% of the total in D. Three orders combine Part 500 with anti-money-laundering and other findings. They carry $88,000,000 between them and state no Part 500 share. We count them in M and C and leave them out of D. Appendix A gives D with them included.

4.2. Assumptions

The measures rest on six assumptions. First, the penalty is the civil money penalty payable to NYDFS under the order. We leave out amounts paid to the New York Attorney General in a joint matter ($4,750,000 from GEICO and $350,000 from Travelers) and a separate compliance spending commitment of $50,000,000 in the Coinbase order.[10,17]

Second, an order cites a section when a numbered paragraph of the order finds a violation of that section. A section named only in an order's opening recitals is not counted. One order, Residential Mortgage Services (2021), finds a missed 72-hour notice and a missing risk assessment without a numbered finding of violation; the press release states a violation of section 500.17, and the order ties the risk assessment finding to section 500.09(a) in a footnote.[2] We count it for risk assessment and late notice, and Appendix A gives the measures with it counted for neither.

Third, an order cites section 500.12 when it finds a violation under any subsection. Nine orders find a violation of the MFA requirement itself. Eight find a violation of the earlier section 500.12(a). Both groups are counted in M, and Appendix A gives the nine alone. One order, Hartford Fire Insurance (2025), describes missing MFA and charges it under section 500.7 (access privileges). We do not count it in M, and Appendix A shows the effect of counting it.

Fourth, each order is assigned to the sector NYDFS names for the entity: insurance licensee (insurers, agencies and licensed producers), mortgage or consumer lending, virtual currency, or

money transmission. Fifth, a cybersecurity event preceded an order when the order describes a breach, phishing compromise, ransomware attack or unauthorized access before the action. One order (Genesis Global Trading, 2024) describes an internal audit finding that privileged access had been given to unauthorized individuals, which we do not count as an event. Sixth, an order is dated by its press release. Five orders had no press release that we could find and are dated by the order.

5. Results

5.1. Requirements Cited

Table 1 reports how often each requirement is cited. Section 500.12 appears in 17 of the 31 orders (M = 54.8%). The annual certification follows at 12 orders, with risk assessment and late notice at 10 each. Twenty-six orders cite at least one of section 500.12, risk assessment or late notice (C = 83.9%).

Requirement cited	Orders (of 31)	Share of orders	Orders (of 28)	Penalties ($)	Share of penalties
Section 500.12 (MFA and access controls)	17	54.8%	17	43,575,000	66.8%
Annual certification (500.17(b))	12	38.7%	10	29,300,000	44.9%
Risk assessment (500.9)	10	32.3%	9	22,500,000	34.5%
Late notice to NYDFS (500.17(a))	10	32.3%	9	22,125,000	33.9%
At least one of 500.12, risk assessment, late notice	26	83.9%	24	56,825,000	87.1%
A cybersecurity event preceded the order	27	87.1%	26	63,025,000	96.6%
All orders	31	100.0%	28	65,225,000	100.0%

Table 1: Requirements Cited in NYDFS Part 500 Consent Orders, March 2021 to November 2026. Penalties are those under the 28 orders whose findings concern cybersecurity alone (total $65,225,000).

The penalty figures point the same way. Of the $65,225,000 in penalties under the 28 orders whose findings concern cybersecurity alone, the 17 orders that cite section 500.12 account for $43,575,000 (D = 66.8%). Figure 1 shows each share, with the nine orders that name MFA itself marked within the first bar.

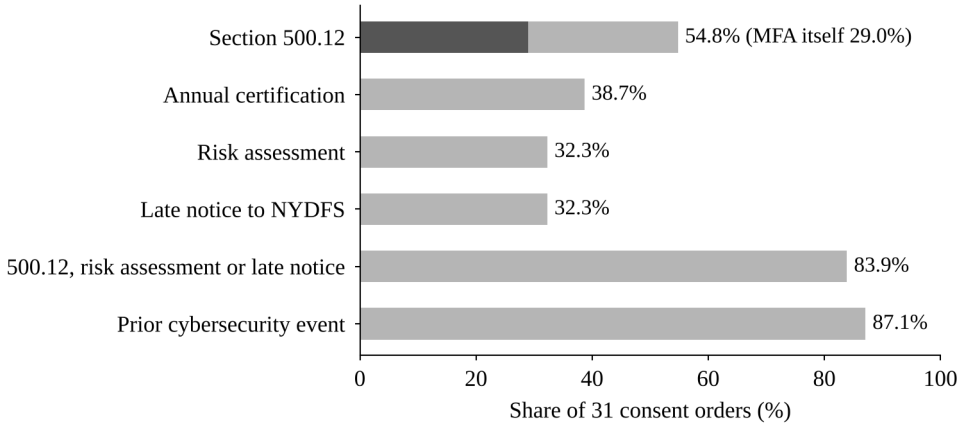


Figure 1: Share of the 31 NYDFS Part 500 Consent Orders Citing Each Requirement, 2021 to 2026. The darker segment of the first bar is the nine orders that name MFA itself.

5.2. Events

A cybersecurity event preceded 27 of the 31 orders (87.1%). Every one of the 17 orders that cite section 500.12 followed an event. The four orders without a prior event were all against virtual currency firms, and none of them cites section 500.12. This pattern suggests that NYDFS has reached access-control findings through its review of incidents.

5.3. Sectors

Table 2 reports the orders by sector. Insurance licensees are party to 20 of the 31 orders and to 14 of the 17 that cite section 500.12. Virtual currency firms account for the largest dollar total, $90,200,000 across five orders, of which $88,000,000 sits in the three orders that combine Part 500 with other findings. None of the five cites section 500.12. No chartered bank is party to any of the 31 orders.

Sector	Orders	Penalties ($)	500.12	Risk assessment	Late notice	Certification
Insurance licensees	20	48,275,000	14	4	7	10
Mortgage and consumer lending	4	12,500,000	2	2	2	0
Virtual currency	5	90,200,000	0	3	1	2
Money transmission	2	2,250,000	1	1	0	0
All orders	31	153,225,000	17	10	10	12

Table 2: NYDFS Part 500 Consent Orders by Sector, 2021 to 2026. Penalties include the three orders that combine Part 500 with other findings.

5.4. Change Over Time

Table 3 reports the orders by year. From 2021 to 2024, 7 of 17 orders (41.2%) cite section 500.12. In 2025 and 2026, 10 of 14 orders (71.4%) do. Eight of the ten 2025 orders were against auto insurers and were announced together on October 14, 2025;[20] six of those eight cite section 500.12. Counting the eight as one action lowers M to 50.0% (Appendix A), so the rise is in part the mark of a single enforcement sweep.

Year	Orders	Penalties ($)	Orders citing 500.12	Share citing 500.12
2021	4	6,450,000	2	50.0%
2022	4	41,400,000	3	75.0%
2023	6	58,800,000	1	16.7%
2024	3	14,200,000	1	33.3%
2025	10	23,125,000	8	80.0%
2026 (to November)	4	9,250,000	2	50.0%
2021 to 2026	31	153,225,000	17	54.8%

Table 3: NYDFS Part 500 Consent Orders by Year of Announcement, 2021 to 2026.

6. Discussion

Our results describe NYDFS enforcement and do not describe the state of any one firm. They show that more than half of the Part 500 consent orders cite a failure under section 500.12, and that those orders carry two thirds of the penalties in orders that concern cybersecurity alone. Almost every order followed a cybersecurity event. For a covered entity, these results suggest that the access paths into its systems, and the controls on each, are the part of the program NYDFS has most often found deficient after an event.

The annual certification is the second most cited requirement. In these 12 orders NYDFS found that the firm had certified compliance for a year in which, on the facts found, it had not complied, or had not filed the certification at all. The acknowledgment of noncompliance, available since the second amendment, gives a firm in that position a filing it can sign accurately.[1] The April 2027 submission covers calendar year 2026, the first full year in which MFA has been required for any individual who accesses the firm’s information systems.[1,24]

The orders point to three steps a covered entity may take before its next submission. The first is an inventory of every path into its information systems, including email, remote access, and portals used by customers, agents, brokers and vendors, with the MFA control on each path recorded and any exception approved in writing. The second is a dated record of the risk assessment and of the evidence behind each Part 500 section, kept to support either a certification or an acknowledgment. The third is a written incident procedure that starts the 72-hour clock for notice to NYDFS when the

firm determines that a reportable event has occurred, since late notice is cited in 10 of the 31 orders.

7. Limitations

Our analysis has six limitations. First, the list of orders may be incomplete. It was built from the NYDFS cybersecurity listing, newsroom and annual enforcement reports for 2021 to 2025, the NYDFS listing proved incomplete, and the 2026 orders rest on the newsroom alone. Second, consent orders are negotiated. Each states the findings NYDFS and the firm agreed to, and a finding left out of an order is not evidence that the control was in place.

Third, the orders are selected by events. They show what NYDFS cites after an event, and they cannot show how often each control fails across all covered entities. Fourth, one enforcement sweep supplies eight of the 31 orders. Fifth, penalties reflect many factors beyond the sections cited, including cooperation and prior history, and no order splits its penalty by section. D therefore measures where penalties fell and should not be read as the price NYDFS sets on any one requirement. Sixth, the orders are those of one regulator. Other state insurance regulators and federal agencies enforce their own rules, and we make no comparison with them.

8. Conclusion

New York requires the top executive and the CISO of each covered firm to sign an annual statement on compliance with Part 500. We evaluate which requirements NYDFS has cited when it penalized a firm under the regulation. Across 31 consent orders from March 2021 to November 2026, with $153,225,000 in penalties, 17 (54.8%) cite section 500.12, and those 17 carry 66.8% of the penalties in orders that concern cybersecurity alone. Nine orders (29.0%) name MFA itself.

Twenty-six orders (83.9%) cite at least one of section 500.12, risk assessment or late notice, and 27 (87.1%) followed a cybersecurity event. The share citing section 500.12 was 71.4% in 2025 and 2026, and insurance licensees are party to 20 of the 31 orders.

Although these counts cannot show how often controls fail, they do show where enforcement has landed. For a firm regulated by NYDFS, the record suggests that confirming MFA on every access path, keeping dated evidence for each section of Part 500, and setting the 72-hour notice procedure in writing may be the most useful preparation for the submission due April 15, 2027.

Appendix A: Sensitivity of the Measures

Table A.1 reports M and D under each alternative reading and period. Table A.2 reports C under the strict reading of the one order without a numbered finding.

Specification	Orders	Orders citing 500.12	Share of orders (M)	Share of penalties (D)
Baseline: all orders, any finding under 500.12	31	17	54.8%	66.8%
Only the nine orders that name MFA itself	31	9	29.0%	40.3%
Hartford Fire Insurance counted as citing 500.12	31	18	58.1%	71.4%
Orders whose findings concern cybersecurity alone	28	17	60.7%	66.8%
Orders preceded by a cybersecurity event	27	17	63.0%	69.1%
The eight October 2025 orders counted as one action	24	12	50.0%	66.8%
Orders to the end of 2025 only	27	15	55.6%	65.8%
Orders from 2021 to 2024	17	7	41.2%	57.1%
Orders from 2025 and 2026	14	10	71.4%	76.7%
D over all penalties, with the three combined orders included	31	17	54.8%	28.4%

Table A.1: Share of Orders and of Penalties Citing Section 500.12 Under Alternative Specifications.

Reading	Risk assessment	Late notice	At least one of 500.12, risk assessment, late notice	Core-control share (C)
Baseline: counted for risk assessment and late notice	10	10	26	83.9%
Strict: counted for neither	9	9	25	80.6%

Table A.2: Core-Control Share (C) Under Two Readings of the Residential Mortgage Services Order.

Across the specifications in Table A.1, section 500.12 is cited in at least 9 orders, and the orders that cite it carry at least 28.4% of the penalties in the base used. Under every specification except the narrowest reading of section 500.12, it is the requirement cited most often; under that reading, the annual certification (12 orders) is cited more often. The level of M depends on whether the earlier access-control finding under section 500.12(a) is counted. The direction of the finding does not.

Appendix B: The 31 Consent Orders

Year	Entity	Sector	Penalty ($000)	500.12	RA	Notice	Cert	Event	Ref.
2021	Residential Mortgage Services	Lend	1,500		Y	Y		Y	2
2021	National Securities Corporation	Ins	3,000	Y		Y	Y	Y	3
2021	First Unum Life and Paul Revere Life	Ins	1,800	Y			Y	Y	4
2021	LifeMark Securities	Ins	150					Y	5
2022	Carnival Corporation	Ins	5,000	Y		Y	Y	Y	6
2022	Robinhood Crypto	VC	30,000*				Y		7
2022	EyeMed Vision Care	Ins	4,500	Y	Y		Y	Y	8
2022	TTEC Healthcare Solutions	Ins	1,900	Y			Y	Y	9
2023	Coinbase	VC	50,000*			Y		Y	10
2023	BitPay	VC	1,000		Y				11
2023	bitFlyer USA	VC	1,200		Y				12
2023	OneMain Financial Group	Lend	4,250					Y	13
2023	SA Stone Wealth Management	Ins	1,350	Y		Y	Y	Y	14
2023	First American Title Insurance	Ins	1,000					Y	15
2024	Genesis Global Trading	VC	8,000*		Y		Y		16
2024	GEICO	Ins	5,000		Y		Y	Y	17
2024	Travelers Indemnity	Ins	1,200	Y				Y	17
2025	PayPal	MT	2,000	Y				Y	18
2025	Healthplex	Ins	2,000	Y		Y	Y	Y	19
2025	Farmers Insurance Exchange	Ins	2,775	Y		Y		Y	20
2025	Hagerty Insurance Agency	Ins	1,850	Y				Y	20
2025	Hartford Fire Insurance	Ins	3,000					Y	20
2025	Infinity Insurance	Ins	2,250	Y	Y	Y		Y	20
2025	Liberty Mutual Insurance	Ins	2,700	Y			Y	Y	20
2025	Metromile Insurance	Ins	2,050		Y		Y	Y	20
2025	Midvale Indemnity	Ins	2,000	Y				Y	20
2025	State Automobile Mutual	Ins	2,500	Y				Y	20
2026	Delta Dental (two companies)	Ins	2,250			Y		Y	21
2026	Order Express	MT	250		Y			Y	22
2026	Rocket Mortgage	Lend	2,000	Y		Y		Y	23
2026	Nationstar Mortgage (Mr. Cooper)	Lend	4,750	Y	Y			Y	23
Total	31 orders		153,225	17	10	10	12	27	

*Table B.1: NYDFS Part 500 Consent Orders, March 2021 to November 2026, by Year of Announcement. Penalties in thousands of dollars. Y = the order cites the requirement (Section 3.3). Sector: Ins = insurance licensee; Lend = mortgage or consumer lending; VC = virtual currency; MT = money transmission. * = order combines Part 500 with other findings and states no Part 500 share. RA = risk assessment; Notice = late notice to NYDFS; Cert = annual certification; Event = a cybersecurity event preceded the order.*

References

1. New York State Department of Financial Services. 23 NYCRR Part 500, Cybersecurity Requirements for Financial Services Companies, as amended November 1, 2023. Sections 500.12, 500.17(b)(1) and (b)(2), 500.21(b), 500.22(d). https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500 (unofficial text published by NYDFS).

2. New York State Department of Financial Services. Press release, March 3, 2021, and consent order, In the Matter of Residential Mortgage Services, Inc. Findings paras. 12 to 14, penalty para. 21. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202103031

3. New York State Department of Financial Services. Press release, April 14, 2021, and consent order of April 12, 2021, In the Matter of National Securities Corporation. Violations paras. 34 to 38, penalty para. 39. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202104141

4. New York State Department of Financial Services. Press release, May 13, 2021, and consent order of May 12, 2021, In the Matter of First Unum Life Insurance Company of America and Paul Revere Life Insurance Company. Violations paras. 31 to 33, penalty para. 34. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202105131

5. New York State Department of Financial Services. Consent order of September 20, 2021, In the Matter of LifeMark Securities Corp. Violation para. 16, penalty para. 18. https://www.dfs.ny.gov/system/files/documents/2021/10/ea20210920_co_lifemark.pdf

6. New York State Department of Financial Services. Press release, June 24, 2022, and consent order of June 23, 2022, In the Matter of Carnival Corporation and subsidiaries. Violations para. 36, penalty para. 37. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202206241

7. New York State Department of Financial Services. Press release, August 2, 2022, and consent order of August 1, 2022, In the Matter of Robinhood Crypto, LLC. Violations paras. 68 to 69, penalty para. 71. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202208021

8. New York State Department of Financial Services. Press release, October 18, 2022, and consent order, In the Matter of EyeMed Vision Care LLC. Violations paras. 35 to 41, penalty para. 42. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202210181

9. New York State Department of Financial Services. Consent order of December 2, 2022, In the Matter of TTEC Healthcare Solutions, Inc. Violations paras. 18 to 21, penalty para. 22. https://www.dfs.ny.gov/system/files/documents/2022/12/ea20221202_ttec_hs.pdf

10. New York State Department of Financial Services. Press release, January 4, 2023, and consent order, In the Matter of Coinbase, Inc. Violation para. 72, penalty para. 73, compliance commitment para. 81. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202301041

11. New York State Department of Financial Services. Consent order of March 2023, In the Matter of BitPay, Inc. Violations paras. 22 to 23, penalty para. 24. https://www.dfs.ny.gov/system/files/documents/2023/03/ea20230316_bitpay.pdf

12. New York State Department of Financial Services. Consent order of May 2023, In the Matter of bitFlyer USA, Inc. Violation para. 17, penalty para. 19.

https://www.dfs.ny.gov/industry_guidance/enforcement_discipline/ea20230501_bitflyer_usa_inc

13. New York State Department of Financial Services. Press release, May 25, 2023, and consent order of May 24, 2023, In the Matter of OneMain Financial Group, LLC. Violations paras. 25 to 29, penalty para. 30. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202305251

14. New York State Department of Financial Services. Consent order of July 2023, In the Matter of SA Stone Wealth Management Inc. Violations paras. 17 to 19, penalty para. 20. https://www.dfs.ny.gov/industry_guidance/enforcement_discipline/ea20230707_sa_stone_wealth_mgmt

15. New York State Department of Financial Services. Press release, November 28, 2023, and consent order of November 27, 2023, In the Matter of First American Title Insurance Company. Violations paras. 23 and 27 to 28, penalty para. 29. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311281

16. New York State Department of Financial Services. Press release, January 12, 2024, and consent order of January 11, 2024, In the Matter of Genesis Global Trading, Inc. Violations paras. 53 to 60, penalty para. 61. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr2024011224

17. New York State Department of Financial Services. Press release, November 25, 2024 (joint with the Office of the New York State Attorney General), and consent orders, In the Matter of Government Employees Insurance Company (violations paras. 38 to 44, penalty para. 45) and In the Matter of Travelers Indemnity Company (violation para. 28, penalty para. 29). https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20241125

18. New York State Department of Financial Services. Press release, January 23, 2025, and consent order, In the Matter of PayPal, Inc. Violations paras. 21 to 22, penalty para. 23. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250123

19. New York State Department of Financial Services. Press release, August 14, 2025, and consent order, In the Matter of Healthplex, Inc. Violations paras. 28 to 31, penalty para. 32. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20250814

20. New York State Department of Financial Services. Press release, October 14, 2025, and consent orders of the same date, In the Matter of Farmers Insurance Exchange; Hagerty Insurance Agency, LLC; Hartford Fire Insurance Company; Infinity Insurance Company; Liberty Mutual Insurance Company; Metromile Insurance Company; Midvale Indemnity Company; and State Automobile Mutual Insurance Company. Pre-amendment text of section 500.12(a) quoted in the Midvale order, para. 18. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20251014

21. New York State Department of Financial Services. Press release, April 30, 2026, and consent order of April 29, 2026, In the Matter of Delta Dental Insurance Company and Delta Dental of New York, Inc. Violation para. 27, penalty para. 28. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20260430

22. New York State Department of Financial Services. Press release, August 5, 2026, and consent order of August 3, 2026, In the Matter of Order Express, Inc. Event paras. 7 to 8, violation para. 17, penalty para. 20. https://www.dfs.ny.gov/reports_and_publications/press_releases/pr20260805

23. New York State Department of Financial Services. Press release, November 19, 2026, and consent orders, In the Matter of Rocket Mortgage, LLC (violations paras. 21 and 23, penalty para. 24) and In the Matter of Nationstar Mortgage LLC d/b/a Mr. Cooper (violations paras. 31 to 32, penalty para. 33). https://www.dfs.ny.gov/PR20261119

24. New York State Department of Financial Services. Multi-Factor Authentication (guidance). September 2025. https://www.dfs.ny.gov/system/files/documents/2025/09/multifactor-authentication.pdf

25. New York State Department of Financial Services, Consumer Protection and Financial Enforcement Division. Annual reports for 2021, 2022, 2023, 2024 and 2025. https://www.dfs.ny.gov/reports_and_publications/dfs_annual_reports

Disclaimer

This report is published by Bridgham Technology Institute for informational and analytical purposes only. It does not constitute investment advice, legal counsel, or a solicitation of any kind. All data are drawn from public NYDFS press releases, consent orders, regulation text and guidance. No client data, proprietary data or survey data was used, and no organization was contacted. Reproduction or redistribution of this report, in whole or in part, requires attribution to Bridgham Technology Institute. For questions regarding methodology or data, contact headofresearch@bridghamcyber.com.