The New York Department of Financial Services (NYDFS) recently released draft amendments to its “Part 500” cybersecurity regulation, which covers all financial services providers authorized by the department - including many large insurance companies, foreign banks, and digital asset firms - as well as certain third parties that provide services to them. The amendments contain significant updates to the agency’s existing expectations, including:

- **Stricter requirements for larger firms.** The amendments would create a new category of “Class A companies,” which are firms with 2,000 employees or an average of $1b in gross annual revenues over the past three years. These firms would be required to (1) undergo an independent annual audit of their cybersecurity programs; (2) conduct a risk assessment at least once every three years with an external expert; (3) review information systems at least weekly and report any gaps to the Board and senior management; (4) implement a password vaulting system for privileged accounts; and (5) implement an endpoint detection and response system to monitor for anomalous activity and generate alerts.

- **Prescriptive rules for data management and access controls.** Firms would be required to keep an ongoing “complete asset inventory,” limit access to privileged accounts, and maintain backups isolated from network connections. The amendments also add new requirements around multi-factor authentication (MFA), eliminating text messages as a permissible form of authentication due to their vulnerability to SIM swap attacks, requiring MFA for all external access to privileged accounts, and removing CISOs’ ability to approve alternative controls.

- **New notification requirements.** Under the draft amendments, firms would be required to notify NYDFS within 72 hours of any cybersecurity event in which an unauthorized user has gained access to a privileged account or in which ransomware has been deployed within a material part of the firm’s systems. They would also be required to notify NYDFS within 24 hours of any extortion payment connected with a cybersecurity event. The current rule only requires reporting for cyber incidents that have a material likelihood of harming the firm’s normal operations.

- **Increased governance expectations.** Chief Information Security Officers (CISOs) would be expected to have authority to manage cyber risks and report to the Board at least annually on plans for remediating inadequacies in the cyber program. Policies and procedures would require at least annual approval by the firm’s senior governing body (Board or Board equivalent). Boards would also be expected to either have or be advised by persons with sufficient cyber expertise. In addition to the CISO, the CEO would have to co-sign the annual certification.

- **Operational resilience planning, testing, and training in focus.** The amendments would expand current expectations around incident response plans to require that they incorporate the possibility of ransomware incidents. Firms would also be required to implement business continuity and disaster recovery plans that are reasonably designed to ensure the availability and functionality of the covered entity’s services. NYDFS would expect firms to periodically test plans with all applicable staff, including senior management, and update them as necessary and conduct routine training of key stakeholders.

Comments on the draft amendments are due by August 18th. NYDFS is expected to issue a formal proposal with a 60-day comment period shortly thereafter. The majority of the amendments would require compliance 180 days after they become effective. Although the proposed changes include transition periods for some provisions such as changes to password management, multi-factor authentication and monitoring requirements, finalization before year end would mean firms would have to be fully compliant for the December 31, 2023 certification, which would be due April 15, 2024.
The cyber landscape has evolved significantly in the five years since NYDFS released its original rule, with a series of high-profile incidents, the rise of ransomware and vulnerabilities associated with digital assets. Now, the agency is making it clear that firms need to keep up. Given the significant amount of time and resources required for some of these new expectations, firms should not wait until a final rule to act - especially considering the tight 180-day compliance deadline. Conducting a complete asset inventory will be a significant undertaking for many firms, and some firms may find themselves scrambling before the deadline unless they start now. Similarly, the removal of text messages as a permissible portion of an MFA solution and the elimination of the CISO’s ability to allow for “equivalent controls” may prove challenging for firms that have relied on these provisions of the current rule. In addition, enhancing and testing incident response and business continuity plans with all applicable staff will also take careful thought, time and training. With the ongoing “war for talent,” especially in the cybersecurity field, ensuring that Boards have adequate cybersecurity expertise may be a challenge for some firms. Despite these challenges, the draft amendments bring NYDFS’s expectations in line with what has become best industry practice. Regardless of the eventual final rule, using the amendments as a guidepost to enhance cyber programs will not only make firms well-equipped to handle regulatory scrutiny but will better protect their customers, their reputation, and themselves.

On August 1st, Securities Industry and Financial Markets Association (SIFMA), Investment Company Institute (ICI), and Depository Trust & Clearing Corporation (DTCC) released a playbook outlining implementation activities for accelerating the settlement cycle from trade date plus two days (T+2) to trade date plus one day (T+1). This publication follows a December 2021 report by the same industry groups outlining recommendations for the T+1 transition and a February 2022 SEC proposal of rule changes to complete the transition by March 31, 2024.

The playbook begins with an overview of the previous transition from T+3 to T+2 in 2017 and how it has informed the current transition. It then covers activities, timelines, dependencies and risk impacts pertaining to trade processing, asset servicing, documentation, securities lending, prime brokerage, funding and liquidity. It also discusses implementation considerations including documentation changes, regulatory rule changes, testing readiness and migration plans. Industry Steering Committee (ISC) will develop an industry-wide communication and socialization plan, create a T+1 Command Center and set protocols for migration. The playbook assumes a Q3 2024 transition date but notes that this could be updated depending on when the SEC proposal is finalized.

As the playbook describes, the shift to T+1 presents a more stark difference than the previous transition to T+2. With a one-day buffer for allocations, affirmation and disaffirmation processes, there is increased pressure on the speed and accuracy of these activities and a decreased tolerance for issues such as settlement errors and fails. With the target date for T+1 now just over a year and a half away, firms should not wait to develop a plan to identify its impact across their organization. An essential early step is the establishment of a central project management office (PMO) to coordinate the impact assessment, implementation efforts, and communications both within the organization and with other market participants. This playbook provides a useful guide for the PMO to understand the extensive pre-work that is needed to effectively transition processes to accommodate one day settlement, but firms will still need to assess its application to their unique business models and operations. In addition, they may need to expand on topics covered in the playbook. For example, while it does not extensively cover data quality improvement, many firms may find it to be a significant prerequisite for accelerating their settlement processes.
Firms should also note that this transition is a precursor for further acceleration in the settlement cycle, including the prospect of real-time settlement. The transactions landscape is constantly evolving, most recently with digital assets becoming a separate asset class as well as the emergence of distributed ledger technology architecture and industry interoperable solutions. While the SEC and industry groups are still focused on successfully completing the transition to T+1 before considering real-time settlement, firms should be planning enhancements to their people strategy, technology optimization and process re-engineering to remain flexible for further transformation.

For more, see *T+1 and beyond: A forward-looking transition approach*.

### 3. CFPB to scrutinize digital marketing and data security practices

On August 10th, the CFPB issued an [interpretive rule](#) clarifying that firms - including big tech companies - that provide digital marketing and advertising services to financial institutions can be held liable by the agency (or other federal and state regulators) for violating consumer protection laws such as by committing unfair, deceptive, or abusive acts or practices (UDAAP). The rule explains that while traditional platforms that provide “time and space” for advertisements such as television and radio are excluded from CFPB scrutiny, digital marketers go beyond these traditional functions by collecting data, identifying customers and personalizing content. In a speech, CFPB Director Rohit Chopra described this activity as “an amalgam of an ad, a private investigator, and a digital door-to-door sales force.” He expressed concern that these practices have resulted in protected classes being excluded from the reach of certain financial services marketing efforts, resulting in violations of fair lending rules.

In addition, on August 11th, the CFPB published a [circular](#) to notify financial institutions, including nonbanks and fintechs, that failing to effectively safeguard consumer data could expose them to liability under the Consumer Financial Protection Act. The circular explains that “inadequate security for the sensitive consumer information collected, processed, maintained, or stored by the company can constitute an unfair practice” even in the absence of a breach or intrusion. It also highlights several widely used data security practices that are not required but could increase risk of triggering liability if not utilized, including multi-factor authentication, adequate password management and timely software updates.

*Our Take*

Director Chopra has made it a priority of his tenure to expand the CFPB’s reach beyond traditional financial services firms and into tech companies, recently explaining his interpretation that the Dodd-Frank Act provides the agency with authority over certain nonbanks and ordering big tech companies to provide information around their data harvesting and monetization practices. Fair lending will receive significant scrutiny from this initiative, especially considering the recent launch of a joint DOJ and CFPB anti-redlining initiative, but it will apply to the marketing of both credit and non-credit products. We have seen firms respond to this scrutiny by (1) implementing “variance reduction systems” to ensure that protected classes receive financial advertisements in equal proportion to other customer segments and (2) restricting financial services firms from customizing customer segments. Digital marketers that provide personalized advertisements tailored to the recipient should be aware of the growing scope of UDAAP including recent updates on discriminatory practices and deceptive review policies, and carefully review whether such content does not violate these laws.

The CFPB’s notification on potential consumer financial protection liability is just the latest of a long list of consequences that could arise from ineffective consumer data protection, but it demonstrates that regulators will not necessarily wait for a breach to cite a firm for deficiencies in security practices. While Chopra’s efforts to push the limits of CFPB oversight may receive legal challenges - and fiery hearings should the Republicans retake either house of Congress in November - the message is clear that the current Administration will not let any company engaging in financial services, including big tech firms, off the hook when it comes to discrimination and inadequate data security resulting in consumer harm.
4. SEC and CFTC propose private fund reporting amendments

On August 10th, the SEC and CFTC jointly proposed amendments to Form PF that would require more information from large hedge funds and their investment advisers. Form PF was instituted following the financial crisis to require certain private equity and hedge funds to report financial, ownership, performance and exposure details to the government on a quarterly and annual basis. The agencies noted that the additional data requested in the proposal would be used to help the Financial Stability Oversight Council (FSOC) monitor potential systemic risk in the private fund space.

Specifically, the proposal would require advisers to large hedge funds (i.e., with a net asset value of over $500m) to report new details on their investment, borrowing, counterparty, country, currency and industry exposures; market factor effects; turnover; central clearing counterparty reporting; risk metrics; investment performance by strategy; portfolio correlation and liquidity. It would also require hedge funds to report additional information on their investment strategies with more granular categories; trading and clearing mechanisms; and counterparty exposures. In addition, it would require private fund advisers to report details including identifying information; assets under management; withdrawal and redemption rights; gross asset value and net asset value; inflows and outflows; base currency; borrowings and types of creditors; fair value hierarchy; beneficial ownership; and fund performance. The proposal would also remove aggregate reporting requirements for large hedge funds and require separate reporting of component funds in complex structures.

The SEC will accept comments until October 9th or 30 days after publication in the Federal Register, whichever is later.

Our Take

This proposal is just the latest step by the SEC to gain insight into the risks posed by the rapidly growing private fund industry. This industry has faced several other rulemaking proposals this year\(^1\) and is likely to protest the extent of the new reporting requirements proposed this week. While this proposal would not make Form PF public, as some had feared from Gensler’s past comments, it would require private funds and their advisers to source and validate considerably more data than they currently report on Form PF. Given the short comment period, hedge fund advisers should quickly collect their views on areas where the proposal requirements may not be practical or duplicative of existing reporting.

5. On our radar

These notable developments hit our radar this week:

- **SEC proposes clearing agency governance rules.** On August 8th, the SEC proposed rules to mitigate conflicts of interest on boards or governing bodies of registered clearing agencies. The proposal would impose requirements concerning board composition and director independence as well as policies and procedures around conflicts of interest and oversight of critical service providers.

- **Treasury continues digital asset-focused sanctions.** On August 8th, the Treasury Department’s Office of Foreign Assets Control sanctioned a virtual currency “mixer” for laundering more than $7 billion, including significant amounts in violation of North Korea-focused sanctions. Mixers are tools used to obfuscate the origin, destination and counterparties of digital asset transactions.

- **Senate passes Inflation Reduction Act.** On August 7th, the Senate passed a reconciliation bill known as the Inflation Reduction Act with a tie-breaking vote by VP Kamala Harris. In addition to Democratic initiatives on climate and prescription drug pricing, the bill contains a number of revenue raising provisions with tax impacts on corporations and partnerships. For more on the tax impact of the Inflation Reduction Act, see PwC’s latest Tax Insights.

---

\(^1\) In January, the SEC proposed another set of Form PF amendments to require large fund advisers to file reports within one day of certain events, lower the current threshold for filing by large PE advisers, and require them to report more granular information. That proposal has not yet been finalized.
Additional information

For additional information on Our Take series or PwC’s Cyber, Risk and Regulatory Practice please contact:

**Adam Gilbert**
Financial Services Advisory Regulatory Leader
914 882 2851
adam.gilbert@pwc.com

**Roberto Rodriguez**
Managing Director of Regulatory Strategy
310 497 3215
roberto.j.rodriguez@pwc.com

**Contributing authors:** Joe Nocera, Matt Gorham, Robert Donovan, Shawn Lonergan, Amanda Cox, Nicole Anderson, Pete Driscoll, Chris Pullano, Geoff Dworkin, Jared Feldman, Natalie Povolotskaya, Dileep Venkatakrishnan, Jason Magesis, Shilpi Jain, Philip Aquilino, Eileen Curran, Michael Horn and Tanya Pazhitnykh.

To learn more about financial services regulation from your iPad or iPhone, [click here](#) to download PwC’s Regulatory Navigator App from the Apple App Store.

© 2022 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see [www.pwc.com/structure](http://www.pwc.com/structure) for further details.

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. PwC US helps organizations and individuals create the value they’re looking for. We’re a member of the PwC network of firms in 157 countries with more than 276,000 people. We’re committed to delivering quality in assurance, tax, and advisory services. Tell us what matters to you and find out more by visiting us at [ww.pwc.com/us](http://ww.pwc.com/us).