AN A.S. PRATT PUBLICATION
OCTOBER 2018
VOL. 4 • NO. 8

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 4 NUMBER 8 OCTOBER 2018

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at 908-673-3380
Email: .... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at .... (800) 833-9844
Outside the United States and Canada, please call .... (518) 487-3385
Fax Number .... (800) 828-8341
Customer Service Web site .... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or .... (800) 223-1940
Outside the United States and Canada, please call .... (937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [4] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [247] (LexisNexis A.S. Pratt)

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2018–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

CCPs as Third Party Service Providers: Breach Notification Issues

Douglas Landy, John Williams, Nicholas Smith, Joel Harrison, and James Kong*

The authors of this article explain breach notification issues when central counterparties are considered third party service providers.

Among the requirements placed on New York chartered- or licensed-financial institutions is that, pursuant to Section 500.17 ("Notices to the Superintendent"), each such entity must notify the superintendent of the New York State Department of Financial Services as promptly as possible but in no event later than 72 hours following a cybersecurity event.[1] This is a difficult standard to meet within a tight timetable under the best of circumstances; however, in many events the cybersecurity incident will occur not in the financial institution but within a third party service provider (a "TPSP").[2]

Section 500.11 requires each covered entity to have a TPSP security policy.[3] Generally speaking, covered entities include New York chartered banks (such as Goldman Sachs Bank and The Bank of New York), and licensed branches and agencies of foreign banks (such as the New York branches of Deutsche Bank and BNP Paribas) (collectively, "Covered Entities"). As part of this policy, every Covered Entity must have written policies and procedures (based on the risk profile of the entity) that include relevant guidelines for due diligence and/or contractual protections addressing notice to be provided to the entity following a cybersecurity event "directly impacting . . . [the entity's] Nonpublic information being held by the [TPSP]." This requirement seems to directly link to the requirement of such entity to provide the 72 hour notification.

---

* Douglas Landy (dlandy@milbank.com) is a partner at Milbank, Tweed, Hadley & McCloy LLP and a member of the Leveraged Finance Group. John Williams (jwilliams@milbank.com) is a partner at the firm and a member of the Alternative Investments Practice. Nicholas Smith (nsmith@milbank.com) is a partner in the firm's Technology Practice. Joel Harrison (jharrison@milbank.com) is a partner at the firm specializing in technology and data privacy and cybersecurity. James Kong (jkong@milbank.com) is an associate in the firm's Leveraged Finance Group.

1 According to the New York Department of Financial Services ("NYDFS"), "[a] Cybersecurity Event is reportable if it falls into at least one of the following categories: the Cybersecurity Event impacts the Covered Entity and notice of it is required to be provided to any government body, self-regulatory agency or any other supervisory body; or the Cybersecurity Event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity. An attack on a Covered Entity may constitute a reportable Cybersecurity Event even if the attack is not successful." In a separate answer, the NYDFS noted "notice to the Department under 23 NYCRR Section 500.17(a)(2) would generally not be required if, consistent with its Risk Assessment, a Covered Entity makes a good faith judgment that the unsuccessful attack was of a routine nature." https://www.dfs.ny.gov/about/cybersecurity_faqs.htm.

2 Federal regulation also contains requirements on TPSPs. *See, e.g.*, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

3 23 N.Y. C.R.R. § 500.11.

Part 500 defines Nonpublic Information ("NPI") more broadly than did prior, applicable federal law.[4] NPI includes (1) business related information of the entity the tampering with which, or disclosure, access or use of which, would cause a material disruption to the business, operations or security of the entity, (2) certain information of individuals which can be used to identify such individual, and (3) certain health care information. Of particular interest is (1), which would cover large and uncertain amounts of an entity's information held by TPSPs.

The most commonly thought of TPSPs are service providers to Covered Entities that handle the entities' information, such as technology service providers (including vendors under outsourcing contracts and cloud computing providers), software companies, couriers, law firms and accounting firms. These TPSPs must now include detailed breach notification provisions in their agreements with financial institutions so that the TPSPs will determine a cybersecurity event has occurred and provide enough detailed information to Covered Entities so that the entity can meet its own 72 hour notification obligation pursuant to Section 500.11.

There is a large category of TPSPs that may not consider themselves covered by Part 500: central counterparties ("CCPs"). CCPs appear to meet the definition to be covered as TPSPs: they are not affiliates of financial institutions, they provide services to financial institutions, and they have access to NPI from the financial institutions (although the amount and type of NPI each CCP holds will vary depending on the services it provides). But there is one difference between CCPs and other TPSPs: CCPs do not negotiate contracts with individual members. As regulated entities themselves (by the Securities and Exchange Commission (the "SEC") for securities CCPs and by the Commodity Futures Trading Commission (the "CFTC") for derivatives or commodities CCPs), each CCP promulgates a set of rules that govern its actions. These rules are issued by each CCP in its status as a self-regulatory organization ("SRO"), which means they are issued for public comment and approved (by the SEC) or made effective (by the CFTC).

When members join the CCP, they agree to be bound by its rules. They generally do not have the ability to negotiate individual requirements. Many CCP rules do not contain the types of specific, detailed provisions that Covered Entities are negotiating with TPSPs in order to satisfy their requirements under Section 500.11. Therefore, it

[4] Title V of the Gramm-Leach-Bliley Act of 1999 ("GLBA"). In particular, Section 509(3) of the GLBA defined NPI as, among other things, "personally identifiable financial information – (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution. . ." Similarly, the European Union General Data Protection Regulation ("GDPR"), which will apply from May 25, 2018, applies to "personal data," rather than NPI under Part 500.

is unclear if Covered Entities subject to Part 500 that have memberships in CCPs will be able to meet the 72 hour cybersecurity event notification requirement in relation to a cybersecurity breach affecting a CCP.

CCP RULES AND REQUIREMENTS – BIS REQUIREMENTS

Every CCP is different, and each one has its own set of rules. There are, however, national and international requirements that each CCP must meet. For example, in April 2012 the Committee on Payment and Settlement Systems of the Bank for International Settlements ("BIS") promulgated the Principles for Financial Market Infrastructure ("PFMIs"), which are perhaps the most comprehensive set of standards for CCPs.[5] Sections 3.17.2 and 3.17.16 of the PFMIs note that a CCP must prepare for and communicate with authorities about cyberattacks. The PFMIs do not address notifications to members.

In June 2016, the BIS supplemented the PFMIs with Guidance on cyber resilience for financial market infrastructures.[6] This guidance detailed how CCPs were expected to enhance their cyber resilience, and provided supplemental detail to that in the PFMIs. The guidance does not, however, state that CCPs should put in place procedures to ensure proper notice of cybersecurity incidents to their members. Rather, the guidance instead proposes that CCPs rely on their members and other stakeholders to support CCP preparations. The focus is on assisting the CCPs in responding to a cyber incident and quickly resuming normal operations and maintaining financial stability; it does not mention assisting the CCP members in complying with their own, separate obligations. Section 6.4.3 of the guidance states the following:

> 6.4.3 Crisis communication. FMIs should plan in advance for communications with participants, interdependent FMIs, authorities and others (such as service providers and, where relevant, the media). Communication plans should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cyber incidents may be necessary, FMIs should determine decision-making responsibilities for incident response in advance, and implement clearly defined escalation and decision-making procedures. FMIs should inform relevant oversight and regulatory authorities promptly of potentially material or systemic events.

[5] https://www.bis.org/cpmi/publ/d101a.pdf.
[6] https://www.bis.org/cpmi/publ/d146.pdf.

BUT DO CCPs HAVE "PLANS IN ADVANCE" TO TIMELY COMMUNICATE ABOUT SUCH INCIDENTS WITH MEMBERS?[7]

Both the SEC and CFTC have implemented a series of regulatory provisions to implement certain core principles, as well as the PFMI requirements for CCPs that clear securities (SEC) or derivatives (CFTC) trades.

CFTC

The CFTC in Part 39, Subpart B of its regulations lists the required "System Safeguards" a CCP must have in place.[8] A CCP is required to have a system of risk analysis and oversight designed to minimize sources of operational risk. This program must include numerous provisions on information security and protection. The program is not, however, mandated to provide timely cybersecurity breach notification to CCP members.

The closest the regulatory requirements come to this concept is to say:

> (3) Coordination of plans. A derivatives clearing organization shall, to the extent practicable:
>
> (i) Coordinate its business continuity and disaster recovery plan with those of its clearing members, in a manner adequate to enable effective resumption of daily processing, clearing, and settlement of transactions following a disruption.[9]

The CFTC's Core Principles are focused on returning a CCP to full operation as quickly as possible, and to limit any potential systemic contagion from a disabling cybersecurity event. There is no provision relating to the CCP assisting its members with their own obligations relating to a breach at the CCP.

---

[7] We note that notification requirements may differ in the EU. CCPs are specifically identified as "operators of essential services" under the Network and Information Security Directive ("NISD") (specifically, "Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council" fall within the subset of Financial Market Infrastructure). NISD introduces a number of security requirements, including a requirement on CCPs to notify significant security incidents "without undue delay" (no specific timeframe is given). Despite various types of financial institutions and financial market infrastructure providers being specifically identified in NISD as operators of essential services, NISD provides that where a type of operator is subject to EU-level sectoral legislation having at least equivalent effect to NISD, that type of operator is outside the scope of NISD and the sectoral rules apply instead. The proposed United Kingdom implementation of NISD, for example, does not apply to CCPs even though they are specifically listed in the Directive.

[8] 17 C.F.R. § 39.18.

[9] *Id.* at 39.18(c)(3).

This is not to say that there are no notification requirements at a CCP following a cybersecurity breach – it is a reflection of the fact that the only such notification requirement flows upward (to the CFTC) rather than outward (to members):

> (g) Notice of exceptional events. A derivatives clearing organization shall notify staff of the Division of Clearing and Risk [of the CFTC], or any successor division, promptly of: (1) Any hardware or software malfunction, security incident, or targeted threat that materially impairs, or creates a significant likelihood of material impairment, of auto- mated system operation, reliability, security, or capacity; or (2) Any activation of the derivatives clearing organization's business continuity and disaster recovery plan.[10]

SEC

The SEC has operational risk provisions for the CCPs it regulates that are more vague than those of the CFTC.[11] A CCP must establish and maintain written policies and procedures reasonably designed to:

> (4) Identify sources of operational risk and minimize them through the development of appropriate systems, controls, and procedures; implement systems that are reliable, resilient and secure, and have adequate, scalable capacity; and have business continuity plans that allow for timely recovery of operations and fulfillment of a clearing agency's obligations.[12]

Similarly, the SEC also requires CCPs to:

> (17) Manage the covered clearing agency's operational risks by:
>
> (i) Identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls;
>
> (ii) Ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity; and
>
> (iii) Establishing and maintaining a business continuity plan that addresses events posing a significant risk of disrupting operations."[13]

There is, however, no requirement for a CCP to notify a member of a security breach affecting its information.

---

[10] *Id.* at § 39.18(g).
[11] *See* 17 C.F.R. § 240.17AD-22.
[12] *Id.* at § 240.17AD-22(d)(4).
[13] *Id.* at § 240.17AD-22(d)(17).

BUT DO CCP RULES CONTAIN BREACH NOTIFICATION FOR MEMBERS?

There are a limited number of CCPs registered with the SEC or the CFTC. While it is beyond the scope of this client alert to survey each one to determine whether it is obligatory for a CCP to timely notify its members of a cybersecurity breach, there is an industry tool that surveys (and compares) the relevant rules of each CCP.

The Futures Industry Association ("FIA") CCP Risk Review is a private, industry developed product that permits subscribers to review and compare summaries of the rules and procedures of CCPs worldwide.[14] The FIA CCP Risk Review is the most comprehensive review and comparison tool of CCP rules that exists, and it is used by many of the largest Covered Entities to review and monitor their exposure to CCPs.

> The FIA CCP Risk Review specifically reviews the relevant provisions of CCP rules:
>
> "Question 127. CCP Disclosure of technology/communication procedures.
>
> Question 127.1 How, if at all, does the CCP disclose information on its technology and communication procedures in respect of [the services it provides]?"

An initial review of the FIA CCP Risk Review summaries of each of the major U.S. CCPs does not reveal any affirmative obligation to timely disclose cybersecurity breaches to members.

HOW CAN CCPs HELP THEIR MEMBERS PROTECT THEMSELVES THROUGH TIMELY NOTIFICATIONS OF CYBERSECURITY BREACHES?

CCPs likely use TPSPs themselves to support their operations. We suggest that CCPs seek to address the timing question specifically in their agreements with such TPSPs. TPSPs understand the importance of information security and typically are willing to agree to be bound by security-related contractual obligations, provided that those obligations are generic in wording and give sufficient flexibility to the TPSP in determining how those security obligations are met. A few examples of backstop provisions in the security provisions of security agreements follow:

- The security agreement should specify a minimum level of security, even if it permits the TPSP to modify the security procedures over time. Typically, this is done by reference to the information security policy (of the CCP or the TPSP) which will be attached to the services agreement as an exhibit. This approach creates a one-way ratchet dynamic around information security, and sets out a host of security requirements that can serve as definitive reference points in a security audit, or when undertaking a review of a security incident, evaluating whether the TPSP breached the agreement.

[14] https://www.fiadocumentation.org/fia/ccp-risk-review.

- TPSPs often will propose contractual language obligating them to use commercially reasonable or industry standard practices. Ideally, the service agreement language would supplement such language by specifying that such an obligation includes, but is not limited to, implementing and maintaining industry security standards that are specified by name (e.g., a particular ISO security certification level). In addition to establishing a clearer contractual standard, such industry security standards will provide comfort to the CCP that certain minimum security monitoring and reporting capabilities are maintained on an ongoing basis. TSPSs should also be contractually required to complete security audits at least once annually, and to make the results of those audits available to the CCP.
- TPSPs often will propose contractual language obligating them to inform the client of a security incident "promptly" after an incident is discovered. We suggest expanding this language to cover both confirmed incidents and incidents that are not yet confirmed but that are likely to have occurred, and to include a notice timing backstop: "promptly, but in any event no later than 24 hours after the applicable confirmed or likely security incident is discovered."

CCPs should also amend their rules to provide specific assurance and procedures for members to ensure that members may meet their own notification requirements. Such rule changes will likely require the approval of the SEC or CFTC.

CONCLUSION

Covered Entities have spent a significant amount of time and money implementing comprehensive internal information security programs, as well as negotiating detailed protections in contractual arrangements with TPSPs. This combination of protections should assist each Covered Entity in complying with the requirements of Part 500, and limit the potential regulatory exposure should a cybersecurity breach occur (whether originating within the Covered Entity or at a TPSP). Covered Entities that maintain memberships at CCPs may not have such protections, and may find themselves unable to make timely breach notification requirements such a cybersecurity event occur at a CCP.