The Consumer Financial Protection Bureau ("CFPB") recently released a compliance bulletin (the "CSI Bulletin") reviewing the legal responsibilities of regulated entities relating to the sharing of certain CFPB-related confidential supervisory information ("CSI").¹ The CSI Bulletin provides guidance on the type of information that qualifies as CFPB CSI and, therefore, cannot be disclosed to third parties without the prior written approval of the CFPB. Among the circumstances covered by the CFPB is when regulated entities and third parties enter into non-disclosure agreements ("NDAs") purporting to require or restrict the sharing of CSI.

The CSI Bulletin articulates standards familiar to insured depository institutions, which are subject to similar restrictions from their primary federal banking regulators on the sharing of CSI. Importantly, the CSI Bulletin highlights a significant issue for regulated entities that either (1) have possession, custody, or control over information deemed to be CSI of the CFPB, or (2) have entered into an NDA containing confidentiality provisions that conflict with CFPB regulation and policy. While the CFPB’s approach is similar to that of the prudential bank regulators, entities that have not been subject to comprehensive regulation may be unfamiliar with regulators’ expectations regarding the sharing of CSI. Nonbank entities supervised by the CFPB, including nonbank mortgage companies, debt collectors, credit reporting companies, payday lenders, and private education lenders, must be particularly vigilant about their disclosure and transfer of CSI to any person other than their directors, officers, employees, legal counsel, other authorized external service providers, or the CFPB. Entities already familiar with the CSI requirements imposed by the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), or the Federal Deposit Insurance Corporation ("FDIC") should also review the CSI Bulletin, as the scope of coverage and specific procedures for disclosing CSI varies by regulator.

¹ Nonbank entities supervised by the CFPB, including nonbank mortgage companies, debt collectors, credit reporting companies, payday lenders, and private education lenders, must be particularly vigilant about their disclosure and transfer of CSI...
To avoid potential issues with or action by the CFPB, which could include the possibility of civil money penalties, regulated entities should understand what information constitutes CSI and be aware of the applicable restrictions and disclosure requirements to ensure regulated entity practices conform with the CFPB's expectations.

I. Key CSI Requirements

The CFPB, OCC, FRB, and FDIC each have similar, but not identical, requirements regarding the release of CSI related to the examination and supervision activities of entities subject to their jurisdiction. The examinations of regulated entities result in the creation of reports and other communications that regulators deem to be confidential and the exclusive property of the issuing agency. While the broad protection of CSI may be echoed throughout the various agencies and their corresponding regulations, the CFPB, OCC, FRB, and FDIC each provide their own interpretation of what constitutes CSI, and each has flagged various noncompliance issues in recent years. The following chart summarizes the agency requirements and provides a brief look at the additional regulatory guidance provided by each agency.

<table>
<thead>
<tr>
<th>Scope of CSI</th>
<th>CFPB</th>
<th>OCC</th>
<th>FRB</th>
<th>FDIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFPB CSI includes the following:</td>
<td>&quot;Non-public OCC information&quot; includes the following:</td>
<td>FRB CSI includes the following:</td>
<td>FDIC CSI includes the following:</td>
<td></td>
</tr>
<tr>
<td>- CFPB reports of examination, inspection, and visitation, as well as CFPB non-public operating, condition, and compliance reports to the CFPB (including any information derived from those reports);</td>
<td>- Any record created or obtained by the OCC or the OTS in connection with the performance of its responsibilities (e.g., records concerning supervision, licensing, regulation, and examination);</td>
<td>- FRB reports of examination, inspection, and visitation, confidential operating and condition reports (including any information derived from those reports);</td>
<td>- Records that are contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of the FDIC or any agency responsible for the regulation or supervision of financial institutions.</td>
<td></td>
</tr>
<tr>
<td>- Any documents prepared by, on behalf of, or for the use of the CFPB or any other federal, state, or foreign government agency in the exercise of supervisory authority over a regulated entity, and any information derived from such documents;</td>
<td>- Any record compiled by the OCC or the OTS in connection with either agency’s enforcement responsibilities;</td>
<td>- Information gathered by the FRB in the course of any investigation, suspicious activity report, cease-and-desist orders, civil money penalty enforcement orders, suspension, removal or prohibition orders, or other orders or actions (subject to some exceptions);</td>
<td>See 12 C.F.R. § 309.5(g)(8).</td>
<td></td>
</tr>
<tr>
<td>- Any communications between the CFPB or another government agency and a regulated entity related to CFPB supervision;</td>
<td>- Any OCC or OTS report of examination, supervisory correspondence, investigatory files, or internal agency memorandum;</td>
<td>and</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Any information provided to the CFPB by an entity to enable the CFPB to</td>
<td>- Confidential OCC or OTS information obtained by a third party;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Testimony from, or an interview with, an OCC or former OTS employee, officer, or agent; and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Confidential information relating</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>CFPB</td>
<td>OCC</td>
<td>FRB</td>
<td>FDIC</td>
</tr>
<tr>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Parties Authorized to Review or Receive CSI Without a Specific Request</strong></td>
<td>monitor for consumer risks or to assess whether an entity should be considered a covered person; and - Information that is exempt from disclosure pursuant to 5 U.S.C. § 552(b)(8). <em>See 12 C.F.R. § 1070.2(i)(1).</em></td>
<td>to operating and no longer operating regulated entities. <em>See 12 C.F.R. § 4.32(b).</em></td>
<td>FRB CSI may be disclosed only to the following entities: - Directors, officers, and employees of the regulated entity; - A parent bank holding company or parent savings and loan holding company and its directors, officers, and employees; - Certified public accountants and legal counsel; and - Other persons, with the prior written approval of the FRB. <em>See 12 C.F.R. § 261.20.</em></td>
<td>FDIC CSI may be disclosed only to the following entities: - Directors, officers, employees, or agents of the regulated entity who have a need for such records in the performance of their official duties; - External auditors; and - Other persons, with the prior written approval of the FDIC. <em>See 12 C.F.R. § 309.6.</em></td>
</tr>
<tr>
<td><strong>CFPB CSI</strong></td>
<td>CFPB CSI may be disclosed only to the following entities: - Directors, officers, trustees, members, general partners, or employees of the regulated entity; - Affiliates; - Directors, officers, trustees, members, general partners, or employees of its affiliates; - Certified public accountants, legal counsel, contractors, consultants, or other service providers; and - Another person, with the prior written approval of the CFPB. <em>See 12 C.F.R. § 1070.42(b).</em></td>
<td>&quot;Non-public OCC information&quot; may be disclosed only to the following entities: - Directors, officers, employees, or agents of the regulated entity; - A parent holding company and its directors, officers, or employees; Persons or organizations officially connected with the regulated entity as an attorney, auditor, independent auditor, or consultant; and - Other persons, with the prior written approval of the OCC. <em>See 12 C.F.R. § 4.37.</em></td>
<td><em>Non-disclosure agreements</em>: A regulated entity may not enter into third-party NDAs that attempt to: (1) restrict the entity from sharing certain information with the CFPB; or (2) require the entity to advise a third party when it shares with the CFPB information subject to an NDA. The CFPB warns that these agreements do not alter or limit the CFPB’s supervisory authority or an entity’s obligations relating to CSI. Copy and removal of CSI by directors and officers: It is a breach of fiduciary duty, and a violation of FDIC regulations, for directors and officers of a regulated entity to copy and remove CSI in anticipation of litigation or an enforcement action against that director or officer in his or her personal capacity. <em>See FDIC, FIL-14-2012 (Mar. 19, 2012).</em></td>
<td><em>Non-disclosure agreements</em>: A regulated entity may not enter into third-party NDAs that attempt to: (1) restrict the entity from providing information to FRB supervisory staff; (2) require an entity, without the prior approval of the FRB, to disclose that any information will be or was provided to FRB supervisory staff; or (3) require or permit the entity to inform a counterparty of a current or upcoming FRB examination or any copy and removal of CSI by directors and officers: It is a breach of fiduciary duty, and a violation of FDIC regulations, for directors and officers of a regulated entity to copy and remove CSI in anticipation of litigation or an enforcement action against that director or officer in his or her personal capacity. <em>See FDIC, FIL-14-2012 (Mar. 19, 2012).</em></td>
</tr>
</tbody>
</table>
### Process for Making a Specific Disclosure Request

<table>
<thead>
<tr>
<th>CFPB</th>
<th>OCC</th>
<th>FRB</th>
<th>FDIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>See CFPB, Compliance Bull. 2015-01 (Jan. 27, 2015).</td>
<td>nonpublic FRB supervisory initiative or action. See FRB, SR 07-19 (Dec. 13, 2007).</td>
<td>Entities seeking approval for CSI disclosures that are not specifically authorized by FRB regulation must submit a written request to the FRB's General Counsel at the following address: Legal Division, Board of Governors of the Federal Reserve System, 20th Street and Constitution Avenue, NW, Washington, D.C. 20551. Requests are approved on a discretionary basis. See 12 C.F.R. § 261.20.</td>
<td>Entities seeking approval for CSI disclosures that are not specifically authorized by FDIC regulation must submit a written request to the Director of the FDIC’s Division having primary authority over the records or information sought. Requests are approved on a discretionary basis. See 12 C.F.R. § 309.6(a).</td>
</tr>
</tbody>
</table>

### Supervisory Jurisdiction

<table>
<thead>
<tr>
<th>CFPB</th>
<th>OCC</th>
<th>FRB</th>
<th>FDIC</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CFPB supervises banks with more than $10 billion in assets, and certain nonbank financial entities including mortgage-related firms, private student lenders, payday lenders, and certain other large nonbank consumer financial entities, including debt collection agencies, debt relief firms, consumer finance and similar companies, prepaid card issuers, credit card products, credit reporting agencies, and mobile payment providers.</td>
<td>The OCC supervises national banks and federally chartered savings associations.</td>
<td>The FRB supervises bank holding companies and their nonbank subsidiaries, financial holding companies, savings and loan holding companies, any firm designated as systemically significant by the Financial Stability Oversight Council (“FSOC”), and state banks that are members of the Federal Reserve System.</td>
<td>The FDIC supervises federally insured depository institutions, including state banks and savings associations that are not members of the Federal Reserve System.</td>
</tr>
</tbody>
</table>

### A. The CFPB

The CFPB’s recent CSI Bulletin reviews the existing legal framework for CFPB-regulated entities and articulates a new, and arguably more controversial, position regarding the treatment of CSI and third-party NDAs. Generally, under CFPB rules, any regulated entity lawfully in the possession of CFPB CSI may disclose the information to its directors, officers, trustees, members, general partners, or employees, or its affiliates and their directors, officers, trustees, members, general partners, or employees, to the extent that the disclosure is relevant to the performance of each individual’s...
assigned duties. A regulated entity may also disclose CSI to its certified public accountant, legal counsel, contractor, consultant, or other service provider, as long as the recipient does not utilize, make, retain copies of, or disclose the CSI for any purpose, except as is necessary to provide advice or services to the regulated entity or its affiliate. A regulated entity wishing to disclose CSI to any other party must obtain the prior written approval of the CFPB.

1. **Scope of CFPB CSI**

Compared to other regulatory agencies, the CFPB imposes a more extensive definition of what constitutes CSI upon its supervised entities. CFPB CSI includes all of the following:

- Reports of examination, inspection and visitation, non-public operating, condition and compliance reports, and any information contained in, derived from, or related to such reports;
- Any documents, including reports of examination, prepared by, on behalf of, or for the use of the CFPB or any other federal, state, or foreign government agency in the exercise of supervisory authority over a financial institution, and any information derived from such documents;
- Any communications between the CFPB and a regulated entity or a federal, state, or foreign government agency related to the CFPB’s supervision of the institution;
- Any information provided to the CFPB by a financial institution to enable the CFPB to monitor for risks to consumers in the offering or provision of consumer financial products or services, or to assess whether an institution should be considered a covered person, as that term is defined by 12 U.S.C. § 5481, or is subject to the CFPB’s supervisory authority; and
- Information that is exempt from disclosure pursuant to 5 U.S.C. § 552(b)(8).

The CFPB’s CSI Bulletin provides a “non-exhaustive” list of CSI examples, which includes CFPB examination reports and supervisory letters, all information contained in, derived from, or related to those documents (including an institution’s supervisory compliance rating), all communications between the CFPB and a regulated entity related to an examination of the institution or other supervisory activities, supervisory requests for information from the CFPB to the regulated entity, and the institution’s response, memoranda of understanding, and any related submissions and correspondence, and any other information created by the CFPB in the exercise of its supervisory authority (including workpapers and other documentation prepared by CFPB examiners in preparation for an examination).

Notwithstanding the CFPB’s broad reach, documents are not deemed CSI if they are prepared by a financial institution for its own business purposes and the documents are not in the possession of the CFPB.
2. **CFPB Guidance Regarding NDAs**

Addressing an issue that raises somewhat unique and challenging issues for formerly unregulated nonbank financial firms, the CSI Bulletin discusses the treatment of information subject to NDAs between regulated entities and third parties. The CFPB recognizes that some entities may have existing NDAs that intended to prevent the institution from sharing certain information with a supervisory agency, or require it to advise a third party when the institution provides certain information to a supervisory agency.\(^{10}\) As the CSI Bulletin notes, such NDAs do not alter an institution’s existing obligation to keep CSI confidential, nor do they alter or limit the CFPB’s supervisory authority.\(^{11}\) The CSI Bulletin warns that, should a regulated entity rely on the provisions of an NDA to justify disclosing CSI in a manner not otherwise permitted by law, the CFPB will pursue all available remedies to enforce the requirements of law, including the possible imposition of monetary penalties.\(^{12}\)

**B. The OCC (National Banks and Federal Savings Associations)**

In contrast, the OCC prohibits the unauthorized disclosure of CSI by national banks and federal savings associations.\(^{13}\) Generally, all “non-public OCC information” remains the property of the OCC and is deemed confidential and privileged.\(^{14}\) Specifically, “[n]o supervised entity, government agency, person, or other party to whom the information is made available, or any officer, director, employee, or agent thereof, may disclose non-public OCC information without the prior written permission of the OCC.”\(^{15}\) Furthermore, except as authorized by the OCC, no person obtaining access to non-public OCC CSI may make a copy of such information or remove the information from the premises of the regulated institution, agency, or other party in authorized possession of the information.\(^{16}\)

There are several notable exceptions to the OCC’s general prohibition on the disclosure of CSI. For example, non-public OCC CSI can be released if it is published in “statistical material that does not disclose, either directly or when used in conjunction with other publicly available information, the affairs of any individual, corporation, or other entity.”\(^{17}\) When necessary or appropriate for business purposes, the OCC also allows a national bank, federal savings association, holding company, or any of their directors, officers, or employees to disclose non-public OCC CSI, including information contained in, or related to, OCC reports of examination, to “a person or organization officially connected with the bank or federal savings association as officer, director, employee, attorney, auditor, or independent auditor.”\(^{18}\) The aforementioned persons or entities may also release non-public OCC CSI to a consultant if the consultant is under a written contract to provide services to the bank or federal savings association and has a written agreement that (1) states its awareness of, and agreement to comply with, the prohibition on the dissemination of non-public OCC CSI, and (2) agrees not to use the non-public OCC CSI for any purpose other than as provided under its contract to provide services to the bank or federal savings association.\(^{19}\)

1. **Scope of OCC CSI**

Under OCC regulations, “non-public OCC information” encompasses OCC CSI and includes any record created or obtained “by the OCC in connection with the performance of its responsibilities, such as a record concerning supervision, licensing, regulation, and examination of a national bank, a federal savings association, a federal branch or agency of a foreign bank, a federal savings and loan association, a federal savings and loan holding company, or a bank insurance company.”\(^{20}\) Generally, all “non-public OCC information” remains the property of the OCC and is deemed confidential and privileged.
savings association, a bank holding company, a savings and loan holding company, or an affiliate."20
Any record created or obtained by the Office of Thrift Supervision ("OTS") in connection with the performance of its responsibilities is also covered.21 Other forms of OCC CSI include the following:

- Any record compiled by the OCC or the OTS in connection with either agency’s enforcement responsibilities;
- Any report of examination, supervisory correspondence, investigatory file compiled by the OCC or OTS in connection with an investigation or internal agency memorandum, whether the information is in the possession of the OCC or some other individual or entity;
- Confidential OCC information obtained by a third party or otherwise incorporated in the records of a third party, including another government agency;
- Testimony from, or an interview with, a current or former OCC or OTS employee, officer, or agent concerning information acquired by that person in the course of his or her performance of official duties with the OCC or OTS or due to that person’s official status at the OCC or OTS; and
- Confidential information relating to operating and no longer operating national banks, federal savings associations, and savings and loan holding companies as well as their subsidiaries and affiliates.22

OCC CSI does not include information that the OCC is required to release under the Freedom of Information Act or that the OCC has published or made available, including final orders and other agreements.23

C. The Federal Reserve Board (Holding Companies, Nonbank Affiliates, and State Member Banks)

An entity regulated by the FRB that is in lawful possession of FRB CSI may only disclose such information to its directors, officers, and employees, its parent holding company or bank, or its directors, officers, and employees.24 An FRB-regulated entity may also disclose FRB CSI to its certified public accountant or legal counsel, subject to certain conditions of confidentiality.25 Other disclosures may be made only if the regulated entity requests and receives prior written authorization from the FRB to make the requested disclosure.26

1. Scope of FRB CSI

The FRB defines CSI to include “reports of examination, inspection and visitation, confidential operating and condition reports, and any information derived from, related to, or contained in such reports,” as well as “[i]nformation gathered by the [FRB] in the course of any investigation, suspicious activity report, cease-and-desist orders, civil money penalty enforcement orders, suspension, removal or prohibition orders, or other orders or actions.”27 FRB CSI also includes “[a]ny documents prepared by, on behalf of, or for the use of the [FRB], a Federal Reserve Bank, a federal or state financial institutions supervisory agency, or a bank or bank holding company or other supervised financial

Except in very limited circumstances, banking organizations are prohibited from disclosing their CAMELS rating and other CSI to insurers or non-related third parties without the express permission of the FRB.
institution.” The FRB has also emphasized that a first-day letter sent by a Federal Reserve Bank to a financial institution in anticipation of an examination, as well as an institution’s response to such a letter, is FRB CSI. Further guidance clarifies that “reports of examination or inspection—whether prepared solely by the [FRB] or jointly with a federal or state supervisory agency—are confidential, as is all information contained in such reports, including an institution’s supervisory rating, such as BOPEC, CAMELS or ROCA.” Regulated entities should be particularly wary of requests from insurers who seek the disclosure of their CAMELS rating during the underwriting process for directors and officers liability coverage. Except in very limited circumstances, banking organizations are prohibited from disclosing their CAMELS rating and other CSI to insurers or non-related third parties without the express permission of the FRB. Finally, information related to any non-public enforcement action, such as memoranda of understanding between a Federal Reserve Bank and an institution, is also confidential.

2. FRB Guidance Regarding NDAs

Similar to the CFPB, the FRB has issued guidance clarifying its expectations regarding NDAs between banking organizations and their counterparties or other third parties. The corresponding FRB supervision and regulation letter emphasizes that it is contrary to FRB regulation and policy for agreements to contain confidentiality provisions that do any of the following:

- Restrict a banking organization from providing information to FRB supervisory staff;
- Require or permit, without the prior approval of the FRB, a banking organization to disclose to a counterparty that any information will be or was provided to FRB supervisory staff; or
- Require or permit, without the prior approval of the FRB, a banking organization to inform a counterparty of a current or upcoming FRB examination or any nonpublic FRB supervisory initiative or action.

D. The FDIC (State Nonmember Banks and State Savings Associations)

Finally, under the rules and regulations of the FDIC, so-called “exempt records” or any CSI contained in such records may not be released to “any persons other than those officers, directors, employees, or agents of the [FDIC] who have a need for such records in the performance of their official duties.” While external auditors are permitted to have access to the exempt records relating to depository institutions under audit, regulated entities and their auditors should note that the “information contained in all examination reports, inspection reports, and supervisory discussions—including any summaries or quotations—is CSI and must not be disclosed to any other party without the written permission of the FDIC. Unauthorized disclosure of confidential supervisory information may subject the auditor to civil and criminal actions and fines and other penalties.” Furthermore, even where a regulated entity has possession, custody, or control over FDIC-exempt records or information, all copies of such records remain the property of the FDIC. Thus, except in very limited circumstances, regulated entities may not disclose any exempt record or make public any exempt information without the prior written permission of the FDIC.
1. **Scope of FDIC CSI**

Under the rules and regulations of the FDIC, "exempt records" include "[r]ecords that are contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of the FDIC or any agency responsible for the regulation or supervision of financial institutions." The FDIC interprets the definition of exempt records broadly, extending confidentiality to FDIC reports of examination, supervisory correspondence (including letters, directives, responses to reports of examination, appeals of supervisory determinations, and other FDIC supervisory correspondence), as well as suspicious activity reports.

2. **FDIC Guidance Regarding the Copying and Removal of CSI by Directors and Officers**

The FDIC has also issued guidance regarding the copying and removal of CSI by directors and officers of FDIC-supervised entities. Specifically, the FDIC has observed a limited number of instances where directors and officers of troubled or failing entities have made copies of CSI and then removed such copies from the institution in anticipation of litigation or an enforcement action against them personally. As the FDIC guidance notes, this activity is a de facto breach of the fiduciary duty a director or officer owes to the institution, and also constitutes "an unsafe and unsound banking practice, which may also violate applicable laws and regulations and contravene the financial institution’s information security program." Regulated entities, particularly institutions in troubled condition or subject to increased supervisory scrutiny, should understand the full parameters of the FDIC guidance. Institutions should also take heed of the FDIC’s intention to investigate such breaches to pursue possible enforcement actions, civil money penalties, and/or criminal sanctions.

E. **Potential Issues with Overlapping CSI Requirements and Supervisory Jurisdiction**

As noted above, the CFPB takes the position that CFPB CSI includes any documents prepared by, on behalf of, or for the use of the CFPB or any other federal, state, or foreign government agency in the exercise of supervisory authority over a regulated entity, including other agencies’ reports of examination, and any information derived from such documents. Thus, it appears that the CFPB takes the view that documents or other information prepared by another supervisory authority that constitutes such other agency’s CSI also qualifies as CFPB CSI notwithstanding that such information is entirely and exclusively subject to a privilege that belongs to another agency and that only such other agency may waive. Moreover, it does not appear that the CFPB is asserting this broad authority based on a CFPB supervisory interest in the other agency’s CSI or that the CSI must be related to CFPB supervision (although this may be implied). Thus, this creates a difficult issue of overlapping CSI requirements and supervisory jurisdiction between the CFPB and a prudential regulator such as the OCC, FRB, or FDIC, all of which have strident views regarding the protection of CSI that arises from their own bank examination reporting privilege.

Accordingly, institutions and financial firms that find themselves in circumstances in which the CFPB is seeking to exercise some degree of authority to obtain CSI or control the disclosure of CSI that arises from supervisory information obtained from a prudential federal banking regulator would be wise to exercise a significant degree of caution in handling the situation. At a minimum, the regulated entity should ensure that the prudential regulator is fully engaged regarding the circumstances, and the regulated entity may even deem it appropriate to have a three-party conversation with both the prudential regulator and the CFPB in instances in which the CFPB seeks to assert its own privilege for
the release of CSI jointly claimed by both regulators. This would be the case, for example, where a regulated entity seeks to release certain CSI of its prudential regulator that the CFPB seeks to block. Alternatively, circumstances could arise in which the CFPB seeks to release CSI that is claimed, in whole or in part, as the CSI of one of the prudential regulators without the CFPB obtaining the clear authorization or consent of the prudential regulatory agency to do so. For example, a particular point of concern and potential contention could be the handling of NDAs requiring or restricting the sharing of CSI jointly claimed by the CFPB and a prudential federal bank regulator. Again, a regulated entity should seek to facilitate an open dialogue with both regulators to avoid being placed in a difficult situation regarding the release of or restrictions on CSI, as well as the entity’s own use of CSI claimed by both regulators.

II. Action Plan

While the aforementioned policies and regulations regarding the handling of CSI are not new to banks and other traditionally regulated financial entities subject to federal oversight, the CFPB’s definition of CSI and the agency’s specific restraints on the dissemination of CSI to third parties may be unfamiliar to nonbank entities regulated by the CFPB. Similarly, while banks are familiar with the handling of CSI, new territory for banks created by the CFPB’s CSI Bulletin involves potential issues with overlapping CSI requirements and supervisory jurisdiction of the prudential federal banking regulators and the CFPB for jointly-claimed CSI. As the CSI Bulletin makes clear, the CFPB has placed a renewed emphasis on compliance with CSI disclosure prohibitions and procedures; thus, a real potential for confusion may emerge among both banks and nonbank financial firms with respect to the handling of CFPB CSI. While the CSI Bulletin technically serves as “nonbinding guidance” to banks, savings associations, and credit unions with assets over $10 billion, as well as other nonbank businesses subject to the CFPB’s jurisdiction (e.g., certain payday lenders, private education lenders, large consumer reporting agencies, debt collectors, student loan services, international remittance providers, and mortgage companies), noncompliance with any of the CSI-related regulations may constitute a “violation of law.” Thus, regulated entities facing these standards of confidentiality—or issues regarding overlapping CSI requirements—for the first time should take special care to review the applicable regulations and bring their practices into compliance, as well as reach out to their regulators or counsel, as appropriate, to seek clarification regarding how to handle various situations involving the disclosure or non-disclosure of CSI.

Based on the CSI Bulletin, there are a number of action items that banks and nonbank financial firms should consider when reviewing their internal controls and risk management procedures for CSI compliance. To avoid a formal supervisory action and the imposition of civil money penalties, regulated entities should, at a minimum, consider the following action items:

• Review and understand the types of information that constitute CSI for both their prudential federal banking regulator(s) and the CFPB, and the corresponding laws, rules, regulations, and available guidance related to the disclosure and non-disclosure of CSI to third parties;

• Review and analyze how the regulated entity currently manages CSI in its possession, custody, or control, how such information is maintained and categorized, and whether there are any gaps in compliance monitoring programs and procedures;
• Evaluate all persons with access to CSI at the regulated entity, and determine whether the level of access to CSI of each person is commensurate with their role, job function, and responsibility within the organization;

• Review and update, as appropriate, board of directors, management, and staff training regarding the handling, sharing, disclosure, and nondisclosure of CSI, including training that may be appropriate to highlight issues of overlapping jurisdiction between a prudential regulator and the CFPB;

• Review and revise existing policies, procedures, and internal controls in place to prevent the inadvertent sharing of CSI, including procedures for reporting to regulators if any CSI is inadvertently released; and

• Review all existing NDAs between the institution and third parties for any confidentiality provisions contrary to CFPB regulation and policy, as well as the requirements imposed on the sharing of CSI by a prudential bank regulator.

Regardless of the circumstances, if there is doubt regarding the handling of CSI, a regulated entity should seek appropriate guidance in assessing the disclosure requirements and risks of a particular course of action, as well as the extent to which such course of action could expose potential vulnerabilities in the entity’s policies, procedures, and internal controls regarding the handling of CSI.

* * * * *

Paul Hastings attorneys are actively working with clients to identify and address issues related to CSI disclosure and nondisclosure issues and potential CFPB investigations, as well as to assist clients in reviewing and maintaining robust compliance policies and programs with respect to the handling of CSI.

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

**Atlanta**

Todd W. Beauchamp  
1.404.815.2154  
toddbeauchamp@paulhastings.com

Chris Daniel  
1.404.815.2217  
chrisdaniel@paulhastings.com

Erica Berg Brennan  
1.404.815.2294  
ericaberg@paulhastings.com

Heena A. Ali  
1.404.815.2393  
heenaali@paulhastings.com

Kevin P. Erwin  
1.404.815.2312  
kevinerwin@paulhastings.com

Meagan E. Griffin  
1.404.815.2240  
meagangriffin@paulhastings.com

Diane Holden  
1.404.815.2326  
dianeheldon@paulhastings.com

**London**

Michelle Duncan  
44.20.3023.5162  
michelleduncan@paulhastings.com

Justin S. Jowitt  
44.20.3023.5163  
justinjowitt@paulhastings.com

Stephen Parker  
44.20.3023.5168  
stephenparker@paulhastings.com

Ben Regnard-Weinrabe  
44.020.3023.5183  
benregnardweinrabe@paulhastings.com

Hanna Keever  
44.20.3023.5183  
hannahkeeever@paulhastings.com

2 The National Credit Union Administration ("NCUA") also prohibits the disclosure of CSI except in limited circumstances. See 12 C.F.R. § 792.11 (outlining the type of records that are confidential, privileged and exempt from public disclosure); 12 CFR 792.11; 12 C.F.R. § 792.30 (noting that no officer, employee or agent of a federally-insured credit union may disclose or permit the disclosure of any NCUA exempt record to any person other than authorized NCUA or credit union officers, employees or agents for the performance of their official duties).


4 12 C.F.R. § 1070.42(b).

5 12 C.F.R. § 1070.42(b)(2)-(3).

6 12 C.F.R. § 1070.42(b)(2)(ii).

7 12 C.F.R. § 1070.2(i)(1).


9 12 C.F.R. § 1070.2(i)(2).

10 Id.

11 Id.

12 Id.; see also 12 U.S.C. § 5536(a)(2) (making it unlawful for a regulated entity "to fail or refuse, as required by Federal consumer financial law, or any rule or order issued by the CFPB thereunder—(A) to permit access to or copying of records; . . . or (C) to make reports or provide information to the Bureau").

13 12 C.F.R. § 4.36(d).

Paul Hastings LLP

StayCurrent is published solely for the interests of friends and clients of Paul Hastings LLP and should in no way be relied upon or construed as legal advice. The views expressed in this publication reflect those of the authors and not necessarily the views of Paul Hastings. For specific information on recent developments or particular factual situations, the opinion of legal counsel should be sought. These materials may be considered ATTORNEY ADVERTISING in some jurisdictions. Paul Hastings is a limited liability partnership. Copyright © 2015 Paul Hastings LLP.
13 12 C.F.R. § 4.36(b).
14 Id.
15 Id.
16 12 C.F.R. § 4.36(b)(2).
17 Id.
19 Id.
21 Id.
22 12 C.F.R. § 4.32(b)(1).
23 Id.
24 12 C.F.R. § 261.2(b).
25 12 C.F.R. § 261.20(b). (certified public accountants or legal counsel may review CSI only on the premises of the regulated entity and may not make or retain any copies of the information, nor may they disclose the CSI for any purpose without the prior written approval of the FRB's General Counsel except as necessary to provide advice to the regulated entity, its parent bank holding company, or the directors, officers and employees of the regulated entity and parent bank holding company).
26 12 C.F.R. § 261.20(g).
27 12 C.F.R. § 261.2(c)(1)(i)–(ii).
28 12 C.F.R. § 261.2(c)(1)(iii).
30 Id.
32 The OCC and FDIC take a similar view with respect to the disclosure of examination and similar supervisory ratings.
35 Id.
36 12 C.F.R. § 309.6(a).
38 12 C.F.R. § 309.6(a).
39 Id.
40 12 C.F.R. § 309.5(g)(8).
42 See id.