



Financial Services & Products ADVISORY ■

APRIL 15, 2021

Avoiding Pitfalls During Post-Pandemic Government Investigations

by [*Sanford Brown*](#), [*Cliff Stanford*](#), and [*Brendan Clegg*](#)

As the country begins to emerge from the COVID-19 pandemic and the U.S. economy gets back on track, banks nationwide should expect their activities to come under government scrutiny. The impacts of the coronavirus have touched every corner of the banking industry as institutions have striven to meet the evolving needs of their customers, continue operations in a remote working environment, and stand up new programs in response to government relief efforts, such as the Coronavirus Aid, Relief, and Economic Security (CARES) Act. With 2020 in the rearview mirror, banks' efforts to balance these challenges during a year of unprecedented changes will be put under the microscope as their compliance with an ever-expanding list of laws and regulations is assessed by regulators. The conduct of banks' management, service providers, and even customers will likewise be reviewed.

New leaders installed by the Biden Administration atop the federal banking and securities agencies are certain to take a different approach to enforcement from their predecessors. As if the alphabet soup of federal agencies were not enough, state-level financial supervisors and attorneys general will also be eyeing institutions within their borders. For serious misconduct, the threat of prosecution by the Department of Justice (DOJ) and U.S. attorneys across the country looms.

Many banks may find themselves in the crosshairs as 2021 progresses, as their conduct—or that of their officers and directors, partners, or clients—become the subject of formal inquiries. As detailed in recent press reports, investigations are already progressing into dozens of fraud schemes that siphoned off millions of dollars from taxpayer-funded programs designed to alleviate the devastating effects of the pandemic. Investigations may begin with a subpoena, request for documents, or compliance examination, and reviews by multiple agencies may or may not be coordinated. Some conduct may be referred between agencies with overlapping jurisdiction, but parallel investigations may spawn organically—for example, from customer complaints or whistleblower reports.

The prospect of parallel government investigations raises a number of complex issues for banks to grapple with, entirely separate from any fallout from the investigated conduct. In normal times, banks may rarely encounter situations where these laws and regulations are implicated. But within the context of fast-moving and sensitive investigations, a bank's failure to comprehend and proactively address these issues may cause them legal headaches that plague them long after the investigations are resolved.

This alert is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

Overview

Banks may find themselves in difficult positions as they navigate between pleasing two or more agencies operating with divergent agendas, priorities, and expectations. In the usual course, institutions under government subpoena expend significant effort to produce documents and information in a timely manner, hoping to engender goodwill with the agency. While doing so, a failure to appreciate the significance of regulations could damage relationships with the regulators. Conversely, the consequences of complying—which may mandate providing notice to the regulators or requesting permission—could bring another set of prying eyes.

Confidential Supervisory Information

A government agency subpoena may be broad enough to compel production of a bank's prudential regulator's confidential supervisory information (CSI). Depending on whether a bank is regulated by the Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (FRB), or Federal Deposit Insurance Corporation (FDIC), the scope of information covered by the term CSI differs. (The agencies' definitions of CSI can be found at 12 C.F.R. § 4.32(b) (OCC), § 261.2(b) (FRB), and § 309.5(g)(8) (FDIC).) The Consumer Financial Protection Bureau (CFPB) also has its own definition of CSI at § 1070.2(f). State-chartered banks may find their states use still another CSI definition. Regardless of the exact contours of each CSI definition, all the federal bank regulators take their regulations around disclosure of CSI very seriously, and failure to strictly comply with them can quickly land a bank in hot water.

In general, the federal bank regulators consider CSI to be property of the respective agency and view the term as encompassing records created by the agencies in the course of their supervision of a regulated institution. Thus, the term includes reports of examination or condition, supervisory correspondence or communications, and investigatory requests and files. To get a leg up on their investigations, other regulatory agencies request the records of a bank's prudential regulator documenting prior criticism, compliance deficiencies, or legal violations. However, banks cannot simply turn over those records just because they are the subject of a subpoena.

Even if banks are generally aware of restrictions on sharing this "core" CSI, they may not be aware that the tentacles of the CSI definitions may reach far beyond agency documents. For example, the OCC considers CSI to include records not only created by the OCC, but "obtained by" the OCC in connection with the performance of its responsibilities. The FRB defines CSI as not just information created in furtherance of the Board's activities, but any information "derived from or related to such information." As these examples make clear, even documents printed on a regulator's letterhead—or transmitted back to the agency by the bank—may be CSI.

After determining the scope of a regulator's CSI definition, banks need to follow certain procedures to obtain disclosure approval if they intend to produce that CSI. The regulators generally require written permission from the agency before an institution can disclose CSI to a third party. For reasons entirely beyond an institution's control, the approval process for such requests may be held up or blocked, potentially leaving the bank to explain to another agency why its production obligations cannot be met. In addition, a request to disclose CSI to another government agency—for example, the DOJ—could prompt the regulator to question why the DOJ is seeking the records in the first place. Facing pressure to comply with an outstanding subpoena, banks may be hard-pressed to play the role of the middle man, explaining the restrictions around CSI disclosure and the regulatory hurdles to transmission to another agency unfamiliar with the concept or unsympathetic to the institution's plight. Under their regulations, the banking agencies may also implement conditions on the recipients of disclosed CSI—including sister agencies within the federal government—that the recipients in turn view as detrimental to their investigation.

Suspicious Activity Reports

Another disclosure quandary banks may face during parallel investigations relates to the production of suspicious activity reports (SARs). SARs are designed to provide useful information to law enforcement related to potential illicit conduct, and banks are required to file SARs under the Bank Secrecy Act (BSA). While each banking regulator has its own implementing regulations governing when SARs must be filed—and the Treasury agency responsible for administering the BSA, the Financial Crimes Enforcement Network (FinCEN), has its own requirements applicable to banks—institutions routinely file SARs related to suspicious activity even when these parameters for filing are not met. (Those regulations can be found at 12 C.F.R. § 21.11 (OCC), § 208.62 (FRB), § 353.3 (FDIC), and 31 C.F.R. § 1020.320 (FinCEN).)

Because SARs provide pertinent information collected by financial institutions about suspicious activity—often including customer names, addresses, transactional data, account numbers, and account history—SARs could serve as a natural starting point for other regulatory agencies, including prosecutors, opening an investigation. However, SARs are subject to a very strict disclosure regime: not only are banks generally prohibited from disclosing the SARs themselves, but banks also may not disclose “any information that would reveal the existence of a SAR.” Information that would reveal the existence of a SAR can appear in all types of routinely created internal bank documents. One common example—and often a subject of initial subpoenas from regulators to unfamiliar companies—are board minutes. These records often record presentations from bank officers updating directors on, among other things, the number of SARs filed in a given month, the specific activities of a customer prompting a SAR filing, or the resolution of a matter where a SAR was filed. Thus, even records normally deemed low-hanging fruit for subpoena production may need to be reviewed before those records can be dumped en masse.

FinCEN’s regulation contains a significant exception allowing banks to disclose SARs or SAR-related information to FinCEN, to any “Federal, State, or local law enforcement agency,” or to certain federal or state regulators, if those regulators “examine[] the bank for compliance with” the BSA or administer a state law that requires the bank to comply with the BSA. While this language seems to absolve banks from the need to do a thorough scrub before producing to many agencies, including the DOJ, the exception may not be broad enough to cover other investigatory agencies conducting a parallel civil investigation. This distinction is important because it could leave out, for example, the Securities and Exchange Commission or the Small Business Administration, which implemented the Paycheck Protection Program passed as part of the CARES Act, or offices of inspectors general from various federal agencies.

Moreover, although FinCEN provides an exception, some of the banking agencies’ regulations do not. For example, the FRB’s SAR regulation requires member banks to decline to produce SARs or related information, and to notify the FRB of a request for SARs, without the qualifying language found in FinCEN’s regulation. Beyond causing issues with the agency issuing the subpoena—which, as with CSI, may have a limited understanding of the disclosure restrictions attendant to SARs—sending notice to a regulator that there is an investigation into suspicious activity at a bank may lead the regulator to itself dig in.

Attorney-Client Privilege

In a concept foreign to many outside the banking world, the federal bank regulators, as well as the CFPB, take the position that they can compel their regulated institutions to disclose information that would otherwise be protected by attorney-client privilege and the work product doctrine. The banking agencies maintain this power derives from their plenary statutory authority to examine and supervise these institutions and to access their books and records. Requests for privileged materials necessarily puts banks in a bind, since refusing to comply with the demand can mar the relationship with examiners or, worse still, lead to a separate, formal investigation—through which the agencies

will obtain the information anyway. However, turning over privileged material—for example, a privileged report from an internal investigation conducted by outside counsel—could provide a roadmap to misconduct.

Compelled disclosure by the federal bank regulators, however, does not render any privileges attached to those documents waived. Under federal statute, 12 U.S.C. § 1828(x), the submission of information to the federal bank agencies, CFPB, or state bank supervisors “in the course of any supervisory or regulatory process” shall “not be construed as waiving, destroying, or otherwise affecting any privilege” the bank may claim under federal or state law as to any other third party. This statutory provision ensures that banks can still maintain all privileges under federal or state law against third parties seeking this information, which has important implications not just for private parties that may file litigation against the banks down the road but also against other government agencies seeking disclosure in a parallel investigation.

Many, if not all, government agencies beyond the federal banking agencies do not attempt to compel outright production of privileged documents via their subpoena power; rather, they contemplate the submission of a privilege log. However, a government agency trying to maintain pace with a bank regulator may embed within its subpoena a request for all documents produced as part of any other related government investigation. While banks will acquiesce to their regulators’ demands for privileged documents, they cannot produce these same documents to other government agencies without waiving the attached privileges because Section 1828(x) offers no protection for disclosure to departments outside the section’s scope. Failure to maintain the privilege against these other agencies—even if waiver engenders goodwill by putting them on equal footing with the bank regulator—could have significant negative repercussions down the road if the bank becomes the target of a shareholder derivative lawsuit or a class action. But maintaining the privilege—and explaining why productions to the two agencies will not be equal—may further drive a wedge between the bank and the investigator.

Even if the bank goes to great lengths to ensure that privileged information shared with its regulator is withheld from a parallel investigation, other agencies can still obtain the information. Under another federal statute, 12 U.S.C. § 1821(t), bank regulators’ sharing of privileged information received from regulated institutions with other government agencies is explicitly contemplated. The backstop provided by this statute is, again, a protection ensuring that the transfer between agencies does not waive attached privileges. But even if the privilege remains, the regulators’ sharing of the privileged documents could produce key evidence later used against the bank. In addition, Section 1821(t)’s vaguely worded scope may be subject to a later determination that the receiving agency is not covered by the anti-waiver provision, rendering the privilege waived—through no fault of the bank.

Conclusion

Of course, the complex nature of defending parallel investigations may trigger a host of other issues. For example, executives may be subpoenaed for testimony by multiple agencies, presenting the possibility for conflicting or contradictory sworn statements. If matters related to an investigation get in front of a court, federal bank examiners may assert the “bank examination privilege,” a federal common-law evidentiary privilege, as an intervening third party, shielding disclosure of examiners’ opinions or recommendations that may be exculpatory or beneficial to the institution. To qualify for an exemption from disclosure to third parties under the federal Freedom of Information Act, produced documents need special labels and must be produced alongside explicit language requesting confidential treatment, but the scope of such language may differ depending on who is receiving the information. Finally, if the company is publicly traded, navigating how and when to disclose parallel government investigations in public filings can be a thorny issue to navigate.

Adding to the complexity, the various regulations governing disclosure often contain nuances around who within the organizational umbrella can receive certain information, or whether third parties—including those conducting internal investigations or assisting with the banks' defense against the government—can receive that information without a regulator's blessing. In the course of a fast-moving, high-stakes investigation, bank management may not be contemplating these restrictions as they share information to help with damage control.

As the pace and volume of government investigations and examinations pick up during the Biden Administration, we expect that many banks may be confronted by the prospect of parallel investigations, even if their own conduct is not the subject of a government agency. Each issue carries significant ramifications and could expose the bank to civil or criminal liability.

You can subscribe to future *Financial Services & Products* advisories and other Alston & Bird publications by completing our [publications subscription form](#).

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any member of our [Financial Services & Products Group](#).

Sanford M. Brown
214.922.3505
sanford.brown@alston.com

Brendan Clegg
202.239.3237
brendan.clegg@alston.com

Clifford S. Stanford
404.881.7833
cliff.stanford@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2021

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghai Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Level 20 Bastion Tower ■ Place du Champ de Mars ■ B-1050 Brussels, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333