FEBRUARY 2021

Policies and Procedures Manual

Office of Enforcement | Version 3.2

Statement of Purpose

This Enforcement Policies and Procedures Manual is the source for policies governing the work of the Consumer Financial Protection Bureau (Bureau) Office of Enforcement. No other document, email, or statement is a policy of the Office of Enforcement.

Once approved, new or revised policies will be incorporated into the Manual, the official copy of which is found on SharePoint at:

(b)(7)(E)

The Manual will be periodically updated. Suggestions for corrections or revisions should be submitted to the Enforcement Chief of Staff.

The Policies and Procedures Manual provides internal guidance to Enforcement staff of the Bureau. It does not bind the Bureau and does not create any rights, benefits, or defenses—substantive or procedural—that are enforceable by any party in any manner. While every effort has been made to ensure accuracy, these policies and procedures should not be relied on as a legal reference. Nor do they restrict the Bureau's discretion in exercising its authorities or limit its otherwise lawful investigative or litigation prerogatives.

Table of Contents

Part 1:
Office Policies

Part 2:
Practice Guidance

Part 3:
Administrative Policies.....

Part 1: Office Policies

Definitions

AG contact	The individual on the Enforcement Policy and Strategy Team assigned to maintaining state attorney general relationships
ALD	Assistant Litigation Deputy
ARC	Action Review Committee
AUSA	Assistant United States Attorney
AWS	Alternative Work Schedule
BSA or Bank Secrecy Act	The Currency and Foreign Transactions Reporting Act of 1970
Bureau	Consumer Financial Protection Bureau
CFPA	Consumer Financial Protection Act
CFTC	Commodity Futures Trading Commission
CID	Civil Investigative Demand
CII	Confidential Investigative Information
CMP	Civil Money Penalty
COR	Contracting Officer's Representative
CSI	Confidential Supervisory Information
Database	Law Enforcement Leads Database
Dodd-Frank Act	Dodd-Frank Wall Street Reform & Consumer Protection Act
DOJ	Department of Justice
DSS	Document Submission Standards
DUNS	Data Universal Numbering System
EAP	Enforcement Action Process
ECF	Electronic Case Filing

ECOA	Equal Credit Opportunity Act
ECPA	Electronic Communications Privacy Act
ECS	Electronic Communication Service
Enforcement Personnel	All Office of Enforcement employees
ESI	Electronically Stored Information
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FOIA	Freedom of Information Act
FRB	Federal Reserve Board
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
GPRA	Government Performance and Results Act
Housekeeping Rule	Rule on Disclosure of Records and Information
IGA	Bureau Office of Inter-Governmental Affairs
IGCE	Independent Government Cost Estimate
LD	Litigation Deputy
Legal	Legal Division
MMS	Matter Management System (ENForce)
MOU	Memorandum of Understanding
NCUA	National Credit Union Association
NDA	Non-Disclosure Agreement
NORA	Notice and Opportunity to Respond and Advise
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General

OSP	Office of Supervision Policy
Persons	People and Entities
PIFI	Personally Identifiable Financial Information
PII	Personally Identifiable Information
PST	Enforcement Policy and Strategy Team
PST Deputy	Deputy Enforcement Director for Policy and Strategy
QPR	Quarterly Performance Review
RAM	Recommendation for Assignment of a Matter
RFPA	Right to Financial Privacy Act
RMR	Research, Markets, and Regulations Division
ROE	Report of Examination
SAM	System for Award Management
SAR	Suspicious Activity Report
SBREFA	Small Business Regulatory Enforcement Fairness Act of 1996
SCA	Stored Communications Act
SEC	Securities and Exchange Commission
SEFL	Supervision, Enforcement, Fair Lending
SES	Supervision and Examination System
SL	Supervisory Letter
Staff	Enforcement Attorneys
T&I	Bureau Office of Technology and Innovation
TRO	Temporary Restraining Order
USAO	United States Attorney's Office

Enforcement Style Guide

The following style guidance applies to documents prepared in the Bureau's Office of Enforcement:

- 1" margins
- 12pt Georgia Font (including for footnotes)
- Single space after a period
- Single-line spacing
- Space created between paragraphs and at the end of a section
    - When finished with a paragraph press enter, enter
    - Do not use Word's tool to add space before and after a paragraph
- Tab to start new paragraph
- No indent for section headings
- Bolded section headings
- Align text left (not fully justified)
- Footnotes, not endnotes
- Use "Bureau" rather than "BCFP" or "CFPB"

You should follow Local Rules and standing orders for jurisdictions in which you are filing documents in court.

Document Maintenance and Retention Policies

Maintaining Matter Folders

A matter folder is an investigational or litigation file. Maintaining uniform, complete, and accurate matter folders that document relevant developments throughout the course of Enforcement matters is critical for information sharing, continuity (following personnel turnover), effective litigation management (including the maintenance of litigation holds), Bureau compliance with the Freedom of Information Act (FOIA) and discovery obligations, and file sharing with other law enforcement agencies. Such folders should be maintained electronically to the extent possible.

Matter folders should use the naming convention 20xx-xxxx-xx[name of entity] where the numerical designation is the matter number from the MMS and the name of the entity is the matter name from the MMS.

A matter folder should generally contain the following subfolders:

- Internal documents
- External correspondence
- Agreements
- Civil Investigative Demands (CIDs) and Voluntary Requests for Information
- Information Informally Obtained from Outside the Bureau
- Confidential Supervisory Information
- Witness Statements, Declarations, and Transcripts
- Written Discovery
- Deposition Testimony
- Experts
- Case Pleadings
- Proceeding Transcripts
- Trial/Hearing
- Settlement

A sample matter folder[1] is available on SharePoint. The above procedures for maintaining matter folders should generally be followed. If appropriate and after consulting with the Assistant Litigation Deputy (ALD) assigned to the matter, staff may be authorized to deviate from the procedures.

Some of the reasons to properly maintain matter folders include:

- 12 C.F.R. § 1070.45 authorizes the Bureau to disclose confidential investigative information and other confidential information in certain circumstances. The contents of matter folders may be shared with other law enforcement agencies.
- Federal Rule of Civil Procedure 26(a)(1) requires the Bureau to make certain disclosures at the onset of litigation, including identifying individuals likely to have discoverable information the Bureau may use to support its claims or defenses. Failure to identify such individuals during discovery can result in sanctions, including an Order precluding the Bureau from presenting testimony from those individuals.
- If an investigation results in administrative proceedings, 12 C.F.R. § 1081.206 places upon the Office of Enforcement an affirmative obligation to make available for inspection and copying certain documents it obtained before the institution of proceedings, including documents obtained from persons not employed by the Bureau. Upon commencement of an administrative proceeding, Staff should consult the rule and associated background discussion.

Creating a Matter Folder

As soon as an Investigation is opened (under the Enforcement Action Process (EAP)), the ALD should send a request to the Enforcement Front Office Operations Assistant and copy the Enforcement Administrative Officer requesting the creation on SharePoint of a matter folder that will be used to preserve all documents obtained or created in connection with the Investigation and any subsequent enforcement action.

1 (b)(7)(E)

The request should designate the assigned staff members. Following the creation of the folder, the ALD should move documents from the preliminary research stage into the matter folder.

When saving a document in a matter folder, use a naming convention that conveys the following information, as applicable:

- Type of document (i.e. internal memo, transcript, motion, letter, opinion);
- Title/Subject of the document;
- Author of the document;
- Date of the document;
- The party filing or serving the document; and
- Name of individual producing the document.

Internal Documents Folder

In every matter folder, Staff should create a unique subfolder titled "Internal Documents." This folder is used to preserve all final drafts of documents created by the Office of Enforcement and other Bureau staff in connection with that matter. Within the Internal Documents folder, Staff should save:

- The Investigation Opening Memorandum;
- The Action Memoranda;
- Internal research memoranda;
- All other internal memoranda; and
- Any written notes of significant internal and external meetings.

External Correspondence Folder

In every matter folder, Staff should create a subfolder titled "Correspondence." In this folder save correspondence (including emails) to and from opposing counsel, third- parties, witnesses, and any other individuals with whom Staff correspond in relation to the matter.

Agreements Folder

In every matter folder, Staff should create a subfolder titled "Agreements" to save tolling, confidentiality, and other agreements with potential Defendants or other parties.

CIDs and Voluntary Requests for Information Folder

In every matter folder, Staff should create a subfolder titled "CIDs and Voluntary Requests for Information." Within this folder, Staff should save:

- All voluntary requests for information and CIDs issued by the Bureau in a subfolder titled "Bureau Requests," and
- All correspondence responding to voluntary requests for information and CIDs in a subfolder titled "Responses to Requests."

Information Informally Obtained from Outside the Bureau Folder

In every matter folder, Staff should create a subfolder titled "Information Obtained Informally from Outside the Bureau." Staff should save any information and documents informally received from consumers and other third parties in the course of the investigation in this folder or an appropriate subfolder.

Confidential Supervisory Information Folder

In every matter folder, Staff should create a subfolder titled "Confidential Supervisory Information." Staff should save any information that contains CSI, including final examination or inspection reports provided by Supervision.

Witness Statements, Declarations, and Transcripts Folder

In every matter folder, Staff should create a subfolder titled "Witness Statements and Testimony" to preserve all witness statements, including emails and testimony transcripts obtained during the course of an investigation. Within this folder, Staff should save any witness statements, including testimony transcripts or declarations and associated exhibits. Staff should clearly label and store witness statements in accordance with any protective order or agreement restricting the dissemination of the material outside of the Bureau. Hardcopy materials should also be clearly labeled and stored according to the requirements of the protective order or agreement.

In preserving materials related to witnesses, you should consult 12 C.F.R. § 1081.207 regarding the Bureau's obligation to produce statements of individuals it calls or intends to call as witnesses. The Bureau is required to produce statements that would have to be produced pursuant to the Jencks Act, 18 U.S.C. § 3500. Staff should consider creating subfolders for materials obtained from each witness and for exhibits used during the taking of witness testimony.

Written Discovery Folder

When an action is commenced, in every matter folder, Staff should create a subfolder titled "Written Discovery." Within this folder, Staff should save:

- All Requests for Production, Requests for Admission, and Interrogatories issued by the Bureau to Defendants in a subfolder titled "Bureau's Discovery Requests,"
- All Bureau responses to Requests for Production, Requests for Admissions, and Interrogatories in a subfolder titled "Bureau's Discovery Responses,"
- All Requests for Productions, Requests for Admission, and Interrogatories issued to the Bureau in a subfolder titled "Defendant's Discovery Requests,"
- All Defendants' responses to Requests for Production, Requests for Admissions, and Interrogatories in a subfolder titled "Defendants' Discovery Responses,"
- All subpoenas and subpoena responses in a subfolder titled "Third-party Discovery," and
- All privilege logs.

When multiple discovery requests of the same type are issued or received, Staff should number the requests and responses (*e.g.*, when the Bureau is served multiple Requests for Production in a case, save them as "First Request for Production" and "Second Request for Production").

If a case involves multiple Defendants, consider creating separate discovery subfolders for each Defendant.

Deposition Testimony Folder

When a civil action is commenced Staff should create a subfolder in the matter folder titled "Deposition Testimony." Within this folder, Staff should save all deposition notices, all deposition transcripts, and all deposition testimony outlines.

Experts Folder

In every matter folder, Staff should create a subfolder titled "Experts." Within this folder, Staff should save:

- All expert reports;
- All correspondence, documents, research, data, articles, and other materials sent to, and received from, experts retained by the Bureau;
- A subfolder for things sent to the expert that meet the definition of those communications that are subject to discovery as set out in Fed. R. Civ. P. 26(b)(4)(C), including communications of facts, data, and assumptions on which the expert relies in forming opinions;
- All agreements between the Bureau and retained experts; and
- All invoices from experts and records of payments made.

In organizing and saving expert-witness materials, Staff should consult 12 C.F.R. § 1081.210 and Fed. R. Civ. P. 26(a)(2) and (b)(4) regarding the disclosure of expert witness reports and other information.

Case Pleadings Folder

When a case is opened, Staff should create a subfolder in the matter folder titled "Case Pleadings." Within this folder, Staff should save:

- File-stamped versions of pleadings filed with the Court or Administrative Law Judge, including Witness and Exhibit Lists;
- File-stamped versions of exhibits filed with pleadings (including any redacted and un-redacted versions of the pleadings);
- PDF and Word versions of pleadings filed on behalf of the Bureau;
- Opinions issued by the Court or Administrative Law Judge; and
- Orders issued with opinions.

Proceeding Transcripts Folder

In every matter folder, Staff should create a subfolder titled "Transcripts." Within this folder, Staff should save transcripts from all administrative or court proceedings, including preliminary hearings and arguments.

Trial/Hearing Folder

Once a case has been filed, Staff should create a subfolder in the matter folder titled "Trial." In this folder, Staff should save all trial and administrative hearing-related documents, including witness examination outlines and opening statement and closing argument outlines.

Settlement Folder

In every matter folder, Staff should create a subfolder titled "Settlement" and save all settlement-related documents there.

Subfolders

Within any of the required folders in each matter folder, Staff should create appropriate subfolders for purposes of improved organization. For example, in the Internal Documents Folder, subfolders might include: "Internally-created Fact Memos," "Research Memos," "Notes of Witness Interviews," "Exam-related Documents," "Press Releases," "Reports," and "Legal Research."

Contact List

For every matter folder, Staff should create and keep updated a contact list consisting of information including names, addresses, email addresses, and telephone numbers for all relevant persons or entities, including:

- Members of other divisions in the Bureau involved in the investigation or litigation of the case;
- Co-counsel, including co-counsel at sister agencies participating in the investigation or litigation of the case;
- Opposing counsel;
- Expert witnesses and consulting experts;
- Fact witnesses, including counsel for fact witnesses; and
- Any person not employed by the Bureau who provided documents or information in connection with the investigation or litigation of the case.

The contact list should be maintained in the MMS system.

Service List

To the extent service isn't effectuated through electronic filing, Staff should create a service list identifying the parties that should receive administrative or case pleadings and the manner in which parties should be served.

Case Calendar

When an investigation is opened, Staff should create and keep updated a "Case Calendar" in MMS. The Case Calendar should include:

- Due dates for responses to CIDs and voluntary requests for information;
- Scheduled witness testimony;
- Case management deadlines, such as deadlines to complete discovery, to file expert witness reports, and to file summary judgment motions, and the date set for trial;

- Due dates for responses to discovery served by the Bureau and by the Defendant(s);
- Due dates for oppositions and replies to motions; and
- Depositions and hearings scheduled.

When calculating deadlines, Staff should consult 12 C.F.R. Part 1081, Fed. R. Civ. P. 6, the local rules for the District Court where the case is filed, as well as any Standing Orders of the judge or hearing officer before whom the action is pending.

Maintaining Exam Support Files

This policy pertains to documents and information that Staff may create, obtain, or utilize in connection with supporting Supervision examination activity ("Exam Support Documents"). Exam Support Documents typically fall into two categories:

1. Bureau documents, such as notes, memoranda, examiner work papers, exam reports, and other work product.

2. Non-Bureau documents, such as documents provided by supervised entities ("Supervised Entity Documents") and documents from third parties.

Exam Support Documents may contain confidential supervisory information that Staff should treat as confidential and privileged. *See* 12 C.F.R. § 1070.41. However, in certain circumstances, disclosure of Exam Support Documents may be required or appropriate. *See*, for example, the Office of Enforcement's Affirmative Disclosure and Other Disclosure Obligations for Adjudication Proceedings policy. Accordingly, Staff should properly maintain Exam Support Documents in order to protect their confidentiality and enable required or appropriate disclosures.

Exam Support File

When conducting exam support work, Staff should:

1. Create a unique file on SharePoint ("Exam Support") to maintain Exam Support Documents created, obtained, or utilized in connection with their examination support activity;

2. Contact the Bureau's Service Desk to limit access to the Exam Support File to Staff assigned to the examination; and

3. Create the following three folders within the Exam Support File:

    a. Internal Bureau Documents (*e.g.*, notes, memoranda, exam work papers, exam reports, and other work product);

    b. Supervised Entity Documents (*i.e.*, documents and information obtained from the supervised entity); and

c. Third Party Documents (*i.e.*, documents and information obtained from third parties).

Staff should protect Exam Support Documents by adhering to the following rules:

- Transfer Exam Support Documents only when necessary and through secure methods.
- Do not leave Exam Support Documents (or a laptop/device containing such documents) unattended or use them in public view.
- Alert managers immediately if Staff know or suspect that Exam Support Documents (or a laptop/device containing such documents) have been lost, stolen, or compromised.

Because Supervision personnel will maintain and preserve confidential supervisory information pursuant to Supervision's policies and procedures (*e.g.*, uploading Supervised Entity Documents into the Supervision & Examination System (SES)), Staff should not maintain any original confidential supervisory information (other than documents created by Staff) in the Exam Support File or any other location.
Instead, Staff should store copies of confidential supervisory information obtained or utilized during examination support activity in the Exam Support File and place such confidential supervisory information in the above-described appropriate folders (Internal Bureau Documents, Supervised Entity Documents, and Third-Party Documents).

In order to facilitate coordination between Enforcement and Supervision during examination activity, Supervision often provides Staff with access to exam-related information stored in its files on SharePoint, the SES system, or other database or computer systems. Only certain confidential supervisory information in Supervision's systems may be relevant to Staff's examination support activity. Staff should copy only that information obtained or utilized in connection with the examination support activity (*i.e.*, Exam Support Documents) to the Exam Support File. Because in certain situations, the Bureau has an affirmative obligation to disclose documents obtained from persons not employed by the Bureau (*i.e.*, supervised entities and third parties), Staff should maintain such Exam Support Documents. Examples of confidential supervisory information that should be copied to the Exam Support File include:

- Information that Staff obtain by hand delivery, mail, electronic mail, or fax in the course of exam-support activities.

- Information that Staff use or rely upon to conduct legal analysis or formulate legal opinions, reach factual conclusions, or provide legal or policy advice in connection with the exam.
- Information that may form the factual basis of a potential enforcement action or otherwise may underlie Staff's decision to recommend commencement of a potential enforcement action arising out of an exam.
- Other information relevant to Staff's support of the examination process.

Conversely, Staff should not maintain in the Exam Support File information that is irrelevant to Staff's examination support activity (*e.g.*, Supervision documents that Staff reviews but concludes are irrelevant).

Transfer to Matter Folder if an Investigation Is Opened

If an examination leads to an enforcement matter (pursuant to the Action Review Committee), Staff should:

1. Create a matter folder as outlined in the Maintaining Matter Folders policy;
2. Create a folder within the matter folder labeled "Examination-related Documents;" and
3. Copy the existing Exam Support File (along with the Internal Bureau Documents, Supervised Entity Documents, and Third-Party Documents subfolders) into the newly created Examination-related Documents folder.

The Examination-related Documents folder will help Staff keep track of the documents relating to the examination and make necessary disclosures.

Freedom of Information Act

The Freedom of Information Act (FOIA), 5 U.S.C. § 552, requires federal agencies that receive a request for records under FOIA to:

- Conduct a reasonable records search;
- Appropriately identify exempted and privileged information contained within records; and
- Preserve and produce the responsive records.

While the Bureau's FOIA Office holds primary responsibility for FOIA compliance, the Office of Enforcement should take certain actions to assist in this compliance. Specifically, Staff should facilitate a reasonable records search; identify sensitive, confidential, and privileged information within Enforcement records; and preserve and produce records responsive to a FOIA request.

Because FOIA is a highly litigated area, the Bureau's FOIA Office establishes policies and procedures that meet the latest standards for federal agencies. The FOIA Office also updates policies and procedures to meet recent guidance from courts. When the FOIA Office asks Enforcement Staff to identify responsive records, it is important to closely follow the Bureau's FOIA procedures. Ask for guidance from the FOIA Office before making any deviations from the procedures described here.

Facilitating a Reasonable Records Search

Enforcement personnel should take the following actions to comply with the Bureau's records policy:

1. Identify all materials created or received in the course of official duties and dispose of them only in compliance with the Bureau's records disposition schedule;
2. Segregate federal records from non-federal records (*i.e.*, separate personal email and other records from work-related material); and

3. Organize federal records in such a manner as to enable the FOIA Office to effectively identify records that may be responsive to a FOIA request.

Enforcement personnel should be familiar with and periodically review the Bureau's records management program. Staff should organize electronic and paper folders so as to enable a third-party to find the employee's federal records that are related to particular matters, projects, policies, decisions, or procedures. For guidance on how to organize folders for matter-related documents, see the Office of Enforcement's Maintaining Matter Folders policy.

The FOIA requires federal agencies to search all places that are reasonably likely to contain records responsive to FOIA requests, including the files of all agency employees who may have such records. By organizing your matter folder into subfolders, as explained in the Maintaining Matter Folders policy, you reduce the number of files that must be searched in response to a FOIA request. You also minimize the potential for inadvertent inclusion of non-relevant and sensitive materials. The fact that you may be on leave from work or have a change in duty station does not relieve the Bureau of its search obligations. It is, therefore, important for you to consistently organize your records so as to avoid disrupting the FOIA search process during your absence from the office.

Identifying Sensitive, Confidential, and Privileged Information Contained Within Records

If the Bureau's FOIA Office determines that a Bureau employee would likely possess records that are responsive to a FOIA request, it will conduct an electronic search of the employee's emails and other electronic documents and will request that the employee provide any responsive hard-copy documents. The FOIA Office will then review these records to determine if any information should be withheld from public disclosure. Appropriately marking and filing all records Staff create or receive aids the accuracy of this review.

Before engaging in any matter or project, project leaders and lead attorneys should consider the potential FOIA disclosure obligations. When appropriate, consult training materials, the Office of Enforcement's FOIA point of contact (FOIA POC),

and/or the Bureau's FOIA Office to determine the applicability of any exclusions or privileges. Project leaders and lead attorneys should give appropriate direction to team members.

> Staff should have general knowledge about the FOIA exemptions and exclusions that apply to Enforcement work. It is important to understand what may or may not be made public.

Preserving and Producing Responsive Records

The Bureau's FOIA Office is the only office within the Bureau authorized to respond to FOIA requests. Generally, the Bureau must respond to FOIA a request within 20 business days of receipt, with some exceptions.

Requests from the FOIA Office should be given high priority. When the Bureau receives a FOIA request that pertains to any information in Staff's custody or control, these steps should be followed in sequential order:

1. The FOIA Office forwards all FOIA requests to the Enforcement FOIA POC, who in turn, informs the Office of Enforcement Chief of Staff of the request.

2. The FOIA POC consults the Enforcement MMS, Enforcement records (*e.g.*, Enforcement Action Process opening memos), and Office of Enforcement personnel necessary to identify to the FOIA Office all potential custodians of responsive records, their job title(s) at the times relevant to the request, and all lead attorneys and managers on any matter relevant to the request.

3. The FOIA Office emails a standardized FOIA Questionnaire to all potential custodians of responsive records.

4. Each custodian receiving the FOIA Questionnaire completes the questionnaire and returns it to the FOIA Office by the due date noted in the email (normally within two business days).

5. The FOIA Office determines whether there are potentially responsive records.

6. The next steps depend upon the form and location of the records, as follows:

a. If the FOIA Office determines that a custodian has any potentially responsive electronic records, it will retrieve all responsive records directly from the custodian's email and/or shared network.

b. If the FOIA Office determines that a custodian has any potentially responsive hard copy records, it will schedule a meeting with the custodian to collect and copy the records.

c. If the FOIA Office determines that potentially responsive electronic records exist beyond the grasp of the network (usually, on a remotely-located custodian's laptop), it sends the custodian an encrypted USB drive via overnight mail service. The custodian is directed to save all responsive records to the USB drive and return the drive to the FOIA Office via overnight mail service.

7. The FOIA Office conducts its review of the potentially responsive records.

8. Prior to releasing records to the requestor, the FOIA Office sends a proposed release to the following Enforcement contacts for review:

   a. FOIA POC;

   b. Project leader or lead attorney on the matter(s) involved; and

   c. Office of Enforcement Chief of Staff.

9. The FOIA POC, project leader or lead attorney, and the Chief of Staff determine whether notice to and/or additional consultation by other Enforcement personnel is appropriate.

10. The Enforcement contacts conclude their consultation within two business days of receiving the proposed release.

11. The FOIA Office concludes its processes and responds to the requestor.

12. The FOIA Office provides the Enforcement FOIA POC a copy of the released records (including any transmittal letters) or saves them in the Released Records folder.[1]

---

1 (b)(7)(E)

Maintenance of Documents Collected During an Investigation or Discovery

Electronic Productions

Staff should ensure that electronic productions received during the course of an investigation or in discovery are loaded into an e-document review tool, such as Clearwell or Relativity.

Paper Productions

In general, paper productions are highly discouraged, and Enforcement's document submission standards require paper productions to be scanned and produced electronically by the producing party. In those limited circumstances when accepting paper productions is the only alternative for receiving the requested information, Staff should scan and digitize those paper productions obtained during an investigation or through discovery via optical character recognition (OCR) so the documents can be loaded into an e-document review tool, such as Clearwell or Relativity.

In most situations, paper productions should be scanned and OCR'ed. However, if the size of a production is minimal or an investigation is not likely to lead to enforcement action, you may opt to avoid the expense.

Documents Subject to a Protective Order or Other Agreements

If, during the course of an investigation or discovery, materials are obtained pursuant to agreements restricting the dissemination of such materials outside of the Bureau (for example, from a state attorney general pursuant to a Memorandum of Understanding (MOU)), Staff should clearly label and store the materials according to the requirements of the protective order or agreement.

Litigation Holds

A litigation hold is a process used to preserve all forms of relevant information when litigation is anticipated. Questions about implementing a litigation hold should be

directed to the Special Counsel for eDiscovery or you ALD.

Staff should preserve all documents in accordance with any litigation hold that may be in place with the respect to a Matter.[1]

External Telephone Communications

Staff should memorialize important telephone conversations with outside parties in a matter log kept in the matter folder, including the following information:

- Date of conversation;
- Participants; and
- Notes documenting the content of the conversation.

Follow-up and document any substantive telephone conversation with opposing counsel via email or letter memorializing the substance of the conversation.

Maintenance of Original Documents

Original documents should only be used when necessary to present evidence in court or at a hearing. In order to maintain the integrity of original documents and data, with the exception of large-scale paper document productions, Staff should:

- Scan and save paper documents received in the course of a matter into the appropriate folder in the matter folder.
- To the extent necessitated by the receipt of paper documents, create a paper matter folder with the same folders as in the electronic matter folder. Note that paper copies of documents received electronically should not be created and stored in the paper matter folder.
- Maintain original paper documents in pristine condition. Do not mark or alter them in any way from the condition in which they were originally produced.
- Maintain original hardcopy documents in the appropriate folder within the paper matter folder.
- Segregate original documents from the Staff's personal notes, copies of Staff's emails, or any other documents.

---

1 (b)(7)(E)

- Load into Clearwell or Relativity electronic data received as part of the investigation.
- Ensure that all original electronic data production (*i.e.*, the CD, DVD, or other storage device on which the production was made) is provided to T&I Legal Tech for proper labeling and retention.

Investigative Policies

Opening an Enforcement Matter

This policy governs the opening of matters by the Office of Enforcement based on information that a covered person may have committed or may commit a violation of federal consumer financial law. Matters are divided into two categories: the "research matter" and the "investigation." A matter may be opened at any stage, whether during the research matter phase, the investigation stage, or at the stage when the Bureau is ready to approach a subject to settle or file a complaint.

The decision to conduct either a research matter or an investigation must be carefully considered in light of its impact on:

- The potential subject(s);
- The market in general;
- Bureau and Enforcement resources;
- The Enforcement Strategic Plan;
- Other Bureau divisions; and
- Law enforcement partners.

This policy is designed to promote vigorous enforcement while effectively monitoring investigation activities.

This policy also addresses how to handle the opening of matters that come to Enforcement through the Action Review Committee (ARC) process.

Research Matters

While not necessary in every instance, conducting a research matter prior to deciding whether to open an investigation permits Staff to gather basic information and preliminarily evaluate the potential for successful enforcement of suspected violations of federal consumer financial law while minimizing the disruptions and risks associated with contacting investigation subjects during an investigation.

Research matters should be opened primarily to evaluate nascent ideas for enforcement work to determine if an investigation is warranted. Research matters should be completed fairly quickly after determining whether further investigation is appropriate.

The primary purpose of a research matter is to collect and analyze easily obtainable information in order to:

- Determine whether the relevant conduct likely violates federal consumer financial law and the Bureau likely has jurisdiction.
- Determine whether non-Bureau law enforcement partners are investigating the matter or should be advised of the Bureau's interest in the matter.
- Evaluate whether an investigation is in the best interest of the Bureau and would be an effective use of Office of Enforcement resources.
- Determine how the matter will be staffed.
- Identify and prepare to address issues that may be raised during the Enforcement Action Process (EAP).
- Draft an Opening Investigation Memorandum.

OPENING A RESEARCH MATTER

Any member of the Enforcement Office may propose a research matter according to the following process:

When a team member has an idea for a research matter, she should prepare a Recommendation for Assignment of a Matter (RAM).[1] RAMs should be one page in length and should provide the RAM author's summary views about the following:

- What conduct pertaining to a financial product or service may be taking place that may harm consumers;
- What federal consumer financial law(s) might be violated by the conduct if it is, in fact, occurring;

1 (b)(7)(E)
(b)(7)(E)

- What entities—if any have been specifically identified—may be engaging in this conduct; and
- Limited other relevant information.

The RAM should be shared with the appropriate Enforcement Issue Team who may be able to provide insight on the specific matter and who will confirm that the conduct in question is not currently being handled by the Bureau's Office of Supervision.

Staff is responsible for ensuring that the conduct in question is not currently being handled by the Office of Enforcement or the FTC, by reviewing the Enforcement MMS (ENForce) and OMB Max.

Attorneys and paralegals should provide RAMs to their LD. Other personnel may select any LD to review their RAMs.

LDs may open research matters. If the LD chooses not to open the matter, he should provide notice to the Enforcement Director, Principal Deputy, and Chief of Staff (the Enforcement Front Office).

The team member who presented the RAM may be assigned to the opened research matter. If the team member who presented the RAM is unavailable or not assigned to work on an opened research matter, the LD should assign the matter to other Staff.

Within one week of opening the research matter, the ALD supervising a research matter will notify the Chief of Staff and ask the Legal Assistant assigned to enter the matter into the MMS and OMB Max.

Research matters should generally be open for no longer than two months, during which period Staff should spend a limited amount of time determining whether the issues identified warrant opening an investigation.

After two months, a determination will be made whether the research matter should either become an investigation or be closed with no action. Investigations should generally be opened promptly thereafter, according to the process described below. Issue Teams should monitor closed research matters to determine whether they merit reconsideration or new action by the Office in the future.

LIMITING EXTERNAL CONTACT

During research matters, Staff should avoid any direct interaction with potential investigation subjects, their known agents, or third-party witnesses (other than consumers or potential victims). Evidence gathering should generally be limited to non-identifiable internet searching, review of consumer complaints, media sources, legal research, and contact with other law enforcement agencies and consumers.
Staff should ask consumers that they contact during research matters to keep their conversations confidential, although it is understood that consumers may choose to ignore such requests.

Investigations

Pursuant to the EAP, the Enforcement Director must approve the opening of any new investigation. When submitting a proposal to open an investigation to the Enforcement Director, Staff should follow the procedures described below.

> The Bureau is authorized to investigate merely on suspicion that any person has violated any provision of federal consumer financial law, or to seek assurance that a violation has not occurred. An investigation is a means to gather facts to assist in the determination of whether further action by the Bureau has the potential to address conduct that violates federal consumer financial law. The existence of an investigation does not suggest that the subject has indeed violated the law. It is not necessary to have evidence that a law has in fact been violated before opening an investigation.

An investigation should generally be opened when initial research provides

- A plausible set of facts that, if proven, would amount to a violation of one or more federal consumer financial laws;
- Reason to believe that one or more specific entities may be engaging in the conduct described in those facts;
- Evidence of a magnitude of harm that justifies investment of Office resources;

- That there are sufficient Enforcement resources available to properly address the matter; and
- That the devotion of those Enforcement resources is consistent with the Office's Strategic Plan and articulated priorities or warrants a conscious departure from those plans and priorities.

Prior to proposing the opening of an investigation, Staff should consider a number of factors, including the following:

- Whether there is a need for immediate action to protect consumers;
- Whether there exists a sufficiently credible source of information or set of facts indicating potential violations of federal consumer financial law;
- The statutes or rules potentially violated and defenses that may be raised;
- Whether the conduct is relevant to a Bureau program or priority;
- Whether the conduct involves a possibly widespread and/or emerging industry practice;
- The egregiousness of the potential violation;
- The magnitude of potential harm to consumers;
- Whether the potentially harmed group is particularly vulnerable or at risk;
- Whether the conduct is ongoing;
- Whether the perpetuator of the conduct is a recidivist;
- Whether the conduct can be investigated efficiently and within the relevant statute of limitations period;
- Whether it might be more appropriate for other Bureau components to address the conduct;
- Whether other authorities, including federal or state agencies or regulators, are already investigating the conduct and/or might be better suited to do so than the Bureau;
- Whether the matter presents a good opportunity to cooperate with other civil and criminal agencies including strategic law enforcement partners;
- If the proposed subject is a supervised entity consult with the PST about notice to Supervision that may be required.

- Whether the matter gives the Bureau an opportunity to be visible in a community that might not otherwise be familiar with the Bureau or the protections afforded by federal consumer financial law;
- Whether opening an investigation would be an appropriate use of Bureau resources;
- Whether opening an investigation would advance the goals articulated in the Enforcement Strategic Plan.

The Opening Investigation Memorandum

The following process should generally be used to open an investigation.

Before drafting an Opening Investigation Memorandum (Opening Memo), Staff should discuss the proposed investigation with their ALD and LD.

Staff should draft Opening Memos using the Opening Memo template.[2] The following information should be included in every Opening Memo:

- The investigation's identifying number
- The Examination number, if applicable
- The subject's name
- The origin or source(s) of the investigation
- A brief description of the background facts
- The Bureau's jurisdiction
- The potential legal violations
- Potential violator(s)
- Other relevant parties
- Counsel of potential violators or other relevant parties (if known)
- The Statement of Purpose pursuant to 12 C.F.R. § 1080.5 (see Complying with Rule of Investigation 1080.5 [Notification of Purpose])

2 (b)(7)(E)
(b)(7)(E)

- The investigation's supervising LD and ALD

The Opening Memo should be shared with the appropriate Issue Team for Issue Team and PST input. The Issue Team and PST should, within a week of receipt of the Opening Memo, provide the case team with feedback about whether they believe the investigation should be opened and how this investigation fits into the SEFL Strategic Plan. The Issue Team and PST feedback may be oral and informal, but should also include a short written recommendation to the Enforcement Front Office about whether to proceed with opening the investigation. That written recommendation should be no more than one page long, and should be provided in a document separate from the Opening Memo.

Staff should incorporate Issue Team and PST management feedback, if appropriate, and send the Opening Memo and feedback page to their LD.

Within a week, the LD should make a final determination about whether to advance the Opening Memo and, if advancing, send it to the Litigation Review Inbox (Litigation_Review_Inbox@cfpb.gov), copying the Enforcement Senior Team, for review by the Enforcement Front Office. If an LD chooses not to open an investigation, she should notify the Enforcement Front Office.

The Enforcement Director, in consultation with the Enforcement Front Office, will either approve the opening of the investigation or request that the LD discuss it at her next regularly scheduled check in.

Staff are responsible for ensuring that the Enforcement MMS (ENForce) and OMB Max are updated at all stages of investigations.

ARC Matters

SEFL Staff Memoranda[3] describe the ARC process and associated responsibilities for Enforcement. Staff should familiarize themselves with those policies and follow them in their exam support work. The following procedures apply internally within Enforcement for ARC matters.

Before Staff provide comments on the ARC memo, they should consult with their LD.

---

3 (b)(7)(E)

When Staff recommend to the Office of Supervision Policy that a matter being considered in ARC be addressed through Enforcement, Staff should send a brief email stating as much to the Litigation Review Inbox (Litigation_Review_Inbox@cfpb.gov. This notification should happen as soon as practicable, but no later than the day that the ARC memo is circulated to the Assistant Directors. The Chief of Staff
will ensure that the Enforcement Director, Principal Deputy, and Policy and Strategy Deputy are aware of the recommendation so that informed, strategic decisions can be made about the opening of Enforcement matters through ARC.

The LD and the Policy and Strategy Deputy should consult with the Principal Deputy on the ARC recommendation.

Once an ARC determination has been made that a matter be resolved through Enforcement, the LD supervising the matter is responsible for ensuring that her team take the appropriate steps—in compliance with SEFL Integration 3.3 and Enforcement practices—to proceed with the matter, including ensuring that the matter be entered and properly updated in MMS and OMB Max.

ENForce: Opening Matter Cheat Sheet

Creating New Matters in ENForce

1. Select the "Matters" tab at the top of the screen, and then select the "NEW" button. A new Matter record will open.
2. Complete the fields listed below as follows (required fields are marked with a red band):

TYPE OF MATTER	ENF MATTER
Matter Name	Copy from "Matter Name" on page 1 of the RAM Template.
Matter No.	This field populates automatically (after you enter Matter name).
Date Created	This field populates automatically.
Stage of the Matter	Select either "Research" or "Post ARC" as appropriate. If you need to open a matter in any other stage, contact the ENForce administrator.
Date Closed and Closed Type	Leave these fields blank.
Partnership Matter	Select "Yes" or "No" as appropriate from the drop down.

Nature of Matter	Copy from "Nature of the Matter" on page 1 of the RAM Template.
Institution Type	Copy from "Institution Type" on page 1 of the RAM Template.
Primary Entity	Select the primary entity subject to this matter.
Supervision No.	Leave this field blank.
OMB MAX	Check the "OMB Max" box if the matter has been entered into OMB Max.
Source	Copy from the "Source of Information" on page 1 of the RAM Template. If the source is "Other" describe the source in the "Please Describe" box.
Enf Region	Select the office that is working on the matter: DC, NE, SE, MW, W. If attorneys from multiple offices are working on the matter, select the office of the lead attorney.
Populations	Leave these fields blank.
Most Recent Action Taken	Enter a one or two sentence description of what has happened recently. Include any relevant dates.

Electronic Communications Privacy Act (ECPA) Compliance

The Electronic Communications Privacy Act (ECPA) amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and is designed to protect communications from government surveillance. The law amended the Wire Tap Statute to encompass transmissions of electronic data by computer and prohibits both the interception of electronic communications and access to stored electronic communications.

The Stored Communications Act (SCA), 18 U.S.C. §§ 7201-7212, which is Title II of the ECPA, sets forth a system of privacy rights for customers and subscribers and addresses voluntary and compelled disclosure of stored wire and electronic communications maintained by an electronic communication service ("ECS") provider. The statute reflects policy that greater privacy interests are accorded to stored email than to subscriber account information. In addition, use of certain legal process to obtain information requires notice to the subscriber.

The ECPA places limitations on the Bureau's ability to obtain certain types of information from providers of "electronic communications service" and "remote computing service," including, but not limited to, phone companies, ISPs, electronic Bulletin Board Systems, and third-party data warehouses. *See* 18 U.S.C. § 2703(a)-(b). The ECPA applies to stored "electronic communications" (*e.g.*, email) from such service providers and all other information pertaining to the service provider's customers or subscribers. *See* 18 U.S.C. § 2703. Under the ECPA, the Bureau can use an administrative or trial subpoena to obtain the contents of electronic
or wire communications that have been held in storage more than 180 days, as long as prior notice is provided to the subscriber or customer. *See* 18 U.S.C. §§ 2703(a) and 2703(b)(1)(B). There are certain procedures, however, through which the Bureau can access certain subscriber account information without notifying the subscriber.

Obtaining Subscriber Information Without Triggering Notification

Below is a list of six categories of subscriber information that can be obtained by the government with an administrative or trial subpoena from an electronic communications service or remote computing service without triggering the subscriber/customer notification requirement.

> Note: During May 2014, companies such as Google Inc., Microsoft Corp., and Apple Inc. stated that they will begin notifying users whose information has been requested by the government. Twitter and WordPress have already made such subscriber notifications.

When Enforcement receives any of the following information from an ISP, Enforcement as "a governmental entity receiving records or information" is not required to provide notice to the subscriber or customer:

1. Name;
2. Address;
3. Local and long distance telephone connection records (inbound and outbound, if applicable), or records of session times and durations;
4. Length of service (including start date) and types of service utilized;
5. Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network (IP) address or e-mail address; and
6. Means and source of payment for such service (including credit card or bank account number).

Staff should include the following Cautionary Note in a CID seeking the information referenced above:

> *NOTE: This CID is issued in conformance with Sections 2702 and 2703 of Title 18 of the United States Code (The Electronic Communications Privacy Act). To the extent that you are a provider of electronic*

communication service or remote computing service, your response to this CID should not divulge a record or information pertaining to a subscriber or customer of your service, other than that allowed pursuant to 18 U.S.C. § 2703(c)(2). If you have any questions, please contact Bureau attorney _____ at _____ before providing responsive information.

Prior to issuing a CID covered by the ECPA, Staff should review the CID recipient's confidentiality policy regarding law enforcement subpoenas. If the policy is not available online, Staff should request it from the CID recipient. Before sending the CID, Staff should also request that the recipient keep the CID confidential. Notice to a subscriber or customer is not required if the information sought from the electronic communications service is limited to the six categories referenced above. 18 U.S.C. § 2703(c)(3). If the CID recipient indicates that it will not or may not keep the CID confidential, Staff should discuss with his or her ALD whether to issue the CID.

If it is unclear whether the ECPA applies to the information requested, Staff may want to draft a CID with the standard six requests and more substantive conditional requests that the recipient must answer only if the recipient does not assert that the information is covered by the ECPA. This approach is useful if, despite diligent investigation, Staff cannot determine whether the ECPA applies. Before sending such a request, however, consider whether the recipient is sufficiently sophisticated to determine whether it is a provider of "electronic communications service" or "remote computing service" as defined by the statute.

In general, it is better practice to refrain from issuing a CID to a provider of remote computing service or electronic computing service for the content of email. However, if notice to the subscriber or consumer is acceptable, you may obtain such information pursuant to 18 U.S.C. § 2703(b)(1)(B)(i). Note that the obligation to provide prior notice to the subscriber or customer rests with the government entity issuing process. Consult your ALD before requesting information pursuant to this section. Staff can also require that the service provider preserve records pending the issuance of process. *See* 18 U.S.C. § 2703(f). Note that a subscriber who is notified of process served on an ISP to obtain email has standing to move to quash.

The ECPA has narrow applicability, although it is a complex statute with a growing body of case law. Carefully consider whether the entity from which information is sought is an electronic communications service or remote computing service in determining whether the ECPA applies. The ECPA does not apply to direct requests for electronic communications to consumers and entities. The ECPA generally does not apply to obtaining information, including stored emails, from a corporation or financial institution's internal email network. Additionally, Staff may always access communications or request information "readily accessible to the general public." *See* 18 U.S.C.A. § 2511(2)(g). Staff may also obtain additional information with "the consent of the subscriber or customer to such disclosure." *See* 18 U.S.C. § 2703(c)(1)(C).

Note that the ECPA does not prohibit a service provider from notifying customers. Nonetheless, Staff should request that a service provider keep a CID confidential and seek confirmation in writing that the service provider will do so.

Remember that the ECPA is a criminal law. Improper government access may create liability for the Bureau and result in statutory disciplinary actions against Bureau employees. When in doubt, Staff should consult his or her ALD for further guidance.

RFPA: Obtaining and Sharing Personally Identifiable Financial Information in Compliance with the Right to Financial Privacy

When the Bureau makes a voluntary or compulsory request to a financial institution for personally identifiable financial information (PIFI) about a consumer, that request can implicate the Right to Financial Privacy Act (RFPA), 12 U.S.C. § 3401 *et seq.* While the RFPA generally does not limit the Bureau's ability to request or obtain information, it can impact the Bureau's ability to share such information with law enforcement partners. The procedure described below ensures that Staff will comply with the RFPA when requesting information and when sharing that information. Note that information subject to the RFPA may also be subject to other laws, such as the Privacy Act, 5 U.S.C. § 552a, or the Bureau's confidentiality rules, 12 C.F.R. § 1070.41

Section 1022(c)(9)(A) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) requires that the Bureau obtain consumer permission or comply with the RFPA prior to requesting "personally identifiable financial information" (PIFI) from a covered person or service provider. The Dodd-Frank Act does not define PIFI. However, Enforcement construes the phrase consistently with its use in Section 509 of the Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6809(4), and in the Bureau's rules implementing the GLBA, 12 C.F.R. § 1016.3(q) (1). Accordingly, PIFI is generally construed as information a consumer provides to a financial institution in connection with the offer or provision of a financial product or service, or information about a consumer obtained by a financial institution in connection with a specific transaction. *See* 12 C.F.R. § 1016.3(q)(1). Since in most cases it would be impracticable to seek permission from every consumer when requesting PIFI from a covered person or service provider, the Bureau will ordinarily meet its Section 1022(c)(9)(A) obligations by complying with the RFPA.

The Dodd-Frank Act requires the Bureau to comply with the RFPA. However, Section 3413(r) of the RFPA states that it does not apply to the "examination by or disclosure to the Bureau of Consumer Financial Protection of financial records or information in the exercise of its authority with respect to a financial institution." The focus of this section is on the exercise of the Bureau's authority over the institution to which the request is sent, not whether the institution is itself the focus of an investigation. Consequently, this exemption applies where the Bureau is investigating the financial institution it is seeking information from or a different financial institution. Although the Bureau's exemption under the RFPA is relatively broad, there are limits. Service providers, for example, may include entities that are not "financial institutions." In such cases, the Bureau may use other applicable RFPA exceptions for collecting and sharing information for supervisory and law enforcement purposes. *See* 12 U.S.C. § 3413(b) and (h). In short, the Bureau is generally exempt from the RFPA.

Sharing Personally Identifiable Financial Information

Whether the Bureau can share PIFI with other federal and state agencies depends upon the agency at issue. The sharing of information will be determined on a case-by-case basis by Legal. To avoid any issues that may arise from the unauthorized sharing of PIFI, Staff should follow the certification procedure below.

When Staff seeks PIFI through voluntary requests or CIDs to covered persons or service providers, Staff should provide certification[1] to the institution that the Bureau is in compliance with the applicable provisions of the RFPA. To the extent Staff want to share information with a law enforcement partner, Staff should direct the partner agency to file an Access Request[2] with Legal as described in 12 C.F.R. § 1070.43(b). Questions concerning the Information Access Letter should be directed to Legal. Legal will determine if sharing is permissible under the RFPA and respond appropriately to the request for access.

1 (b)(7)(E)
(b)(7)(E)

2 (b)(7)(E)
(b)(7)(E)

The Bureau's procedures for sharing PIFI with law enforcement partners vary depending on the partner agency. Legal will determine in each case whether and how the RFPA applies. The following are some general guidelines:

The Bureau is a member of the Federal Financial Institutions Examination Council (FFIEC) and has authority to transfer PIFI to the other four council members; the Federal Reserve Board (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Association (NCUA), and the Office of the Comptroller of the Currency (OCC), as well as to the Securities and Exchange Commission (SEC), Federal Trade Commission (FTC), and the Commodity Futures Trading Commission (CFTC). *See* 12 U.S.C. § 3412(e).

Upon certification by a Bureau supervisory official that there is reason to believe that the records containing PIFI are relevant to potential violations of federal criminal law and were obtained in the exercise of the Bureau's supervisory or regulatory functions, records containing PIFI may generally be transferred to the DOJ, United States Attorney's Offices, and the Secretary of the Treasury. The records must be returned to the Bureau upon completion of the investigation or litigation. *See* 12 U.S.C. § 3412(f)(2).

If a matter does not involve violations of federal criminal law, PIFI may be shared with any government agency in connection with a lawful proceeding, investigation, examination, or inspection if the certification discussed above has been sent to the covered person or service provider from whom the records were obtained. *See* 12 U.S.C. § 3413(h)(2).

RFPA is not implicated when sharing PIFI with state agencies and officials, since these entities are not subject to the statute. Sharing PIFI with state agencies and officials is still subject, however, to the Legal Division's approval of an Information Access Letter.

For related information, see the Bureau's policies on criminal referrals and civil referrals.

Suspicious Activity Reports

The Currency and Foreign Transactions Reporting Act of 1970 referred to as the "Bank Secrecy Act" or "BSA," requires U.S. financial institutions to assist U.S. government agencies in detecting and preventing money laundering. Financial institutions are required to keep records of cash purchases of negotiable instruments, to file reports of cash transactions exceeding $10,000 in a daily aggregate amount, and to report suspicious activity that might suggest money laundering or other criminal activities.

Federal law requires financial institutions to file a Suspicious Activity Report (SAR) if a banking transaction raises suspicion of possible violation of law. *See* 31 U.S.C. § 5313 and 31 C.F.R. § 1020.320(e). SARs are maintained by the Financial Crimes Enforcement Network (FinCEN), a bureau of the Department of the Treasury, as part of its regulatory responsibilities for administering the Bank Secrecy Act. Most SARs are supported by additional documentation that is maintained by the financial institution filing the SAR. The Bureau has access to the FinCEN database by virtue of a Memorandum of Understanding (MOU) between FinCEN and the Bureau.[1]

Only staff members that are authorized by the Bureau to access the FinCEN database may do so. Note that there are strict rules concerning the access to information; search limitations; maintenance, physical security, and disposal of records; use and dissemination of information; and record keeping for potential audits. Any staff member intending to review FinCEN database information should attend a briefing by the FinCEN-Bureau liaison.

Financial institutions are required to maintain copies of any SAR filed and the original or business record equivalent of any supporting documentation for five years. *See* 31 C.F.R. § 1020.320(d). The five-year period begins on the date the SAR is filed. Financial institutions are required to make all supporting documentation available to FinCEN and any agency designated by FinCEN as a law enforcement agency. *Id.* FinCEN does not include civil law enforcement agencies, such as the Bureau, in its definition of

1 (b)(7)(E)

"law enforcement" for purpose of obtaining supporting documentation. Therefore, Staff should contact FinCEN through the Enforcement Staff point of contact to obtain supporting documentation.

Generally, banks must file a SAR when they identify any suspicious transaction that is relevant to a possible violation of law, where:

1. The transaction is conducted or attempted by, at, or through the bank;
2. The transaction involves $5,000 or more in funds or assets; and
3. The bank has reason to suspect that:
    a. The transaction involves funds derived from illegal activities or is intended to hide or disguise funds or assets derived from illegal activities, as part of a plan to violate or evade federal law or regulation or to avoid transaction reporting;
    b. The transaction is designed to evade requirements of C.F.R. Chapter X (which relates to, among other things, records and reports to FinCEN) or of any BSA regulation; or
    c. The transaction lacks a business or apparent lawful purpose or there is no reasonable explanation for the transaction. *See* 31 C.F.R. § 1020.320(a).

In addition to the mandatory reporting requirements, financial institutions have discretion to report a suspicious transaction believed to be relevant to a possible violation of law or regulation. *See* 31 C.F.R. § 1020.320.

⚠ Any information that would reveal the existence of a SAR is confidential. The unauthorized disclosure of a SAR is a violation of federal law. *See* 31U.S.C. §§ 5318(g)(2), 5321, and 5322. Civil and criminal penalties may be imposed for SAR disclosure violations. Willful violations include penalties of up to $250,000 and/or imprisonment not to exceed five years. *See* 31U.S.C. § 5322(b). Additionally, civil liability may attach to the disclosure of a SAR or the existence of a SAR, inadvertent or otherwise. *See* generally, 31 C.F.R. § 1020.320(e). The following policies and procedures, which are mandated by FinCEN, are designed to ensure that Staff properly handle and prevent the unlawful disclosure of SARs and SAR information.

Obtaining a SAR and Supporting Documentation

When requesting SARs and supporting documentation, the designated investigator on a matter will telephone FinCEN to determine the best manner to securely obtain the SAR material. This communication is conducted telephonically to prevent inadvertent disclosure through a mistaken email address or otherwise. If FinCEN requires a written request, the Enforcement POC should reference the material stating, "Per our conversation on [date of conversation], please produce any and all Bank Secrecy Act materials filed by [institution/firm/office] on [date]."

Do not request SARs and supporting documentation from the filing institution. However, if the filing financial institution voluntarily offers to provide the additional SAR-supporting documentation, Staff need not go through FinCEN to obtain the same material.

Confidentiality of Suspicious Activity Reports

Remember that a SAR contains unsubstantiated allegations or suspicions. Only the underlying transaction, to the extent that it is proven, has evidentiary value. Internally, Staff should only disclose SARs and supporting documentation to other Staff who have a need to know for Bureau-related purposes. Externally, Staff should not disclose the existence of SARs and supporting documentation to anyone, except to authorized law-enforcement personnel and personnel from the SAR-filing institution that are responsible for the filing and management of SARs. Staff should not disclose any SAR information publicly in any form, including but not limited to, in documents filed in court or in administrative proceedings or otherwise publicly available. Specifically:

- Staff should not disclose the fact that a SAR exists or that a SAR has been filed.
- Staff should not attach or reference a SAR in a CID, charging document, motion, response, or press release.
- Staff should not introduce a SAR as an exhibit during any testimony on-the-record, unless the matter is specifically about a SAR, *e.g.*, failure to file a SAR.
- Staff should not refer to a SAR as a source of information or make it evident that a SAR was the source of any information.
- Staff may disclose the information contained in the SAR, as long as there is no reference to the SAR or any indication that the information came from a SAR. For example, Staff may disclose the information contained in a SAR by writing a Disclosure Letter that lists the factual information obtained from a SAR without disclosing its existence. Another way to disclose information contained in a SAR is to disclose the underlying bank documents kept in the ordinary course of business by the financial institution (provided the documents do not disclose the existence of a SAR).

Staff should use care as to the way in which SARs are referenced in case files and work product. To ensure that the existence of a SAR is not unintentionally disclosed to parties who gain access to case file material through discovery or the Freedom of Information Act, Staff should refer to a SAR in notes or memoranda as "Bank Secrecy Act Information" or "BSA Information."

Staff should pay particular attention to the SAR non-disclosure requirement when conducting discovery. SARs must not be disclosed as part of affirmative disclosure requirements in the Bureau's administrative proceedings. *See* 12 C.F.R. § 1081.206(b) (iv) (exemption for documents where applicable law prohibits disclosure). The SAR supporting documentation may be exempt from disclosure to the extent that it reveals the existence of a SAR.

As noted previously, Staff should make requests for SARs and supporting documentation through the Enforcement FinCEN POC. However, it is possible that when issuing CIDs or when conducting discovery, a request for non-SAR material may result in the production of SAR-related material. Therefore, if Staff believe that the request may result in the production of SARs and supporting documentation, Staff

should state in the request, "If your response to this [discovery request (*i.e.*, document production request)] contains Bank Secrecy Act materials, please segregate and label those materials within the production."

When responding to a discovery request, Staff should pay particular attention to ensure that the Bureau's response does not disclose a SAR or the existence of a SAR. If responding to the request requires the production of a SAR or material that would disclose the existence of a SAR, Staff should note an objection and not comply. For example, Staff could object on the basis that the discovery request requires the production of material that may violate the Bank Secrecy Act and related regulations. *See* 31 U.S.C. § 5311 *et seq.* and 31 C.F.R. Chapter X. If opposing counsel insists on the production of the withheld material, Staff should consult a supervisor. Consideration should be given as to whether it would be appropriate to seek a protective order under seal or to seek a ruling from the court on the production (in camera and under seal).

All concerns about a potential disclosure of a SAR or how to handle a SAR should be brought to the attention of an immediate supervisor.

Storing SARs and Supporting Documentation

Staff should take necessary precautions to secure and segregate SARs and supporting documentation from other work materials. Staff should segregate SARs and supporting documentation from the rest of their case files—both in electronic and hardcopy. Staff should keep SAR material received from FinCEN or otherwise in distinguishable folders or separate from other case material. This separation will assist in preventing accidental disclosure and facilitate securing the SAR information.

- When SAR-related material is not actively being used, Staff should store the material in a secure location such as a locked office or a locked file cabinet within an open work space. SAR material is not being actively used when Staff leaves SAR-related material unattended for anything other than a brief period of time. Therefore, if Staff leaves the SAR-related material for an activity such as lunch, a meeting, or coffee break, Staff should secure the material.
- Staff should include a header that states "Confidential BSA Material" on any memorandum, note, email, or other material that contains a SAR or would disclose the existence of a SAR.

- Emails containing SARs and supporting documentation should be encrypted. Similarly, SARs and supporting documentation placed on thumb drives, flip drives, or USB drives should be encrypted and stored in a secure location.
- When mailing SARs or supporting information, Staff should send the material via a postal courier that provides tracking information. See Securely Receiving and Transmitting Materials for further information.

Civil Investigative Demands

(updated April 2019)

During an investigation, Staff may seek information from companies and individuals by issuing civil investigative demands (CIDs). A CID is an official demand for documentary material, tangible things, reports, answers to written questions, and/or oral testimony, which if necessary, the Bureau can seek to enforce in federal court.
Depending upon the circumstances surrounding a particular investigation. Generally, staff should require certifications and obtain testimony under oath even when seeking evidence voluntarily.

The Bureau's rules for issuing and enforcing CIDs are in Section 1052 of the Dodd Frank Act and in the Rules Relating to Investigations in 12 C.F.R. part 1080 (the Rules). Among other things, the statute and Rules specify the procedures that recipients of CIDs are to follow when seeking to modify or set aside a CID. This policy is intended to provide guidance for handling issues relating to CIDs. Before issuing a CID, Staff should review the relevant portions of the statute and Rules.

Issuing Civil Investigative Demands

THE CID FORM

The operative demand document in a CID package is the CID form[1] signed by the Enforcement Director or a Deputy Enforcement Director. On the form, Staff should enter the CID recipient's full name and address in the "To" field. Staff should research the company's corporate records to ensure the use of the company's full legal name, including "Corp." or other legal structural designation, as well as any appropriate additional designations such as "also d/b/a (doing business as)" or "formerly known as." If the company consists of more than one legal entity, Staff should send separate CIDs to each entity at the outset of CID issuance. This practice reduces the risk
that the recipient will consider certain materials to be beyond the scope of the CID because they are retained by a different legal entity.

Staff should check the appropriate boxes in the "Action Required" section of the CID form. If sending a CID for oral testimony, Staff should include under "Bureau Investigators" the names of each individual who may take testimony during the hearing. For additional guidance, including information about the location of investigational hearings, Staff should review the policy on Taking Testimony.

---

1 (b)(7)(E)

CID NOTIFIC ATION OF PURPOSE

Pursuant to 12 U.S.C. § 5562(c)(2), "[e]ach civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation." 12 C.F.R. § 1080.5 further states that "Any person compelled to furnish documentary material, tangible things, written reports or answers to questions, oral testimony, or any combination of such material, answers, or testimony to the Bureau shall be advised of the nature of the conduct constituting the alleged violation that is under investigation and the provisions of law applicable to such violation." This "Notification of Purpose" should be included in each CID issued. The Notification of Purpose on the CID form should comply with the statutory and regulatory requirements above and should match the "Statement of Purpose" in the Opening Investigation Memorandum. If the scope or circumstances of the investigation have changed since opening the investigation, Staff should consult the LD or ALD supervising the investigation about making appropriate changes to the description in both the Statement of Purpose and any subsequent Notifications of Purpose through an amendment to the Opening Investigation Memorandum.

For guidance on the content of a Notification of Purpose, Staff should review the policy on Complying with Rule of Investigation 1080.5 [Notification of Purpose].

Unless other designation is deemed appropriate, Staff should list their Deputy Enforcement Director as the Custodian of Records and the paralegal assigned to the investigation as the Deputy Custodian. All attorneys assigned to the investigation should be listed as Bureau Counsel.

The Requests

During an investigation, the subject of the investigation or a third-party may be compelled to produce documents, tangible things, reports and answers to written questions, and oral testimony. Staff should carefully consider what requests for information to include in a CID. While seeking what is needed, Staff should consider the burden the CID will impose upon the recipient. A CID should be narrowly tailored to solicit the information necessary for the investigation. If Staff later determines that additional information is needed from the recipient, Staff may issue another CID or request that the CID recipient provide the information voluntarily.

Staff should use the CID templates[2] for the definitions, instructions, and other potentially relevant items.

A CID for the production of documentary material or tangible things[3] should describe each class of material requested with definiteness and certainty. A reasonable return date for the material should be provided. CID recipients should comply with the detailed instructions relating to the productions of documents, including the Document Submission Standards.[4] The instructions should be attached to each CID. Similarly, in a CID for written reports or answers to questions, the CID requests should describe the material requested with definiteness and certainty and specify the return date.

CIDs for oral testimony[5] should provide the date, time, and place for the investigational hearing and identify the Bureau investigators who will take the testimony. CIDs for oral testimony may either identify a specific individual from whom Staff seeks testimony, or describe particular matters for examination for which the entity must designate one or more individuals to testify on its behalf. As described in Rule 1080.6(a)(4)(ii), the testimony of the designated individual is binding upon the entity. Staff should consider, on a case-by-case basis, which type of CID for oral testimony is best-suited to the investigation. Additional procedures for investigational hearings can be found in Rules 1080.7 and 1080.9.

CID TO THIRD PARTIES

When Staff is considering proceeding *ex parte* and does not want to provide notice to the subject of the investigation, Staff may want to gather information from third parties. CIDs to third parties include a request to the recipient, found in the "Instructions" section, to keep the CID confidential. However, the confidentiality of CIDs is not assured. Note that electronic service providers may inform their customers about requests made under ECPA.

---

2 (b)(7)(E)

3

4

5

Even in noticed investigations, it is often helpful to gather facts from other sources to ensure that the evidence is complete. Examples of third-party requests include CIDs to:

- ISPs, web hosts, or domain name registrars to determine who controls a particular website (*e.g.*, GoDaddy, Domains by Proxy);
- Telephone companies to determine who owns certain telephone numbers;
- Banks for account information;
- FedEx for account information; and
- Marketing, advertising, payment processing, building management, office equipment leasing or other service providers.

Compliance with ECPA, RFPA, and SBREFA

Staff should ensure that each CID request complies with the Electronic Communications Privacy Act (see ECPA Policy) and the Right to Financial Privacy Act (see RFPA Policy).

As part of its compliance obligations under the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), the Bureau provides small businesses with notice that they can contact the Small Business Administration's National Ombudsman regarding the fairness of the Bureau's enforcement and compliance activities. This notice is included in the CID form and will be provided to all entities to which Staff sends a CID. To the extent Staff sends an informal request for information to a small business, however, Staff should include the following notice in the access letter:

> *RIGHT TO REGULATORY ENFORCEMENT FAIRNESS*
>
> *The Bureau is committed to fair regulatory enforcement. If you are a small business under Small Business Administration standards, you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888- 734-3247) or www.sba.gov/ ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.*

CID Approval

CIDs must be signed by the Enforcement Director or a Deputy Enforcement Director. Once a CID has been signed, Staff should forward the CID package, including the signed CID form, to the Enforcement Director via the Litigation Review Inbox (Litigation_Review_Inbox@cfpb.gov). Staff are responsible for uploading the signed CID package into the ENForce matter management system and submitting it to the LD for approval prior to sending the CID package to its intended recipient. The Enforcement Front Office will conduct monthly ENForce CID audits to ensure that all CIDs are entered into the ENForce system. For entities supervised by the Bureau, Staff should provide notice to Supervision before serving a CID.

The CID Package

Staff should prepare a CID package to serve on the CID recipient. This CID package may include the following items, as appropriate:

- Signed CID Form
- CID definitions and instructions
- Certificates of Compliance
- Business Records Certificate
- Document Submission Standards
- Rules Relating to Investigations (12 C.F.R. Part 1080)
- Certificate of Compliance with RFPA
- Notice to Persons Supplying Information

Staff may choose to send a cover letter with the CID package. For additional information regarding the items in the CID package, see related policies and the CID checklist.[6]

6 (b)(7)(E)

Service

After the CID has been signed, Staff should serve one copy of the CID package on the CID recipient consistent with the service procedures in Section 1052(c)(8). In most situations, Staff should send the CID package by certified mail, return receipt requested, to the CID recipient's principal place of business. *See* 12 U.S.C. 5562(c)(8)(C). In-person service upon an individual authorized to accept service or service to the principal office or place of business is also permissible. *See* 12 U.S.C. 5562(c)(8)(A)-(B).

In addition to certified mail, Staff may send a courtesy copy of the CID package by another method, such as UPS overnight mail, email, or fax. The sending of a courtesy copy through alternative delivery means depends on whether Staff has had prior contact with the CID recipient or its counsel and whether Staff knows how the CID recipient agrees to accept service. If Staff obtains agreement from the company or from opposing counsel to accept service through another method, Staff should memorialize the agreement in writing.

Regardless of the method of service used, request and retain the tracking information, as it may be needed later to demonstrate service. Generally, CIDs should be served by certified mail. Staff should also consider serving the CID by overnight delivery with a signature required, although this method of service, alone, does not satisfy the service requirement.

> It may be helpful to determine whether CIDs have been issued to the recipient in the past. Information about past CIDs should be available through the Matter Management System.

Meet and Confer

After the CID recipient has been served, the Rules require the recipient to meet-and- confer with Staff to discuss CID compliance. Unless the meet-and-confer requirement has been waived by a Deputy Enforcement Director, the meeting must take place within 10 calendar days or before the deadline for filing a petition to modify or set aside the CID. *See* 12 C.F.R. 1080.6(c). This initial meet-and-confer is often the juncture at which Staff will address any requests for extensions or alterations, which are discussed in more detail below.

At the meet-and-confer, the Rules require that the CID recipient make available personnel with the knowledge necessary to resolve any issues relevant to compliance with the CID. This would include individuals knowledgeable about the CID recipient's information or records management systems and organizational structure. *See* 12 C.F.R. 1080.6(c)(1). Staff may include in the meet-and-confer additional colleagues, including members of the Litigation Support Team, in order to fully discuss and address records management and document submission issues.

At the meeting or another appropriate time, discuss with the CID recipient any potential production of Personally Identifiable Information (PII). Ensure that the recipient understands that such information must be provided in an encrypted format. If hard copy records containing PII are to be provided, other adequate protection must be used. Before arranging for the receipt of sensitive PII or sensitive health information, consider whether the information is needed. For additional guidance regarding encryption, Staff should review the Document Submission Standards.[7]

Follow-up emails or letters should be used to memorialize any proposed agreements made with a CID recipient or counsel during the meet-and-confer and any other communications. Whenever possible, more than one attorney or Bureau Investigator should be present during oral communications with the recipient or their counsel. The second Staff member should take notes and serve as a witness to the representations made during the conversation.

Staff should inquire about a CID recipient's document-retention and destruction policies. The model CID instructions require that during the pendency of the investigation and any related enforcement action, the CID recipient suspend its usual document retention policies with regard to potentially relevant materials.

Requests to Modify CIDs

A CID recipient may seek the Bureau's agreement, by negotiation or petition, to alter the terms of a CID. Such requests may include requests for extension of time for compliance, limiting the scope of a particular request or set of requests, or otherwise changing the terms of compliance with a CID. 12 C.F.R. § 1080.6(d) authorizes the Enforcement Director and Deputy Enforcement Director to negotiate and approve the terms of satisfactory CID compliance and to extend the time to comply for good cause.

---

7 (b)(7)(E)
(b)(7)(E)

All requests for extension of time or for modification to the CID terms should be made in writing and should include all factual and legal information necessary to support the request for extension or modification. The attorney who objects to a CID must sign any objections. Counsel for the petitioner is required to attach a signed statement to any petition, representing that counsel has conferred with counsel for the Bureau in a good-faith effort to resolve by agreement the issues raised by the petition, and has been unable to reach such an agreement. Staff should engage in negotiations with petitioner's counsel to the extent that the requests being made are reasonable.

With regard to requests for extension of time, Staff should consider negotiating a staggered production schedule permitting the CID recipient to produce specified information on a rolling basis. To the extent that Staff negotiates the form of electronically stored information (ESI) production, a member of the Litigation Support Team should be included in the discussions. Note that Bureau investigators may, without serving the petitioner, provide the Director with a statement setting forth factual and legal responses to a petition for an order modifying or setting aside the CID. *See* 12 C.F.R. § 1080.6(e)(3).

At all times during CID compliance negotiation, Staff should make clear to petitioner's counsel that any preliminary agreement is subject to final approval by the Enforcement Director or Deputy Enforcement Director. The proposed agreement should be memorialized in a letter detailing modifications or permitting additional time for CID compliance. The letter should be signed by the Enforcement Director or Deputy Enforcement Director.

Petitions to Modify or Set Aside CIDs

Pursuant to 12 C.F.R. § 1080.6(e), the CID recipient may file a petition to modify or set aside a CID. The petition must be filed within 20 days of CID service or by the return date if that date is less than 20 days from the date of service. The petition must be filed with the Executive Secretary of the Bureau with a copy sent to the Enforcement Director. Before filing a petition, counsel for the petitioner must confer with Staff in good faith in an effort to resolve the issues. The Enforcement Director and Deputy Enforcement Director are authorized to extend the time within which to file a petition to modify or set aside a CID. *See* 12 C.F.R. § 1080.6(e)(2). Petitions and resulting Director's orders in response are made public unless for good cause the Bureau determines otherwise. *See* 12 C.F.R. § 1080.6(g).

Whenever possible, Staff should undertake steps to reduce the likelihood of a petition to modify or set aside a CID. One strategy is to ensure at the outset that the CID is tailored to the needs of the investigation and is not overbroad. Staff should also be amenable to working with the CID recipient to narrow the CID, as described above, consistent with the needs of the investigation.

Enforcement of Civil Investigative Demands

If a CID recipient fails to comply with a CID, Staff may seek enforcement in federal district court. Enforcement will typically represent the Bureau in CID enforcement actions, in coordination and consultation with Legal, unless there is a specific reason for Legal to litigate the matter.

Productions

A CID recipient must make a CID response under a sworn certificate attesting that all of the requested information in the recipient's possession, custody, or control has been produced. Certificates of Compliance for Requests for Documents and for Interrogatory Answers and Reports[8] should be included in the CID package. If a CID recipient withholds responsive information, it must assert a claim of privilege and provide a schedule of the items withheld. As to each item the recipient must state: the type, specific subject matter, and date of the item; the names, addresses, positions, and organizations of all authors and recipients of the item; and the specific grounds for claiming that the item is privileged. Both the person who submits the schedule and the attorney stating the grounds for a claim that any item is privileged must sign it. *See* 12 C.F.R. § 1080.8(a). Compliance with 12 C.F.R. § 1080.8(a) is in lieu of filing a petition for an order modifying or setting aside a CID pursuant to 12 C.F.R. § 1080.6(e).

8 (b)(7)(E) (b)(7)(E)

If during CID production, the recipient inadvertently discloses privileged materials, the privilege is not waived if the disclosure was inadvertent; the privilege holder took reasonable steps to prevent disclosure; and the privilege holder promptly took reasonable steps to rectify the error, including notifying a Bureau investigator of the claim of privilege or protection and the basis for it. *See* C.F.R. § 1080.8(c).

Material produced pursuant to a CID is confidential and any disclosure of the information outside the Bureau must proceed pursuant to the Bureau's Rules on the Disclosure of Records and Information at 12 C.F.R. Part 1070.

When appropriate, Staff may negotiate an agreement with the CID recipient to produce its privilege log on a rolling basis, tracking any agreed-upon staggered production of documents. The CID recipient may request a deferral agreement which provides that it does not have to produce a privilege log until the Bureau files a complaint in the matter. Staff should consult with the Deputy Enforcement Director or Assistant Litigation Deputy regarding such requests.

As stated in the model CID instructions and described in the Document Submission Standards, CID recipients should produce all materials in electronic format. Staff should make a plan for the intake of materials—particularly ESI—in advance (*e.g.*, loading ESI into Relativity and coordinating with litigation support).

For samples of letters in response to requests to modify or extend time to file a petition, requests for third-party fees, or for CID cover letters or withdrawal letters, click here or see the file on SharePoint.[9]

"Notice to Persons" Supplying Information Form [Witness Rights]

During an investigation, when Staff request documents, data, or answers to questions voluntarily or under oath—whether in writing or in an investigational hearing or deposition—certain Constitutional and statutory rights of witnesses may be implicated. The Notice to Persons Supplying Information (Notice to Persons) form1 should be provided to prospective witnesses as set forth in this policy.

9 (b)(7)(E)
(b)(7)(E)

Staff should include the Notice to Persons form when issuing a CID or a letter or other written request for voluntary production of documents or data. For CIDs, include the form in the CID package. For letters and other written requests, include the form in the letter, or otherwise transmit the form simultaneous with the transmittal of the letter or request.

During the preliminary stage of the investigational hearing, Staff should mark the Notice to Persons form as the first exhibit. Bureau counsel should ask the witness questions sufficient to confirm that first, the witness previously received the Notice to Persons form, and second, the witness previously reviewed the form, or if not, has been given an opportunity to review it in the hearing. Also, in cases where a person not represented by counsel has been issued a CID or voluntary request other than for oral testimony, Staff may want to confirm with the witness that he or she received, reviewed, and understood the Notice to Persons form.

It is not necessary to provide the Notice to Persons form to consumers and other third-party witnesses participating in informal, voluntary telephone interviews. However, in certain circumstances Staff may want to consider providing the form to such a witness and discussing it briefly with him or her prior to the interview.

Complying with Rule of Investigation 1080.5 [Notification of Purpose] (updated April 2019)

Section 1052(c)(2) of the Dodd-Frank Act, 12 U.S.C. § 5562, and Section 1080.5 of the Bureau's Rules Relating to Investigations, 12 C.F.R. § 1080.5, require that CIDs state "the nature of the conduct constituting the alleged violation that is under investigation and the provisions of law applicable to such violation." All CIDs should comply with this requirement.

At the outset of the investigation, Staff should draft a description (1) of the nature of the conduct constituting the alleged violation that is under investigation, and (2) the potentially applicable provisions of law. This language should be included in the Opening Investigation Memorandum[1] in the section headed "Statement of Purpose Pursuant to 12 C.F.R. § 1080.5."

1 (b)(7)(E)
(b)(7)(E)

If Staff seek to issue a CID, the statement of purpose from the Opening Investigation Memorandum[1] (as it may be amended) should be included in the section of the Bureau CID Form[2] labeled "Notification of Purpose Pursuant to 12 C.F.R. § 1080.5." Including this information in the CID is important to ensure that the CID is valid and would be enforced by a court if necessary. For more information about how this language is used in conjunction with CIDs, see the CID Policy.

This notification of purpose should typically identify one or more business activities subject to the Bureau's authority. For example, in an investigation of potentially unfair, deceptive, or abusive acts and practices under the CFPA, the notification of purpose will typically identify business activities that relate to a consumer financial product or service, such as collecting debts. In investigations where determining the extent of the Bureau's authority over the relevant activity is one of the significant purposes of the investigation, Staff may want to consider stating that in the notification of purpose. The notification of purpose should also describe, in general terms, the potentially wrongful conduct. For example, the potentially wrongful conduct in an investigation under the CFPA might be "making false or misleading representations to consumers." The description of the potentially wrongful conduct should be tailored to the circumstances of the investigations.

Finally, the notification of purpose should identify the potentially applicable provisions of law. Staff should endeavor to provide specificity in this part of the notification, although precise citations within the relevant statute or regulation may not always be practical in complex investigation.

Staff should be mindful that notifications of purpose must comply with 12 U.S.C. § 5562, 12 C.F.R. § 1080.5, and account for relevant case law on notifications of purpose. This includes any developments in such case law. Staff should consult the LD or ALD supervising the investigation if they have questions regarding how to comply with applicable law. Staff should revisit the statement of purpose if the purposes of the investigation evolve, through an amendment to the Opening Investigation Memorandum.

Staff should contact the Legal Division for advice on drafting notifications of purpose and consider any legal analysis provided by the Legal Division on notifications of purpose.

---

1 (b)(7)(E)

2

Taking Testimony

The Dodd-Frank Act authorizes the Bureau to conduct investigations to ascertain whether any person is or has been engaged in conduct that, if proved, would constitute a violation of federal consumer financial law. Section 1052 of the Dodd- Frank Act sets forth the parameters that govern these investigations. Investigations conducted by the Bureau may include witness testimony.

Compliance with Existing Laws

In connection with any witness testimony, Staff should exercise and perform their duties in accordance with the laws of the United States and the regulations of the Bureau. Prior to conducting an investigational hearing, Staff should be familiar with Section 1052 of the Dodd-Frank Act, which grants the Bureau authority to conduct investigations, and the Rules Relating to Investigations that implement Section 1052 of the Dodd-Frank Act, particularly 12 C.F.R. §§ 1080.7 and 1080.9 that address taking testimony. Staff should also comply with the Office of Enforcement's Notice to Persons Supplying Information policy. If Staff is asked whether a witness is the target of an investigation, Staff must adhere to the No Targets of Investigations policy. Staff should further be aware of the limitations the Electronic Communications Privacy Act (ECPA) and the Right to Financial Privacy Act (RFPA) place on the Bureau's ability to obtain and share information, and should refer to the policies related to those laws to determine if the limitations are applicable to the hearing.

The Rules Relating to Investigations draw from the investigative procedures of other law enforcement agencies, including the procedures used by the Federal Trade Commission (FTC), the Securities Exchange Commission, and the prudential regulators. In constructing these rules, the Bureau drew most heavily from the FTC's investigative procedures, in part due to the similarities between Section 1052 of the Dodd-Frank Act and Section 20 of the FTC Act, 15 U.S.C. § 41. You, therefore, may find case law related to the FTC's rules pertaining to investigations and the FTC Act to be a useful resource if issues arise.

Preparing for an Investigational Hearing

IDENTIFY INVESTIGATORS

The Bureau investigator(s) that will conduct or be present at the investigational hearing should be the same as those identified in the CID. A Bureau investigator is any attorney or investigator of the Bureau charged with the duty of enforcing or carrying into effect any federal consumer financial law.

Staff should consider whether they want to take testimony with a partner or other Bureau investigators. If so, such a person should be listed on the CID.

CONTACT WITNESSES

Compelled Testimony

Issuing a CID is the only means for Staff to compel a witness to provide testimony in the course of an investigation. Please also review the Office of Enforcement's policy regarding issuing CIDs.

You are not limited to taking a witness's testimony in a single day if the circumstances of your investigation necessitate multiple days of testimony. If you know in advance multiple days of testimony are necessary, the CID should set forth multiple dates.

Voluntary Testimony

A witness may agree to provide testimony in a voluntary investigational hearing with a court reporter present to record and transcribe the testimony. To conduct a voluntary investigational hearing, a witness must consent to the hearing being governed by 12 C.F.R. Part 1080. In determining whether a voluntary investigational hearing is appropriate, Staff should consider that:

- The witness would be testifying voluntarily;
- The witness may decline to answer questions that are asked; and
- The witness would be free to leave at any time.

Petitions Challenging a CID

Petitions challenging the Bureau's authority to conduct an investigation or the sufficiency or legality of a CID should be submitted to the Bureau in advance of the investigational hearing in accordance with 12 C.F.R. § 1080.6(e). Arguments in support of any such petition at the investigational hearing are not permitted.

ARRANGE LOCATION AND TRANSCRIPTION SERVICES

Staff should select a location for an investigational hearing in the judicial district of the United States in which the witness resides, is found, or transacts business, unless otherwise agreed upon by the Bureau investigator and the witness.

Staff are responsible for reserving a location for the investigational hearing. Absent compelling circumstances, Staff should first contact federal and state government offices in the area to inquire about possibly reserving space in those offices. If Staff are unable to reserve space at a federal or state government office, then Staff may reserve a space through the court reporting vendor. As a last resort, Staff may use their Government Travel Card to pay for the cost of reserving the space. Staff should fill out a Travel Approval Form, which requires approval from the supervising Assistant Litigation Deputy (ALD), prior to incurring the expense. Staff should contact the Office of Enforcement's Administrative Officer with questions regarding the Travel Approval Form and space reservation process.

Staff are responsible for making the appropriate arrangements to have a court reporter attend the investigational hearing and obtaining a transcript. The paralegal assigned to the investigation is authorized to obtain a court reporter. Staff should notify the appropriate paralegal of their need for a court reporter as far in advance as possible, but no later than two weeks in advance of the hearing unless there are exigent circumstances.

MEET AND CONFER

The Office of Enforcement's policy on meet and confers can be found in the CID policy. This section is meant to supplement, not replace, the meet and confer procedures in the CID policy. The following is a list of topics Staff should cover in the course of a meet and confer after issuing a CID compelling testimony:

- Advise the witness and counsel that investigational hearings are governed by 12 U.S.C. § 5562 and its implementing regulations, and objections that may be properly raised are limited as set forth in the regulations;
- Advise that only the recording arranged and procured by the Bureau for the hearing is permitted, and no other recording may be created;

- If Staff would like a person not listed in 12 U.S.C. § 5562(c)(13)(B) to attend the hearing, ask the witness and counsel if they consent to the presence of such person. The attendance of a person not listed in 12 U.S.C. § 5562(c)(13)(B) should be agreed upon in advance of the investigational hearing; and
- Where a CID requires testimony from an entity, pursuant to 12 C.F.R. § 1080.6(a)(4)(ii), Staff need a list of the individuals designated to testify on the entity's behalf and the subject areas each designee will be testifying about in advance of the hearing.

Conducting an Investigational Hearing

PREPARING EXHIBITS

Staff should identify and prepare the requisite number of copies of the exhibits they wish to use in the course of the hearing.

In order to introduce a new exhibit in an investigational hearing, Staff should do the following:

- State that they are handing a document to the court reporter to mark it as exhibit #[Fill in Number].
- Describe the document, *e.g.*, what it is, the date, the parties to the document if relevant, and the Bates numbers if applicable.
- Instruct the court reporter to attach an exhibit sticker, containing the matter number followed by the exhibit number that corresponds to the chronological introduction of the document at the hearing (*e.g.*, 2015-xxxx-xx Ex. 1, 2015 - xxxx-xx Ex. 2). After the first investigational hearing, exhibits will be marked in chronological order starting with the number that follows the last number entered in the most recent investigational hearing. The court reporter should mark the exhibit sticker with their initials and hand it back to the Staff.
- Present the exhibit to the witness and continue the line of questioning.

In order to use a previously marked exhibit, Staff may hand the witness the previously marked exhibit, reference the exhibit by its number, and continue with the line of questioning.

The court reporter may include a list of the exhibits introduced in the investigational hearing in the transcript, but *is not permitted to retain the exhibits.* Staff should collect all of the exhibits at the conclusion of the hearing.

To assist in tracking exhibits and the witnesses that have identified them, Staff can keep a chart that lists the exhibits by number, along with a brief description and a list of witnesses that have identified the exhibit.

PARTIES PERMITTED TO ATTEND INVESTIGATIONAL HEARINGS

Only the parties in the following list are permitted to be present at an investigational hearing. Before testimony is given, the Bureau investigator should exclude all other persons from the hearing room.

- The Bureau investigator(s)
- The person giving testimony
- The attorney for the person giving testimony
- Any investigator or representative of an agency with which the Bureau is engaged in a joint investigation
- Any court reporter taking testimony
- At the discretion of the Bureau investigator, and with the consent of the person giving testimony, persons other than those listed above for either side

COUNSEL REPRESENTING THE WITNESS

A person compelled to give oral testimony may be accompanied, represented, and advised by counsel at the investigational hearing. If the witness is being represented by counsel, advise the witness and counsel they will be asked at the hearing to state on the record that counsel represents the witness. While counsel for the witness may represent another party in the investigation (*e.g.*, the witness's employer), counsel must be appearing as the witness's attorney to be present at the investigational hearing.

To the extent Staff are aware that counsel for the witness is representing other parties in the investigation, and this representation raises a potential conflict of interest, Staff should consult with the supervising ALD regarding the potential conflict of interest, and determine how the issue should be addressed, if at all.

PRIOR TO COMMENCING TESTIMONY

Staff should advise the witness and witness's counsel that the Bureau investigator controls the record at the investigational hearing, and to the extent either the witness or witness's counsel wishes to go off-the-record, those requests should be directed to the Bureau investigator. It is in the Bureau investigator's discretion to grant or deny any such request.

The Bureau investigator should provide the court reporter with the caption of the investigation. Captions for investigations should follow the same convention as matter folder names, explained in Maintaining Matter Folders. To the extent possible, Staff should assist the court reporter with the spelling of proper names and unusual words.

COMMENCEMENT OF THE RECORD

In commencing an investigational hearing, the Bureau investigator should:

1. Have the witness state his or her name for the record, and state whether he or she is represented by counsel;

2. If the witness is represented by counsel, have counsel identify himself or herself, and state that counsel is representing the witness;

3. Have any person not from the Bureau identify himself or herself, or Staff may identify these additional parties by name, address, and employer;

4. Have any person from the Bureau identify himself or herself, or Staff may identify these additional parties;

5. If any person not listed in 12 U.S.C. § 5562(c)(13)(B) is in attendance, confirm the witness's consent to the presence of such person;

6. Ask the witness if he or she had the opportunity to review the CID compelling his or her testimony and the Notice to Persons Supplying Information provided to the witness, and if the response is no, provide the witness time to review both documents before continuing;

7. For a witness appearing as an individual designated to testify on behalf of an entity, confirm the subject areas that the designee will be testifying about;

8. Advise the witness and counsel that this is an investigational hearing governed by 12 U.S.C. § 5562 and its implementing regulations, and objections that may be properly raised are limited as set forth in the regulations; and

9. Advise that only the recording arranged and procured by the Bureau is permitted, and no other recording may be created.

TESTIMONY GIVEN UNDER OATH AND TRANSCRIBED

Witness testimony should be given under oath or affirmation before an officer authorized to administer oaths and affirmations by the laws of the United States or of the place at which the examination is held. The testimony should be taken stenographically and transcribed.

If the testimony will be recorded by audiovisual means, Staff should consult with the supervising ALD prior to incurring the additional expense of having the testimony videotaped. Staff should provide advance written notice to the witness or witness's counsel, as appropriate. At an investigational hearing, only the recording arranged and procured by the Bureau is permitted. No other recording may be created.

After receiving a copy of the transcript, the Bureau investigator should ensure the court reporter provides, as part of the transcript, a certification that the witness was duly sworn and that the transcript is a true record of the testimony given by the witness.

COUNSEL'S ABILITY TO ADVISE THE WITNESS

The Bureau investigator should permit the attorney to advise the witness, in confidence, either upon the request of the witness or upon the initiative of the attorney, with respect to any question asked of the witness where it is claimed that a witness is asserting privilege. Except in the limited circumstance of claiming privilege to refuse to answer, counsel may not otherwise consult with a witness while a question is pending. *See* 12 C.F.R. § 1080.9(b)(1).

OBJECTIONS MADE AT THE INVESTIGATIONAL HEARING

The witness or counsel for the witness may only refuse to answer or object to questions on the grounds of a constitutional or other legal right or privilege, including the privilege against self-incrimination. If a witness refuses to answer a question on the grounds of privilege against self-incrimination, Staff should follow the Office of Enforcement's policy on a witness asserting his or her Fifth Amendment right.

Staff may want to remind the witness and counsel that this is an investigational hearing governed by 12 U.S.C. § 5562 and its implementing regulations, and objections that may be properly raised are limited as set forth in the regulations. Staff may also want to inform counsel or the witness that an investigational hearing is not a deposition, and it is not governed by the Federal Rules of Civil Procedure.

Counsel is prohibited from making statements on the record, but may ask the Bureau investigator that the witness be allowed to clarify any of his or her answers. It is in the Bureau investigator's discretion to grant the request. The proper time for a witness to clarify his or her answers is at the end of the examination.

AVOIDANCE OF DELAY OR DISORDERLY CONDUCT

The Bureau investigator is authorized to take action in the course of an investigational hearing to avoid delay, to prevent disorderly, dilatory, obstructionist, or contumacious conduct, and to restrain or prevent contemptuous language. If counsel for a witness refuses to conduct himself or herself in accordance with these obligations or any other obligation under 12 C.F.R. Part 1080, Staff may state, for the record, counsel's conduct, and report the conduct to the supervising ALD for further action, if any.

Remember, when recounting counsel's conduct, you are creating a record to support a petition to enforce the CID or to inform the Director on whether to issue an order requiring counsel to show cause why he or she should not be suspended or disbarred from practice before the Bureau, so it is essential that you cover all of the relevant behavior and events. Be particularly aware that the transcript will not convey tone, the volume of counsel's voice, or nonverbal communications, so to the extent such conduct is relevant, you must describe that conduct for the record.

If counsel for the witness is obstructing the proceeding, you should consider whether counsel is responding in this manner to a particular topic or line of questions. If it is a particular topic or line of questions that is causing an issue, you should address the other areas you want to cover with the witness first, and then proceed with questions on the topic drawing obstructionist reactions. To the extent that you find yourself at an impasse with counsel, after creating a record of his or her conduct, you may advise counsel that an investigational hearing concludes when you are satisfied that the witness adequately complied with the CID, and to the extent the Bureau finds the events that transpired to amount to noncompliance, the Bureau has the ability to enforce the current CID.

DOCUMENTING AN UNPREPARED ENTITY WITNESS

If a CID is issued compelling entity testimony, the individual(s) designated by the entity must be able to "testify about information known or reasonably available to the entity." 12 C.F.R. § 1080.6(a)(4)(ii). If the witness is generally unable to provide information about a specific subject area, Staff should establish for the record that the witness was generally unprepared by asking questions related to:

- The amount of time the witness spent preparing for his or her testimony;
- Who the witness spoke to in order to prepare for his or her testimony; and
- The volume of documents the witness reviewed in preparation for his or her testimony.

INTERMIT TENT BREAKS

Staff may permit breaks in the course of an investigational hearing as necessary.

CONCLUDING THE INVESTIGATIONAL HEARING

The investigational hearing should not be adjourned unless and until the Bureau investigator is satisfied that the witness adequately complied with the CID. Staff should collect all copies of documents provided at the conclusion of the investigational hearing.

In closing an investigational hearing, the Bureau investigator should ask the witness if he or she is willing to waive his or her right to examine and read the transcript, which is permitted under 12 U.S.C. § 5562(c)(13)(E)(ii).

WITNESS FEE

Any witness compelled to testify at an investigational hearing is entitled to the same fees and mileage that are paid to witnesses in the district courts of the United States as set forth in 28 U.S.C. § 1821. Staff should contact the Office of Enforcement's Administrative Officer with any questions regarding payment of fees and mileage to a witness.

WITNESS'S RIGHT TO OBTAIN COPY OF TRANSCRIPT

Following an investigational hearing, the Bureau "shall furnish a copy of the transcript (upon payment of reasonable charges for the transcript) to the witness only, except that the Bureau may for good cause limit such witness to inspection of the official transcript of his testimony." 12 U.S.C. § 5562(c)(13)(G).

The Bureau should not provide a copy of the transcript to the witness or counsel, rather, the witness can only buy a transcript from the court reporter vendor with the approval from the Bureau. The court reporter should not provide a copy of any transcript without Bureau authorization.

A witness should submit his or her request in writing to a Bureau investigator present at the investigational hearing, within a reasonable time following the hearing. When a witness or witness's counsel requests a copy of the transcript, Staff receiving the request should authorize the court reporter to allow the witness to obtain a copy of the transcript (upon paying the vendor fees) unless Staff has reason to believe there is (or may be) good cause to provide the transcript for inspection only.

When Staff has reason to believe there is (or may be) good cause to refuse to provide a copy of the transcript, they should consult with their supervising ALD and LD about whether refusing to provide a transcript is appropriate under the circumstances, taking into account the considerations listed below. The determination of whether there is "good cause" to prevent a witness from obtaining a transcript should be made by the supervising LD, who will keep the Enforcement Director informed about any decisions in that regard.

While witnesses are generally allowed to obtain transcripts, the Office of Enforcement may determine that there is good cause not to provide a copy of a transcript where, among other potential circumstances:

- The witness is a third-party recipient, and the subject of the investigation is not aware of the investigation, the particular theories that the Office of Enforcement is considering, and/or the contents of the witness's testimony;
- There are specific articulable reasons to believe that provision of the transcript at that time would compromise a confidential investigation; or

- Other relevant considerations as articulated by the Staff at the time of the determination.

When a transcript is provided, Staff may, if appropriate, ask that the transcript not be shared with any other person until the investigation is complete. Such a request may be appropriate where the party requesting the transcript is not the subject of the investigation and where there is reason to believe that the requester would support the Office of Enforcement's goal of preserving the confidentiality of the investigation.

REVIEW AND SIGNING OF TRANSCRIPT

Once an investigational hearing is complete, the court reporter will prepare one original hardcopy bound transcript, one electronic transcript, and one e-Transcript version and transmit them to the Bureau. Staff should forward the original transcript to the Bureau custodian, who is identified on the CID and who generally will be the paralegal assigned to the investigation.

The Bureau investigator should then provide the witness a reasonable opportunity to review the transcript of his or her testimony. The witness has 30 days from the date the transcript was first made available, including the date the witness or witness's counsel received the transcript, to sign the Certification of Witness form[1] and return to the Bureau the original signed Certification of Witness, the copy of the transcript, and the Errata Sheet for Changes to Transcript,[2] if used by the witness.

When the Bureau decides to deny a witness's request to obtain a copy of the transcript, the witness should be provided the opportunity to examine the transcript of his or her testimony in a supervised location. Otherwise, a copy of the witness's transcript will be provided by the Bureau to the witness for examination, but any such copy must be returned to the Bureau. The procedures for both types of examinations are set forth below in greater detail.

---

1 (b)(7)(E)

2

Examination of a Transcript

The following steps should be followed for the review of the investigational hearing transcript:

- When the Staff instruct the paralegal to do so, the paralegal will email an e-Transcript version of the transcript to the witness or witness's counsel as directed. The e-Transcript version can be viewed and forwarded, but it cannot be saved or printed.
- Emailing the e-Transcript version is the usual method for transcript review. However, if for a specified reason Staff does not want to use the e-Transcript process, Staff can mail the bound copy of the transcript, IH Cover Letter for Transcript Review, IH Certification of Witness form, and IH Errata Sheet for changes to the transcript. Staff should track the package to ensure that they can account for the date of delivery. Since a witness has 30 calendar days to read, review, and sign the transcript, including the date of receipt by the witness or witness's counsel, it is important the Bureau has a record of the date the transcript was made available to the witness. Staff should make a calendar entry to follow-up after 30 days to determine whether the witness has returned the Certification of Witness and the transcript copy. Staff must make sure the witness has returned the copy of the transcript provided to him or her.
- Also in the email will be: (1) IH Cover Letter for Transcript Review;[3] (2) IH Certification of Witness form;[4] and (3) IH Errata Sheet[5] for changes to the transcript. (These and all investigational hearing-related forms can be found in the Templates and Forms folder on SharePoint.) The use of the Errata Sheet for Changes to Transcript satisfies the Bureau investigator's obligation under 12 U.S.C. § 5562(c)(13)(E)(iii) to enter and identify any of the witness's desired changes in form or substance to the transcript and that those changes are accompanied by a statement of reasons. Where Staff should insert the name of the investigation on a form, use the matter folder name dictated by the Office of Enforcement's policy on maintaining matter folders.

3 (b)(7)(E)

4

5

- If a signed Certification of Witness is not received within 30 calendar days, Staff should execute an IH Bureau Statement re Non-Signature form[6] (found in the Templates and Forms folder on SharePoint), and attach the document to the transcript. Staff signing the IH Bureau Statement re Non-Signature form fulfills the requirements under 12 U.S.C. § 5562(c)(13)(E)(v) to "sign the transcript and state on the record the fact of the waiver, illness, absence of the witness, or the refusal to sign."

Examination of a Transcript in a Supervised Location

When the Bureau decides to deny a witness's request to obtain a copy of the transcript, the Bureau investigator still needs to arrange for the review and signature of the witness. In a supervised location, Staff should provide the following to the witness for review and signature:

- A copy of the transcript;
- A cover letter, using the IH Cover Letter for Transcript Review Supervised template;[7]
- A Certification of Witness using the IH Certification of Witness form[8] with the fields completed (*e.g.*, the "In the Matter of"; "Witness Name"; "Hearing Date" and "Bureau Investigator(s)" fields); and
- An IH Errata Sheet[9] form for changes to transcript, with the fields completed (*e.g.*, the "In the Matter of"; "Witness Name"; "Hearing Date" and "Bureau Investigator(s)" fields). In place of the name of the investigation on a form, Staff should use the name of the matter folder.

All investigational hearing-related forms can be found in the Templates and Forms folder on SharePoint.[10]

(b)(7)(E)

The use of the IH Errata Sheet for changes to transcript satisfies the Bureau investigator's obligation under 12 U.S.C. § 5562(c)(13)(E)(iii) to enter and identify any of the witness's desired changes in form or substance to the transcript and that those changes are accompanied by a statement of reasons.

After the witness has completed the review, the Bureau investigator should collect the transcript, errata sheet, and signed certification form.

If the witness refuses to sign the transcript or provides a written waiver of signature, then the Bureau investigator should execute an IH Bureau Statement re Non-signature form[11] and attach the document to the transcript. Staff signing the IH Bureau Statement re Non-signature form fulfills the requirements under 12 U.S.C. § 5562(c)(13)(E)(v) to "sign the transcript and state on the record the fact of the waiver, illness, absence of the witness, or the refusal to sign."

11 (b)(7)(E)
(b)(7)(E)

Interacting with Whistleblowers (updated January 2019)

Tips from current and former employees and other industry insiders (such as competitors can serve as a valuable resource for the Office of Enforcement in identifying potential violations of federal consumer financial laws. Enforcement has a whistleblower tip hotline (855-695-7974) and email inbox (whistleblower@cfpb.gov) where individuals can provide tips concerning potential legal violations. Enforcement also received tips via mail, Consumer Response, and other internal and external sources. A team of on-call staff members (Whistleblower Team) handles the intake of incoming whistleblower tips. The primary role of Whistleblower Team Staff in receiving submissions is to document the information provided by tipsters and route the tips to Issue Team subject matter experts for review and determination of appropriate next steps.

Staff may receive whistleblower tips and/or interact with whistleblowers as part of casework or when tips are submitted directly to Staff, instead of to the whistleblower hotline or inbox. This section provides guidance on how Staff should route tips and engage with whistleblowers.

Routing Tips to Enforcement's Whistleblower Team

Tips need to be routed to Enforcement's Whistleblower Team to be processed and reviewed properly. Tips submitted to Staff instead of the whistleblower hotline, inbox, or Whistleblower Team, should be re-directed to the whistleblower inbox or ENF Administrative Operations Assistant so that they can be integrated into Enforcement's routine tip intake process.

Re-directing Consumer Complaints to Consumer Response

If the submitter is not a whistleblower but instead a consumer with a complaint about a financial institution or general inquiry, Staff should direct them to contact Consumer Response via the Consumer Response hotline at (855) 411-2372 or online complaint portal at https://www.consumerfinance.gov/complaint/.

Engaging with Whistleblowers

Staff should follow these best practices for the topics described below when engaging with whistleblowers:

Determining if Whistleblowers are Represented by Counsel

Staff should ask the individual if they are represented by counsel in relation to the information they are providing. If so, Staff should ask for the attorney's contact information to get approval to communicate directly with the individual. Staff should follow up with their ALD once they have spoken to counsel about next steps.

In the case of a current employee, if the employee responds that they are not represented by counsel in relation to the information they are providing, Staff should next ask whether the employee's company is represented by counsel in relation to the information the employee is providing. If the answer is yes, Staff should ask for the employee's title/position. If the employee responds that they are a manager or director of the company, Staff should end the conversation and consult with their ALD before proceeding in order to avoid any potential Rule 4.2 issues. If, based on the current employee's response, Staff are unsure whether the employee is a manager or director, staff should terminate the conversation and consult with their ALD before proceeding.

In the case of a former employee, Staff should avoid soliciting information that implicates the former employer's attorney-client privilege. Staff should not inquire about any legal advice received by the former employee from in-house counsel.

Making Representations to Whistleblowers

Staff should not make any promises or representations to individuals regarding any potential action that the Bureau might take in response to the information provided. Staff should only inform individuals that they may be contacted if additional information is required.

While communicating with individuals, Staff should refrain from providing legal advice and clearly articulate that the Bureau does not represent individual consumers. Staff should also refrain from opining on whether the conduct described constitutes a violation of law.

Staff should not promise individuals that their information will be kept confidential. Staff can inform individuals that the Bureau takes their privacy seriously and will keep their identities confidential to the extent permitted by federal law.

Obtaining Documents from Whistleblowers

Staff should never implicitly or explicitly communicate to whistleblowers that they should: (a) obtain documents to provide support for their allegations; or (b) submit privileged documents to the Bureau.

If whistleblowers volunteer that they have documents they are willing to provide the Bureau, Staff should consult with their ALD before accepting the documents to discuss any potential legal or ethical issues associated with accepting the materials.

When appropriate, Staff should instruct individuals to submit any additional information through the Whistleblower hotline or inbox.

Whistleblower Protections

If individuals indicate they have suffered adverse job actions, Staff should inform current employees that under the Dodd-Frank Act, they may be protected from termination or other forms of workplace retaliation. Staff should direct individuals to www.whistleblowers.gov or to call the U.S. Department of Labor Occupational Safety & Health Administration at (800) 321-6742 for more information. Staff should refrain from offering any legal advice to individuals on their potential claims.

Section 1057(a) of the Dodd-Frank Act prohibits "covered persons" or "service providers" from terminating or discriminating against employees for providing information to the Bureau about potential violations of the laws it enforces. Individuals who believe they have been terminated or discriminated against in violation of Section 1057(a) are required to file a complaint with the Secretary of Labor within 180 days of the alleged retaliatory conduct. The Secretary of Labor can award relief which may include reinstatement, back pay, and compensatory damages.

Responding to Consumer Inquiries

Unsolicited communications from consumers, including complaints and inquiries about completed enforcement actions, can provide the Bureau with valuable information regarding individual experiences with consumer financial products. Because the Office of Enforcement does not represent individual consumers, generally such communications should be routed to the Bureau's Office of Consumer Response.

While communicating with consumers, Staff should refrain from providing legal advice, including whether an individual may or may not be affected by a specific Bureau enforcement action, and from providing information about on-going investigations or internal Bureau policies and procedures.

Staff should clearly articulate that the Office of Enforcement does not represent individual consumers. Enforcement Personnel should encourage consumers to provide the unsolicited information, complaint, or inquiry to the Bureau [Consumer Response] by submitting a complaint through the Bureau website or by telephone. The contact information is as follows:

- https://www.consumerfinance.gov/complaint/
- 1 (855) 411-2372 (Toll Free)

If the unsolicited communication concerns a specific enforcement action, Staff should contact the Enforcement attorney handling the matter to determine if there are any other procedures that should be communicated to the consumer. (For example, the entity subject to an order may have a toll-free number available for consumers to ask questions about their accounts.) In addition to requesting that consumers provide the information to the Bureau through the appropriate Consumer Response channels, Enforcement Personnel should also suggest that consumers contact the entity if they are or were a customer of the entity.

If the unsolicited communication concerns an investigation or examination, after referring the consumer to the consumer response options above (Consumer Response portal), Enforcement Personnel should pass on the information to the attorney handling the investigation or supporting the investigation.

EX AMPLE RESPONSE

If an email response is appropriate, the following template maybe used:

> *Dear [CONSUMER]:*
>
> *Thank you for your email inquiry. We ask that you submit your [inquiry, complaint, information] online or by telephone as follows:*
>
> *http://www.consumerfinance.gov/complaint/1*
>
> *(855) 411- 2372 (Toll Free)*
>
> *The information you provide will help inform our work of protecting consumers.*
>
> *Sincerely, [NAME]*

No Targets of Investigations

At some point during most Bureau investigations, usually upon being contacted by Enforcement Staff, people will ask (directly or through counsel) whether they are the "target" of the investigation. The Staff's answer to this question should always be "No, Bureau investigations do not have targets."

There are many reasons for this uniform response. "Target" is a term of art in criminal law that carries a specific meaning with legal consequences. In the grand jury process, individuals are often identified as the target of a criminal investigation, and that characterization has important Fifth and Sixth Amendment implications. Because Bureau investigations are civil, the notification of "targets" is not required. Furthermore, the term "target" incorrectly implies that the objective of an Enforcement investigation is to reach a specific result (legal action against the target) rather than to search for the truth. Although some parties involved in investigations eventually may be named as defendants or respondents in subsequent litigation, the Bureau does not have targets of its preliminary inquiries or investigations. Therefore, Staff should never use the designation "target" to describe the subjects of Enforcement investigations.

NORA—Notice and Opportunity to Respond and Advise

The Notice and Opportunity to Respond and Advise (NORA) process affords people and entities (Persons) under investigation an opportunity to present their positions to the Office of Enforcement and the Bureau Director before the authorization of a lawsuit against them. It was modeled on similar procedures at other federal agencies, with modifications made to account for experience with those procedures over time and dissimilarities between those agencies and the Bureau. The NORA procedures strike a balance between fairness to Persons under investigation and protection of the public interest. The informal, discretionary framework of the NORA process allows the Bureau to retain its ability to respond to unlawful conduct in a timely fashion.

Purpose of the NORA Process

The primary objectives of the NORA process are to:

- Allow Persons under investigation the opportunity to be heard before the filing of a lawsuit in situations where delay will not unduly harm consumers;
- Help ensure that enforcement actions are based on sound policy, and that they effectively further the Bureau's priorities;
- Alert the Bureau to potential unintended and undesirable consequences of enforcement actions; and
- Help ensure that the Bureau is aware of any material facts relevant to both its investigations and contemplated enforcement actions.

Supervisor Approval

NORA recipients' requests for deviation from the standard NORA procedures, such as extensions of time, should be made in writing, clearly state the basis for the request, and be directed to the staff member who provided the NORA.

⚠ Before sending a recommendation memorandum about a proposed enforcement action to the Director, Staff should obtain ALD and LD approval to initiate the NORA process, or to determine that the NORA process should not be used. Staff must obtain the supervising Enforcement Director's approval before allowing any discretionary deviation from the NORA procedures described in the current NORA Bulletin.[1]

Initiating or Foregoing the NORA Process

The NORA process should be used in most cases when Staff expects to recommend a lawsuit, but Staff have discretion to forego the process, with approval from the Enforcement Director, if there is a valid reason to do so. When used, Staff should issue a NORA before sending an action memorandum to the Director.

Staff should be aware that sending a NORA may raise issues relevant to other Bureau units, and therefore should consider whether to inform those units prior to issuing a NORA.

During joint investigations with other federal or state agencies, Staff should determine whether the issuance of a NORA might create problems for a partner agency, or whether a partner agency might have its own notice requirements, and if so, should consider such issues when deciding whether or when to issue a NORA.

Pursuant to the Bureau's Litigation Hold policy,[2] if the obligation to preserve evidence has not already arisen and the Bureau has not yet issued a litigation hold, the issuance of a NORA triggers the requirement of a litigation hold.

If prompt enforcement action is necessary to protect consumers, providing a NORA and waiting for a submission may not be practical. For example, it is unlikely that a NORA would be appropriate before a recommendation to file an emergency action requesting a temporary restraining order and asset freeze to stop an ongoing fraud.

---

1 (b)(7)(E)

2

The primary considerations in determining whether or when to provide a NORA are:

- Whether the investigation is substantially complete as to the NORA recipient; and
- Whether immediate enforcement action is necessary for the protection of consumers.

Risks to consider when providing a NORA include:

- Alerting other potential defendants, thereby jeopardizing emergency action against them, or other aspects of an ongoing investigation;
- Flight of potential parties;
- Dissipation of assets; and
- Destruction of records.

Method of Providing a NORA

⚠ Staff should provide the current NORA Bulletin[3] and Notice to Persons Supplying Information[4] to every NORA recipient. The bulletin and form must be attached to every NORA letter;[5] if no NORA letter is sent, the bulletin and form must be delivered to the NORA recipient by email.

Unless there is a reason to do otherwise, a NORA should be delivered by a telephone call to the attorney representing the Person under investigation (or directly to an unrepresented Person), followed by a letter memorializing the telephone conversation. Staff may elaborate on the substance of the claims and other information in the telephone call, but should follow the template when sending the NORA letter. The following information should be conveyed in the telephone call and/or letter:

---

3 (b)(7)(E)

4 (b)(7)(E)

5 (b)(7)(E)

1. The Office of Enforcement is considering recommending or intends to recommend that the Bureau file an action or proceeding against the Person;

2. Identification of the charges Staff is considering recommending to the Director, including the specific laws Staff believes were violated, a general description of the violative conduct and key evidence uncovered in the investigation, and any other information necessary to make the NORA meaningful;

3. A general description of the types of relief, remedies, and penalties available to the Bureau in the contemplated action;

4. The NORA recipient has the opportunity to provide a voluntary statement explaining why the Bureau should not bring an action against them;

5. The deadline for notifying the Office of Enforcement of the Person's intention to make a NORA submission (the deadline should generally be seven days after the initial NORA notification, but it may be extended);

6. The deadline for submitting the NORA materials (the deadline should generally be 14 days after the initial NORA notice, but it may be extended or shortened);

7. The restrictions/guidelines for NORA submissions, including their length (the length should be no more than 40 pages, but it may be expanded) and the requirement that any factual assertions relied upon or presented in the written statement must be made under oath by someone with personal knowledge of such facts;

8. The NORA submission will be provided to the Director together with any request for authority to sue;

9. Instructions regarding the Office of Enforcement staff member to whom the NORA submission should be sent, including that staff member's email and mailing address; and

10. Any NORA submission may be used by the Bureau in any action or proceeding that it brings and may be discoverable by third parties in accordance with applicable law.

Rejecting a Noncompliant NORA Submission

While a NORA gives its recipient the opportunity to make a voluntary submission to the Bureau regarding proposed enforcement action, the Bureau may reject NORA submissions if:

- The submissions do not comply with the NORA submission requirements (*e.g.*, they exceed the length limitations specified in the NORA);
- The submissions are received after the submission deadline, and we have not granted a request for an extension of time; or
- The Person making the submission has limited its admissibility under Federal Rule of Evidence 408, or has otherwise limited the Bureau's ability to use the submission.

Providing NORA Submissions to the Director

⚠ Compliant NORA submissions should be provided to the Director along with any Staff recommendation of enforcement action against that Person.

Staff may, on their own initiative, with approval from the supervising Enforcement Deputy, provide any NORA submission to the Director at any time.

Requests to Review the Investigative File

NORA recipients may request to review portions of the Staff's investigative file. It is the Office of Enforcement's general policy to deny such requests.

⚠ Staff must consult with the supervising Enforcement Deputy if a NORA recipient makes a request to review portions of the investigative file, and should receive approval from the supervising Enforcement Deputy before granting such a request.

Meeting Requests

NORA recipients may request a meeting to discuss the substance of the Staff's proposed recommendation to the Director.

⚠ Staff should consult with the supervising Enforcement Deputy if a NORA recipient makes a request to meet with Staff or the Enforcement Director. Staff should receive approval from the supervising Enforcement Deputy before granting such a request.

A NORA recipient generally will not be accorded more than one post-NORA meeting. Any such meeting granted should be scheduled promptly to avoid any undue delay.

Offers of Settlement

⚠ Staff may accept unsolicited offers of settlement from NORA recipients, but may not engage in settlement discussions or express opinions to NORA recipients except as authorized by the Bureau's Enforcement Action Process. Staff must notify the Director of unsolicited settlement offers when making any related recommendation for enforcement action.

Submissions Outside of the NORA Process

Apart from the NORA process, Staff may ask for more information from a subject at any point in the enforcement process, to inform a request for settlement authority or for any other reason. To ensure that we obtain the information we need in the context of settlement negotiations, Staff may consult with the subject to obtain necessary information where such dialogue would be helpful and appropriate. Information provided by a subject for this purpose may be included in memos seeking authority to settle, sue, or settle/sue.

Closing an Enforcement Matter

A supervising LD may close a matter at his or her discretion with advance notice to the Assistant Director for Enforcement. Closing an investigation also requires subsequent notice to the following Bureau components: Supervision; Office of Fair Lending; Research, Markets, and Regulations; Legal Division; and Consumer Engagement.

The following procedures describe when and how Staff should recommend closing a matter and how a matter should be formally closed upon approval by an LD.

Closing a Research Matter

After the supervising LD has approved closing a research matter, Staff should fill out the form for closing a research matter.[1]

Staff should recommend the closure of a research matter as soon as it becomes clear that no investigation will be opened, even if every possible research action has not been completed.

Closing an Investigation

ACTIONS REQUIRED BEFORE CLOSING AN INVESTIGATION

Prior to closing every investigation, Staff should complete the following steps.

- Review and follow Enforcement's FOIA procedures to ensure compliance with FOIA.
- To the extent a litigation hold is in place, take appropriate steps to release the hold, including notifying all persons subject to the hold.
- Review and follow the Bureau's document retention and destruction policies to ensure the appropriate preservation, organization, and storage of physical and electronic documents collected or created during the investigation.
- Complete an Investigation Closing Memorandum,[2] have the supervising LD sign the memorandum, save it in the matter folder, and submit the closing memo in ENForce for approval. Once fully approved, the ENForce status of the matter will automatically change to "Closed."

---

1 (b)(7)(E)

2 (b)(7)(E)

- Notify third parties who received a document retention letter or were otherwise required to retain documents, including CID recipients that the matter is terminated and a litigation hold is no longer required.

The Investigation Closing Memorandum provides a record of how you conducted the investigation, a description of any legal action taken and its resolution, or an explanation of the reasons you decided to conclude it without enforcement action. The memorandum may be used to inform any evaluation of subsequent activity by the investigation's subjects, or to facilitate oversight of the Bureau's enforcement program.

CLOSING AN INVESTIGATION WITH NO ENFORCEMENT AC TION

Staff should send a Termination Letter[3] as soon as the supervising LD decides that no enforcement action will be recommended against any person or entity who:

- Was identified as a potential violator of consumer financial laws in the Opening Investigation Memorandum and who Staff contacted to make aware of the investigation, including any subject who received a CID;
- Submitted or was solicited to submit a NORA submission;
- Received a third-party CID and subsequently requested written confirmation that Staff would recommend no enforcement action against them; or
- Staff otherwise reasonably believes is aware that Staff considered recommending an enforcement action against the subject.

Staff should send Termination Letters to the above individuals or entities even if an investigation remains open as to other potential defendants or respondents. If Staff decide not to send a Termination Letter to persons or entities that fall into any of the above categories, Staff should get approval for this decision from the supervising LD.

3 (b)(7)(E)

Staff should recommend the closure of an investigation as soon as it becomes apparent that no enforcement action will be recommended, even if every possible investigative action has not been completed.

Closing an investigation without recommending enforcement action may require a difficult judgment call, but failing to do so interferes with your ability to do other more productive work. Avoid the temptation to delay recommending closing an investigation based solely on the possibility that some unforeseen development could make an enforcement action more likely. You should consider the following factors when deciding whether to recommend the closure of an investigation without enforcement action:

- Seriousness of the conduct and potential violations
- Staff resources necessary to pursue available relief
- Sufficiency and strength of the evidence
- Extent of potential consumer harm if an action is not commenced
- Realistic expectation of meaningful victim restitution after successful Bureau action
- Expectation that actions will be commenced by other government agencies
- Expectation that consumers will be compensated through private litigation
- Age of the conduct underlying the potential violations

INVESTIGATIONS RESULTING IN ENFORCEMENT ACTION

Staff should recommend closing an investigation that resulted in the Bureau taking enforcement (legal) action as soon as:

- The legal action (including appeals) has concluded;

- Staff have followed through on every step authorized by the Director;
- Defendants have made all payments they owe pursuant to the action's resolution; and
- There is no ongoing investigation into additional conduct or entities that were not the subject of the legal action.

You should recommend closing any investigation as soon as there is nothing further to investigate and defendants have made all financial payments they owe as a result of the enforcement action. Because investigations may have multiple subjects, and all enforcement actions arising from an investigation may not be commenced simultaneously, investigations may remain open after the conclusion of any particular legal action.

MONETARY COLLECTIONS (BEFORE CLOSING INVESTIGATIONS WITH ENFORCEMENT ACTION)

Staff should not recommend that an investigation be closed until all litigation (including appeals) in the case is complete and all ordered monetary relief is accounted for, meaning:

- All restitution, disgorgement, and civil penalties have been paid in full or a decision has been made to terminate collection of any unpaid amounts;
- All funds collected have been distributed to consumers; and
- All money collections and distributions have been properly recorded.

When the only work that remains to be done on a matter is the collection or disbursement of monetary relief, Staff should change the matter's MMS status accordingly.

An investigation cannot be closed if any debts of a defendant or respondent are the subject of collection activity by the Bureau or on the Bureau's behalf (*e.g.*, by the Department of the Treasury's Financial Management Service or the Department of Justice), or if any funds are being held pending final distribution.

Litigation Policies

Statutes of Limitations and Tolling Agreements

During an investigation and before recommending an enforcement action, Staff should consider whether the alleged violations fall within the applicable statutes of limitations, and whether it would be prudent to seek an agreement tolling the applicable limitation periods.

Determining Applicable Statutes of Limitations

Subtitle E of the Dodd-Frank Act states that "except as permitted by law or equity, no action may be brought under this title more than 3 years after the date of discovery of the violation to which an action relates." 12 U.S.C. § 5564(g)(1). However, for actions arising "solely under" the enumerated consumer laws or the transferred laws, the action may be brought in accordance with the requirements of that provision of law. *See* 12 U.S.C. § 5564(g)(2)(B).

Most of the enumerated consumer laws do not contain an explicit time period for bringing a Bureau enforcement action. Where no statute of limitations is specified in the law, an action seeking a fine, penalty, or forfeiture must be brought within five years from the date the claim first accrued pursuant to 28 U.S.C. § 2462. However, under the enumerated consumer laws, unless specified otherwise, there is no limitations period when bringing an action for other relief, including equitable monetary relief.

You should be familiar with the statute of limitations issues arising under 28 U.S.C. § 2462, such as when limitation periods begin to accrue. You should also be aware of the statutes of limitations for any enumerated consumer laws that may be relevant to your investigations. You should thoroughly research the applicable statutes of limitation and related issues at the early stages of your investigation and prior to recommending an enforcement action.

Tolling Agreements

If at any point during the investigation Staff believes there might be a statute of limitations issue, Staff should consult with their supervising LD about whether to ask the potential defendant or respondent to enter into a tolling agreement.

Notice and Ex Parte Preliminary Ancillary Relief [TRO/PI]

There are situations in which the Bureau will find it necessary to seek preliminary ancillary relief, such as seeking a notice or *ex parte* temporary restraining order (TRO), asset freeze, receivership, and other preliminary ancillary relief.[1] *Ex parte* relief is an extraordinary remedy that is sought without providing notice to adverse parties and should be sought only in certain situations.

Legal Standard for a Notice Temporary Restraining Order

The purpose of a TRO is to maintain the status quo pending a more complete hearing on the matter—such as a preliminary injunction hearing and/or a trial on the merits. Incident to their authority to issue permanent injunctive relief, courts have the inherent equitable power to grant all temporary and preliminary relief necessary to effectuate final relief. To prevail on a motion for a TRO, the Bureau will have to meet the specific evidentiary requirements of the court in which the action is filed. The standard for obtaining a TRO is generally the same as that to obtain a preliminary injunction.

Traditionally, a litigant must satisfy a four-prong test in order to prevail on a motion for a TRO and preliminary injunction by showing:

- Irreparable injury unless the TRO is granted;
- Substantial likelihood that the Bureau will prevail on the merits;
- A balance of the equities in favor of issuing the TRO; and
- The TRO would not be adverse to the public interest.

Legal Standard for an *Ex Parte* Temporary Restraining Order

The purpose of an *ex parte* TRO is to maintain the status quo when notice would make further prosecution fruitless or impossible. Consumer fraud cases often fall into this category. If the Bureau provides notice to individuals and corporations engaged in consumer fraud schemes, it is likely that those involved in the scheme will hide
or dissipate assets and move or destroy business records and other inculpatory

---

1 Section 1054 of the Dodd-Frank Act, 12 U.S.C. § 5564(a) specifically allows the Bureau to seek temporary injunctions as permitted by law.

evidence. Expedited action without notice will allow the Bureau to prevent immediate and irreparable harm and preserve the Bureau's ability to secure effective final relief to consumers through funds and assets frozen by the court's order.

The Federal Rules of Civil Procedure provide that a court can issue an *ex parte* TRO only if the legal standards for a notice TRO and the following requirements are met:

- Specific facts in an affidavit or verified complaint clearly show that immediate and irreparable injury, loss, or damage will result to the movant before the adverse party can be heard in opposition; and
- The movant's attorney certifies in writing any efforts made to give notice and the reasons why it should not be required. Fed. R. Civ. P. 65(b).

Seeking a Notice or *Ex Parte* Temporary Restraining Order

Provided that an investigation has been opened through the Enforcement Action Process, Staff should use their best judgment to determine whether a particular case merits a notice or *ex parte* proceeding based on the factors listed below. If Staff believe that the case merits a notice or *ex parte* TRO, Staff should consult with their supervising ALD as soon as possible to determine the appropriate course of action.

Staff should consider seeking an *ex parte* TRO in the following situations:

- Where the facts of the investigation demonstrate that assets and evidence stemming from the unlawful activity will be dissipated, destroyed, or otherwise made unavailable pending the outcome of litigation; or
- Where ongoing conduct of the defendant(s) threatens or continues to subject consumers to harm; and
- Where the situation meets the legal standard for *ex parte* TRO relief under the Federal Rules of Civil Procedure and relevant case law.

Contemporaneously with the filing of a motion for a notice TRO, Staff should file all other necessary pleadings to effectuate the TRO. These pleadings usually include, but are not limited to the following:

- Motion for a TRO;
- Memorandum of points and authorities in support of the motion;

- Proposed TRO;
- Motion for a preliminary injunction (sometimes referred to as a motion to show cause why a preliminary injunction should not issue);
- Memorandum of support for the preliminary injunction;
- Proposed preliminary injunction; and
- Civil complaint.

If Staff seek an *ex parte* TRO, contemporaneously with the filing of a motion for an *ex parte* TRO, Staff should file all other necessary pleadings to effectuate the TRO. These pleadings usually include, but are not limited to the following:

- Motion for *ex parte* TRO;
- Memorandum of points and authorities in support of the motion;
- Attorney affidavit pursuant to Fed. R. Civ. Pro. 65(b)(1)(B) attesting to efforts made to give notice and reasons why notice should not be required;
- Proposed TRO;
- Motion for a preliminary injunction (sometimes referred to as a motion to show cause why a preliminary injunction should not issue);
- Memorandum of support for the preliminary injunction;
- Proposed preliminary injunction;
- Civil complaint; and
- Motion to seal all documents and memorandum in support.[2]

---

2 Until a policy regarding filing under seal is issued, Staff should consult with their supervising ALD regarding a determination of whether the civil complaint, TRO pleadings, and preliminary injunction pleadings should be filed under seal. To seal information, Staff generally must file a motion to seal with a brief memorandum in support and a proposed order. Any proposed order to seal the civil complaint should provide for the seal to be lifted automatically after notice of service on the defendant(s) (and restraint of assets, if any) has been filed with the court or within 14 days from issuance of the TRO or whichever occurs first.

Additional pleadings and other material may be necessary to support the TRO depending on case-specific facts and the local rules where the motion is filed. Staff should always review local rules and seek out any judge-specific rules when seeking a TRO. The Bureau is not required to provide security, as is normally required of private litigants seeking injunctions and restraining orders, and Staff should note this fact in the memorandum of support for the TRO and the proposed TRO. *See* Fed. R. Civ. Pro. 65(c).

Staff should consider including the following fact-related provisions in a proposed notice and *ex parte* TRO:

- Asset freeze
- Accounting of assets
- Repatriation of foreign assets
- Expedited discovery
- Prohibition on filing for bankruptcy without prior court approval
- Stay of other actions
- Limitations on business activities
- Obtaining defendants' credit reports
- Service upon the Bureau
- Appointment of a court-appointed receiver
- Immediate access to the business premises/Forensic Collection of Evidence

Additional filings and considerations may include, for example, a motion for admission to the court *pro hac vice*, a motion to seal the court filing for a limited time, or having a local attorney on the pleadings—*i.e.*, a Bureau attorney admitted to practice in that district or a Civil Division Assistant United States Attorney for that district. As federal

government attorneys, Staff may appear in any court in the country and motions to be admitted *pro hac vice* should not be necessary. However, some courts require such admission and local electronic case filing (ECF) registration before appearing.

A sample ex parte TRO[3] can be found on SharePoint.

ADDRESSING THE MERITS OF A TRO

Staff should be prepared to address the merits of a TRO on very short notice. Some courts will decide the motion in chambers on the pleadings without a formal hearing in court and some courts will conduct a brief hearing in court. In the latter situation, if Staff seeks an *ex parte* TRO Staff should have the court closed to the public and be prepared to have an investigator testify as to evidence necessary to establish the elements for a TRO. Because hearsay testimony is admissible to establish a TRO, most courts will not require witnesses be present for a TRO determination. Still, it is advisable to have the case investigator present and, if possible, to seek guidance from the court regarding whether it will expect or want other witnesses present. Staff generally will not know which judge has been assigned until after the case has been filed and docketed with the Clerk of the Court. However, once the Clerk's Office assigns the case to a particular judge, Staff should provide a mobile number to the assigned Judge's courtroom deputy clerk so that Staff may be reached easily should the court have questions or want to decide the motion in chambers. Staff should also consider communicating with the local United States Attorney's Office Civil Division to obtain further information relating to local practice and whether there is a district court duty judge to whom TROs are assigned.

SEEKING CONTINUANCE FOR A TRO

TROs are valid only for a limited time and good cause must be shown to extend a TRO. *See* Fed. R. Civ. Pro. 65. Once a TRO is granted, the court will likely set a date for the preliminary injunction hearing. Staff should always ensure that the preliminary injunction hearing is set prior to the expiration of the TRO, which is 14 days from date of issuance. Fed. R. Civ. Pro. 65(b)(2). If the court overlooks this planning, Staff should seek a continuance of the TRO. When seeking any continuance, Staff should lay the foundation that the continuance has been granted for good cause as required in the Federal Rules of Civil Procedure. This additional finding will assist in preventing an appellate issue regarding the timing and/or continuance of the TRO.

3 (b)(7)(E)

SENDING A TRO TO DEFENDANTS

Staff should be prepared immediately to send a copy of the signed TRO via email, facsimile, U.S. mail, FedEx, or personal service to financial institutions where the defendants have accounts or other businesses used by or holding assets of the defendants. Each financial institution will likely have different procedures for receipt of court orders. Generally, financial institutions require that a TRO be served on its legal-process or subpoena department. Many financial institutions require a hardcopy be sent via overnight delivery or FedEx. This may not always be necessary if your TRO specifically provides for service via facsimile and email. This process is particularly important because once the financial institution has received notice of the TRO it may be liable for the release of funds from the frozen accounts.

SEEKING A COURT- APPOINTED RECEIVER

Staff should consider whether it is necessary to seek a court-appointed receiver when seeking either a notice or *ex parte* TRO. A court-appointed receiver acts under the authority granted to it by the court. *See* Fed. R. Civ. Pro. 66. Although the request for a receiver may come from the Bureau, the receiver is independent from the Bureau and accountable to the court. Thus, it is important that any proposed TRO that includes an appointment of a receiver clearly state the receiver's authority and power are granted by the court to the receiver.

When the Bureau seeks to have the court appoint a receiver as part of either a notice or *ex parte* proceeding, to avoid the appearance of an impropriety, *i.e.*, favoritism in using certain receivers, Staff should be prepared to recommend *at least two* potential receivers to the court for consideration. The receivers recommended by Staff must be in good standing with the applicable state bar association or other professional organization(s). In addition, the recommended receiver should have some experience as a receiver or business monitor, including but not limited to, the following: working with federal government agencies (*e.g.*, Federal Trade Commission, Securities and Exchange Commission, Commodities Futures Trading Commission, or the prudential regulators), auditing and managing businesses, financial accounting practices, and/or management and liquidation of assets in bankruptcy.

Staff should maintain close communications with the receiver, assist the receiver when necessary, and monitor the receiver's costs and expenditures. The proposed TRO should state how the receiver will be paid. The court may require the receiver to submit periodic reports and to seek authorization from the court to be paid. Staff

should monitor the receiver's expenses to ensure that there are no miscellaneous or unexplained expenses. Staff should also ensure that the receiver's expenses are justified by the work performed. The amount of funds paid out to the receiver from any business taken over will determine the amount of funds returned to consumers for redress, as most receivers are paid either from the business profits or the liquidation of the business assets. An experienced receiver will minimize expenses or costs and maximize consumer redress.

A court-appointed receiver will also likely need immediate access to the business premises (discussed in the next section). Thus, Staff should include a provision in a proposed TRO allowing the receiver to enter the business premises or anywhere business is conducted and to secure such premises. For more information about such a provision, see the draft provisions template once it is finalized.

IMMEDIATE ACCESS TO BUSINESS PREMISES/ FORENSIC COLLEC TION OF EVIDENCE

If Staff believe that an immediate access to a business premises should be included as part of either a notice or *ex parte* TRO, Staff should obtain approval from Staff's supervisory ALD to include such a request as part of a TRO. Staff should also provide the Director of Professional Support with as much advance notice as possible regarding the seeking of a TRO. The Director of Professional Support will notify the Bureau's Office of Technology and Innovation and coordinate the procurement of any necessary contractor services for forensic collection of evidence (collectively "forensic collection team") from the immediate access and from the forensic collection.

If a TRO provides for the appointment of a receiver, Staff should coordinate with the receiver to ensure that the business premises will be secured by local, state, or federal law enforcement immediately prior to Staff and the receiver's entry into the premises. Staff should not enter the premises until it is secured by law enforcement. If a TRO does not provide for the appointment of a receiver, but does provide for an immediate access to a business premises, Staff should directly coordinate with law enforcement to ensure that the business premises will be secured prior to Staff's entry into the premises. If Staff is present at an immediate access, Staff should maintain a safe distance from the business premises until informed by law enforcement that the premises are secure. Only then may Staff enter the premises.

If Staff seek an immediate access to the business premises through a receiver, Staff should consider having present at least one attorney, investigator, and paralegal or legal assistant, in addition to the forensic collection team. Any investigators or other Staff present at the immediate access should be prepared to potentially testify as a witness as to what occurred at the immediate access.

Staff should ensure that the necessary steps have been taken to coordinate the immediate access with local or other law enforcement and that forensic and other evidence necessary for the successful prosecution of the case will be collected and preserved. Staff should consider asking law enforcement to remain present during forensic collection while employees of the business are present.

Once inside the business premises, Staff should assist, if necessary, in reviewing evidence, including but not limited to records, documents, and electronic information discovered at the immediate access that may be used for the prosecution of the case. Staff may also assist in interviewing employees, but should only do so in the presence of other Bureau Staff, such as the case paralegal, investigator or other third party that can testify about the interview.

Identifying and Procuring an Expert/Consulting Witness
(updated January 2019)

The policies and procedures below help define the process to identify and set up a contract to procure an expert witness. Case teams may request the assistance of expert witnesses at any time during their investigation if the following criteria is met:

1. Funding is available in the fiscal year you wish to bring on an expert (check with the Enforcement Administrative Officer (AO) or Resource Management Officer (RMO));

2. Approval is provided by their ALD or LD and Enforcement Chief of Staff.

Additional cost/benefit analysis may be requested from the Enforcement Chief of Staff for certain investigations or experts or firms that greatly exceed the average contract amount. Case teams cannot bring on expert witnesses without consulting with the AO or RMO. The roles of the AO and RMO are to explain the procurement process, assist teams with forms and procedures, and act as a point of contact with the other offices in the bureau that need to be involved in the procurement process.

Further information on the procedures for procuring an expert witness (consulting and/or litigating) can be found on SharePoint.[1] Rather than the lengthy background security check required of all other types of contractors, the Bureau requires that Staff conduct certain "due diligence" in selecting an expert based on practices at similarly situated agencies, and obtain clearance from an FBI name search. Because an FBI name search is not normally required by other agencies, Staff should advise a prospective expert that this is a condition of the award. If the expert declines to be considered for the job or does not obtain clearance for reasons that appear unwarranted, please advise either the AO or RMO as this procedure could be reconsidered.

Identifying the Appropriate Expert

Prior to reaching out to any expert witnesses, the case team should email the Assistant Director and Deputy Assistant Director in the Office of Research a full list of expert witnesses that they would like to interview. The Office of Research will respond

1 (b)(7)(E)

to the case team if they deem there is a potential conflict of interest and/or if they have any other individuals/experts in mind that they can recommend for this type of work.

As part of their research, case teams should review the CVs of experts that Enforcement has brought on board over the past few years. Information about these experts, including links to their CVs, can be found in the Expert Witnesses List on SharePoint.[2]

Bureau attorneys will identify potential and actual conflicts of interest by combing through each expert's CV. When an expert is not previously known to the Bureau, is not recommended by a trusted source, or if there is a significant time gap since the expert last performed services for the government, the Bureau attorneys will more vigorously research third-party sources. For example, the attorneys will conduct a detailed internet and legal-database search for information about the expert.

Prior to any discussions, the prospective expert will complete, sign, and return the non-disclosure agreement (NDA)[3] that prohibits disclosure of certain information without prior Bureau approval and ENF staff will notify the expert of civil and criminal penalties that may follow wrongful disclosure. Bureau attorneys will then conduct an initial screening interview with each prospective expert to determine the fit between the expert's abilities and the Bureau's need.

Bureau attorneys will interview the prospective expert for the purpose of performing due diligence, including inquiring whether there is anything in the expert's background that could impugn the expert's testimony or work product. Topics for the interview should include at least:

- Prior expert witness engagements;
- Whether a court, arbitrator, hearing officer, or administrative law judge has ever excluded the expert from testifying or reached an adverse conclusion as to the individual's expert status;
- Any civil lawsuits to which the expert has been a party;

---

2 (b)(7)(E)

3

- The amount and percentage of the expert's income that is derived from government contracts;
- Whether the expert has ever been under criminal investigation or indictment for, or been convicted of or pled guilty to, any crime or misdemeanor;
- Whether any civil penalties have been assessed against the expert;
- Whether the expert has any unpaid liabilities to the federal government; and
- Whether the expert has timely filed all required federal tax forms within the past three years.

The expert should be advised that they will have to undergo a limited background FBI name check background. This process is not usually required by other government agencies, so it may be unfamiliar to the expert. The name check will result in a positive or negative result. If the name check produces a negative result (*i.e.*, the FBI discovers red flags in criminal databases), then a trained adjudicator will evaluate the expert's suitability.

Bureau attorneys should keep a record of all expert candidates considered and should submit that list to Procurement with the expert witness procurement package described below.

> **!** Note: The expert cannot receive payment for any work done prior to the award of the contract.

Procuring the Proposed Expert

Please set up an initial expert procurement kickoff meeting with the RMO and AO and they will walk you through the process, which is summarized in a PowerPoint deck.[4]

PROPOSING AND APPROVING COSTS

The legal team needs to obtain written approval from a supervisor (ALD or LD) to obtain an expert at the proposed costs.

---

4 (b)(7)(E)

Costs include labor rates for all personnel, multiplied by the hours anticipated, for the anticipated period up to one year. It is very important to identify and separately itemize *any other costs that are in addition to the labor rates*. This means that any equipment, supplies, travel, or other items or activities not covered by the hourly rate must be itemized separately. If needed items arise later that you have not originally accounted for, a modification to the contract with additional funding will be necessary, which will delay implementing the contract.

Work with the RMO and the AO to submit a buy request for the expert. The buy request directs OCFO to obligate the funding necessary to procure the expert. Instructions for items that should be included on the buy request are below. The buy request will be filled out by the RMO or AO so the details below are largely informational. The requests should include:

- A Project Title and description of goods or services to be provided. While procurement materials can be disclosed for litigating experts, information about consulting experts are generally not publicly disclosed. The description should be specific enough to identify what contract you are funding, but broad enough not to identify the specific case or case strategy, or limit your potential future investigative approaches.
- The AO or RMO who will be listed as the COR and ACOR on the reward.
- The Period of Performance. This is the time range over which you expect to use the expert. The period may cross the fiscal year and it may exceed one year in time; however, be advised that funding is done on an annual basis. This means that for contracts exceeding one year, you will need to submit a new buy request to add funds in increments of one year.

Assuming the request is under $500,000, you only need the Chief of Staff's signature on the completed buy request. If he or she is not available, the Enforcement Director is also able to sign.

The Bureau can only make an award to a person who is registered in the System for Award Management (SAM)[5] and has obtained a DUNS number. If your expert has not previously registered, they should proceed to do so.

SUBMITTING THE APPROPRIATE PROCUREMENT MATERIALS

Procurement recently unveiled a new online system called BEAMS (Bureau Enhanced Acquisition Management System) which consolidates and improves the processing of procurement forms/contracts. The following procurement materials need to be submitted through the BEAMS system (which are forwarded to the assigned Contracting Officer. The heading for each section below contains a link to a template or example. The AO and RMO will be notified as to who the assigned Contracting Officer is once the buy request has been approved by OCFO.

Independent Government Cost Estimate (IGCE)[5]

The link above shows an example from a case of a cost estimate. It breaks down the hours and cost per hour for each consultant, travel, cost per trip, and any other supplies and equipment not covered by the labor hours that you anticipate will be needed. Procurement often asks for proof that the fees/rates are what the expert charges others. If you can provide such proof (i.e. previous contract) along with the other required materials, it can help expedite the procurement process.

All costs should be included on an Independent Government Cost Estimate (IGCE) sheet. You can find an IGCE template on SharePoint.[6] The IGCE will likely need to be split into three phases:

- Phase 1 will be any work related to drafting the expert report.
- Phase 2 will be any pre-trial work, including deposition prep and attendance, investigational hearing prep, etc.
- Phase 3 will include any trial related work.

It is possible that any trial and pre-trial work will be out of scope for the purposes of your expert requirements. If this is the case, you will enter most items into a single phase for the purposes of the IGCE.

Statement of Work[7]

This document describes the work that you are asking the expert to do. The template contains some suggested language that may be useful to you. The SOW should be detailed enough to identify the tasks, scope of work, tests, and work product—what we

---

5 (b)(7)(E)

6

7

expect to obtain for the money the Bureau pays. However, it is recommended that it not be so detailed as to require a modification to the scope of work if there is a shift in focus in the case or to prejudice your case strategy if it is publicly disclosed. It should be more detailed than simply stating, "provide necessary analytical work, tests, and reports as directed," but not contain the specific questions the expert is retained to opine on. One approach is to explain the background of the need for this service and that Enforcement needs this analytical support to report on what is required to address this need, and identify deliverables or outcomes.

Again, include any other expenses or activities, particularly the anticipated number of trips. Travel is not paid by the Concur system for federal employees; rather, the expert pays for their own travel and then charges the Bureau through the contract; thus, they will be limited to the amount that is identified in the contract. If all items are not addressed in the SOW, the award will have to be modified later and funding added, which will delay implementing the award.

Based on the materials listed above, along with the information the RMO/AO submits in BEAMS, Procurement creates a draft award document, which they will provide to the COR. The legal team should carefully review it, provide edits to Procurement, and ultimately approve it. The contract sets the terms and conditions of the expert's employment. Procurement sends the award contract to the contractor and will contact the COR with any issues that may arise.

During the course of the award, if there is a need to modify the contract, extend the contract, add material changes or funds, respond to a failure to perform, or make other changes, please work with Procurement and your COR on those changes.

SECURITY BACKGROUND CHECK

Experts are required to pass a security background check, but it is much more streamlined than the standard process for other contractors. There are three forms, listed below, to obtain from the consultant and submit to Personnel Security at BureauPersonnelSecurity@cfpb.gov. The security review consists of an FBI name check, which you should inform your expert of early in your discussions. Once these forms are submitted, the COR will be contacted by Security with a start date. The contractor is not allowed to start work until they receive this start date. Security advises that you can generally expect a response in five days. You may be asked to get additional information from the expert in order to expedite the security screening process.

Expert FBI Release Form[8]

Expert Name Check[9]

Contractor Non-Disclosure Form[10]

Providing Information to the Expert

In general, the Bureau should provide data to experts in a way that does not contain direct personal identifiers, unless Bureau Staff conclude that the expert has a demonstrated business need for such identifiers. Experts will be granted access only to data and information that is necessary to the deployment of their expertise in the matter for which they were contracted. Experts cannot have access to Bureau systems or facilities. Rather, the data should be produced out to them and retained in a separate folder per the outgoing production policy.[11]

8 (b)(7)(E)

9

10

11

Remedies Policies

Civil Money Penalties

Section 1055(c)(1) of the Dodd-Frank Act states that "[a]ny person that violates, through any act or omission, any provision of Federal consumer financial law shall forfeit and pay a civil penalty pursuant to this subsection."[1] However, the Bureau may not assess a civil money penalty (CMP) for a violation of any federal consumer financial law unless it first provides the person accused with a notice and an opportunity
for a hearing, or the appropriate court has ordered such assessment and entered judgment in favor of the Bureau.[2] Section 1055(c)(2) of the Dodd-Frank Act sets forth a three-tiered framework for the maximum CMP the Bureau may assess based on whether the person who committed the violation knowingly or recklessly violated the law.

Three-Tiered Framework

FIRST TIER: PENALTY FOR ANY VIOLATION

The Bureau may assess first tier CMPs for the "violation of a law, rule, or final order or condition imposed in writing by the Bureau," but such penalty "may not exceed $5,000 for each day during which such violation...continues."[3]

SECOND TIER: PENALTY FOR ANY RECKLESS VIOLATION

Section 1055(c)(2)(B) of the Dodd-Frank Act raises the maximum daily CMP to $25,000 where a person recklessly engages in a violation of a federal consumer financial law.[4]

THIRD TIER: PENALTY FOR ANY KNOWING VIOLATION

For any person that knowingly violates a federal consumer financial law, the Bureau may assess a CMP of up to $1,000,000 for each day the violation of law continues.[5]

---

1 12 U.S.C. § 5565(c)(1). "Federal consumer financial law" includes "the provisions of [the CFP Act], the enumerated consumer laws, the laws for which authorities are transferred under subtitles F and H of [the CFP Act], and any rule or order prescribed by the Bureau under [the CFP Act], an enumerated consumer law, or pursuant to the authorities transferred under subtitles F and H. The term does not include the Federal Trade Commission Act." 12 U.S.C. § 5481(14).

2 12 U.S.C. § 5565(c)(5).

3 12 U.S.C. § 5565(c)(2)(A).

4 12 U.S.C. § 5565(c)(2)(B).

5 12 U.S.C. § 5565(c)(2)(C).

Consideration of Statutory Mitigating Factors

Section 1055(c)(3) of the Dodd-Frank Act, 12 U.S.C. § 5565(c)(3), also requires the Bureau or a court to take into account the appropriateness of the CMP amount with respect to the following factors, which are discussed in detail below:

- Size of financial resources
- Good faith
- Gravity of the violation or failure to pay
- Severity of the risks to or losses of the consumer
- History of previous violations
- Such other matters as justice may require

Staff should always consider whether to seek a CMP where there is a violation of a federal consumer financial law. If they believe a CMP may be appropriate in the matter, they should calculate the CMP within the parameters of the three-tiered framework. Staff should always consider all of the mitigating factors as required by the statute. In cases where the violations of law occurred prior to the transfer date, however, Staff should calculate the CMP amount in accordance with the appropriate provision of law in effect at the time of the violation.

In circumstances where the same conduct by a person violates multiple laws (*e.g.*, the person failed to disclose a fee, which both violated the Truth in Lending Act and was deceptive under Section 1036 of the Dodd-Frank Act), imposing only one CMP is appropriate. However, in cases where a person's practice or conduct leads to multiple, separate violations (*e.g.*, the person's initial marketing was deceptive and the person also engaged in separate credit reporting violations), Staff should consult with the supervising ALD to determine whether multiple CMPs are appropriate.

When submitting a recommendation memorandum for authority to sue or to enter into settlement negotiations, Staff should include a recommendation for a CMP amount or range or explain why Staff recommends not pursuing a CMP.

Staff should consider seeking the statutory daily maximum based on the three-tiered framework. Staff should not specify the tier level of the CMP in public documents, including Consent Orders and Complaints. However, Staff should plead each of the

elements of the underlying violations that justify the penalty sought or imposed in the statement of facts, including the level of *scienter* where necessary (*e.g.*, reckless or knowing).

If Staff have questions regarding whether a person's conduct may be characterized as "reckless" or "knowing" for purposes of Second and Third Tier penalties, Staff should consult the supervising ALD for guidance.

For purposes of calculating the appropriate CMP amount, Staff should consider each violation of law affecting an individual consumer as a separate violation. For example, if a company engaged in a deceptive telemarketing scheme for three months and deceptively induced 3,000 consumers to purchase a product, the number of violations would equal 3,000 rather than 90 (the number of days the deceptive telemarketing scheme was in place). If Staff believes that the circumstances of a case warrant a different calculation (*e.g.*, a calculation based on the number of days the violation lasted or the number of days the violative conduct lasted), Staff should consult the supervising ALD for guidance.

Certain statutes provide specific CMP amounts for violations of law that are different from the amounts set forth in Section 1055 of the Dodd-Frank Act.[6] If a particular statute provides a different maximum CMP amount or framework for calculating CMPs, Staff may choose to rely on the framework set forth in that particular statute or may rely on Section 1055 of the Dodd-Frank Act for violations of that statute that occurred after the transfer date. Before relying on the penalty framework set forth in such statutes, Staff should carefully review the applicable penalty procedures to ensure compliance with any technical requirements.

Staff should generally require that a CMP be paid in full at the time an Order to pay a CMP is issued. In cases where Staff determines that a suspension of a CMP or a payment plan for a CMP is appropriate, Staff should consult with the supervising ALD to determine whether one of these options is appropriate.

---

6. For example, the Real Estate Settlement Procedures Act, 12 U.S.C. § 2609(d), the Interstate Land Sales Full Disclosure Act, 15 U.S.C. § 1717a, and the Secure and Fair Enforcement for Mortgage Licensing Act, 12 U.S.C. § 5113(d).

In cases involving CMPs against individuals, Staff should generally require that individuals pay CMPs with their own resources and not be indemnified by another entity. In cases where Staff determines that allowing an individual to be indemnified by another entity would be appropriate, Staff should consult with the supervising ALD.

When considering the statutory factors, Staff should take into account the following:

- **Size of Financial Resources.** In considering the size of a person's financial resources, you should determine whether a person has the ability to pay a potential CMP by requesting and examining financial statements or other financial records during your examination or investigation into the person's misconduct. The individual and corporate financial disclosure forms and the List for Ability to Pay Reviews are in the Templates and Forms folder on SharePoint.[7] If the respondent claims an inability to pay, the respondent should also complete the Waiver Request Claiming Inability to Pay[8] (individual and corporate). Note that obtaining information from the subject regarding their financial resources may be necessary to determine an appropriate penalty amount. You may also want to consider the amount of the CMP and its potential deterrent effect. For example, a smaller CMP may have a large impact on a small non-banking institution while a smaller CMP may be considered the cost of doing business for a multi-billion dollar institution. In cases where the defendant raises a valid claim of financial hardship and redress may not be possible, you should consider imposing at least a nominal CMP so that victims may be eligible to receive future payments from the Bureau's Consumer Financial Civil Penalty Fund. You may also want to consider a person's bankruptcy when evaluating financial resources; however, whether a CMP would be dischargeable in bankruptcy may depend on the facts and circumstances of the case.
- **Good Faith.** When considering a person's good faith, it may be appropriate to lower the maximum penalty amount when a subject cooperates throughout an investigation, has established a strong compliance management system, provides evidence or other information that indicates the subject did not intend to violate the law, or voluntarily reimburses customers or engages in other corrective action.

7 (b)(7)(E)

8

- **Gravity of the Violation or Failure to Pay.** When you are considering the gravity of a particular violation, you may want to consider the maximum statutory penalty for violations that are particularly egregious, whereas technical violations may warrant lower penalties.
- **Severity of the Risks to or Losses of the Consumer.** In examining the severity of the risk to or losses of consumers as a result of a violation of consumer financial law, you should take into account the number of products or services sold or provided and the magnitude of each consumer's loss.[9] For example, you should consider whether the product was sold nationwide or to a narrow group of consumers; whether the violation involved a minor fee or caused consumers great financial distress; and whether the product was marketed for years or for a matter of months.
- **History of Previous Violations.** As you examine the person's history of previous violations, a larger CMP may be appropriate where the person has a history of engaging in the same types of violations for the same or similar products or the person has previously been the subject of enforcement actions for violations of consumer financial laws. In a case where the person has a strong history of compliance with consumer financial laws, a lower CMP may be warranted.
- **Such Other Matters as Justice May Require.** Factors to consider include: whether the person received material or substantial benefit from its practices or violations of law; whether the amount of the penalty would have a sufficiently deterrent effect; and whether previous supervisory or enforcement actions (*e.g.*, Memoranda of Understanding or cease-and-desist orders) have been ineffective in eliminating or deterring a violation or practice. You may also want to consider whether the subject should have known that their acts or practices violated the law or whether the Bureau's enforcement action involved novel interpretations of a particular statute or regulation.

---

9 12 U.S.C. § 5565(c)(3)(C).

Consideration of Precedent

Consider the past precedent of the Bureau by consulting the Bureau's Public Enforcement Actions Chart,[10] and to a lesser extent, the past precedent of the Federal Trade Commission and the prudential regulators by using their CMP guidance and previous CMP assessments as a tool to determine whether your proposed penalty is appropriate under the circumstances.

For example, see the Interagency Policy Regarding the Assessment of Civil Money Penalties by the Federal Financial Institutions Regulatory Agencies, which outlines 13 factors that the Federal Financial Institutions Examination Council (FFIEC) agencies[11] should consider in addition to the statutory factors found in each agency's enabling statute.[12] These factors, which you may wish to consider, include:

1. Evidence that the violation or practice was intentional or was committed with a disregard of the law;
2. The duration and frequency of the violations or practices;
3. The continuation of the violations or practices after the respondent was notified or, alternatively, its immediate cessation and correction;
4. The failure to cooperate with the agency in effecting early resolution of the problem;
5. Evidence of concealment of the violation or practice, or alternatively, voluntary disclosure of the violation or practice;
6. Any threat of loss, actual loss, or other harm to the institution, and the degree of such harm;

---

10 (b)(7)(E)

11 At the time the policy was published, the Federal Financial Institutions Examination Council agencies included the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, and the National Credit Union Administration.

12 See Federal Financial Institutions Examination Council: Assessment of Civil Money Penalties, Notice of Revised Policy Statement, 63 Fed. Reg. 30226-02 (1998). The statutory factors cited in each agency's enabling statute are nearly identical to the list of mitigating factors found in Section 1055(c)(3) of the CFP Act. However, Section 1055(c)(3)(C) of the CFP Act contains an additional factor, namely "the severity of the risks to or losses of the consumer, which may take into account to number of products or services sold or provided." 12 U.S.C. § 5565(c)(3)(C).

7. Evidence that a participant or his or her associates received financial gain or other benefit as a result of the violation or practice;

8. Evidence of any restitution paid by a participant of losses resulting from the violation or practice;

9. History of prior violations or practices, particularly where they are similar to the actions under consideration;

10. Previous criticism of the institution or individual for similar actions;

11. Presence or absence of a compliance program and its effectiveness;

12. Tendency to engage in violations of law; and

13. The existence of agreements, commitments, orders, or conditions imposed in writing intended to prevent the violation or practice.[13]

In order to implement the policy, each of the agencies adopted a "CMP Matrix" that serves as a formula for calculating CMPs. Each of the thirteen FFIEC factors is assigned a numerical value as well as a multiplier, which is based on how the individual agency weighs the relative significance of each of the factors. Once the appropriate penalty tier is established, a value is assigned for each factor and is plugged into a mathematical formula that yields a point total that correlates to a range of possible CMPs for the offense.

---

13 Although the 13 factors also reference specific safety and soundness concerns, such as breaches of fiduciary duty and losses to the institution, those references are omitted here because they are not applicable to violations of federal consumer financial laws. Guidance from other agencies, including matrices published by the prudential regulators, are also included in the CMP Guidance folder for your reference. Although you may want to use these tools as a way to gauge whether your potential CMP would be comparable to a CMP assessed by other regulators, you should rely primarily on your calculation of the statutory daily maximum, Bureau precedent, and other statutory factors in determining the appropriate CMP in your case.

Adjudicative Proceedings Policies

Affirmative Disclosure and Other Disclosure Obligations for Adjudication Proceedings [Rule206 and 207 Bureau Rules of Adjudication]

Rules 206 and 207 of the Bureau's Rules of Practice for Adjudication Proceedings (page 10-15), 12 C.F.R. §§ 1081.206, 1081.207, impose on the Office of Enforcement certain obligations to produce material without request and shortly after the commencement of adjudication proceedings (Rule 206) or upon request of the respondent (Rule 207). It is the Office of Enforcement's policy to interpret its disclosure obligations under these Rules broadly and to err on the side of disclosure. This policy should be read in conjunction with

1. The Office of Enforcement's Maintaining Matter Folders policy, which is designed, in part, to ensure that documents and information will be maintained in a way that enables Staff to comply efficiently and timely with Rules 206 and 207;

2. The Bureau's eDiscovery Framework,[1] which guides the review of material for privilege as well as the production of electronically stored information (ESI); and

3. The Bureau's Rules of Practice for Adjudication Proceedings and the section-by-section analysis.

Compliance with Rule 206

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should take steps to ensure that the materials required to be disclosed under Rule 206 are gathered to ensure that Staff timely comply with this Rule.

Staff should review the following folders in the matter folder to ensure that each folder contains all required documents:

- Agreements Folder;
- CIDs and Voluntary Requests for Information Folder;

1 (b)(7)(E)

- Information Informally Obtained from Outside the Bureau Folder; and
- Witness Statements and Testimony Folder.

If these folders do not contain a complete record of all required documents, Staff should gather any missing documents and save them to the appropriate folders as required by the Maintaining Matter Folders policy.

Rule 206 describes the documents the Office of Enforcement must make available for inspection and copying by any respondent. When reviewing the folders described above, Staff should refer to Rule 206 as well as the commentary on Rule 206 contained in the section-by-section analysis published in the Federal Register.[2] Generally, the Rule requires Enforcement to make certain documents available for inspection and copying. This applies to documents in connection with the investigation, leading to the institution of proceedings, that were obtained by the Office of Enforcement prior to the institution of proceedings from persons not employed by the Bureau, including:

- Any documents turned over in response to CIDs or other written requests to provide documents or to be interviewed issued by Enforcement;
- All transcripts and transcript exhibits; and
- Any other documents obtained from persons not employed by the Bureau.

Rule 206 also requires Staff to make available for inspection and copying by any respondent:

- Each CID or other written request to provide documents or to be interviewed issued by Enforcement in connection with the investigation leading to the institution of proceedings; and
- Any final examination or inspection reports prepared by any other Office of the Bureau if Enforcement either intends to introduce any such report into evidence or to use any such report to refresh the recollection of, or impeach, any witness.

---

2 https://www.gpo.gov/fdsys/pkg/FR-2012-06-29/pdf/2012-14061.pdf

TIMING AND FORM OF PRODUCTION

The Office of Enforcement must commence making documents available to the respondent for inspection and copying no later than seven days after service of the notice of charges. 12 C.F.R. § 1081.206(d). Note: Staff may need to provide notice to third parties that provided information during an investigation prior to disclosure, as detailed below. *See infra* 12 C.F.R. § 1081.119(a). Rule 206 provides the Office of Enforcement with discretion regarding the timing and format of production (*e.g.*,
paper, electronic copies, or making documents available for inspection and copying). However, the Office of Enforcement has committed to making documents available to the respondent as soon as possible (but in any event commencing no later than seven days after service of the notice of charges) and to producing the information in electronic format, unless electronic production is not feasible.

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should contact the Technology and Innovation Department (T&I Team) to discuss producing documents and the format of production by sending an email to the DL_CFPB_eDiscoveryIT listserv. Topics to address with the T&I Team include:

- Determining the timing of production;
- Identifying data sources and data for inclusion in the production set;
- Assisting the T&I team in determining appropriate production format; and
- Performing quality check of production data to prevent inadvertent disclosure of privileged information.

Situations in which Staff should consider providing hard copies or delaying production of materials include when the information to be produced includes:

- Physical evidence not susceptible to reproduction in electronic format (*e.g.*, oversized documents, such as advertising posters or banners, or physical objects);
- Documents subject to a non-disclosure agreement (*e.g.*, documents obtained from a state pursuant to a confidentiality agreement) that are the subject of a pending motion for a protective order; and

- Confidential documents or documents prohibited from disclosure under law that are the subject of a pending motion for a protective order.

Staff should consult with the supervising ALD or supervising LD assigned to the matter to determine whether other situations warrant providing hard copies or delaying production in particular cases.

MATERIAL EXCULPATORY EVIDENCE

The Office of Enforcement cannot withhold material exculpatory evidence that would otherwise be required to be produced under Rule 206(a). If the Office of Enforcement is prohibited from disclosing a document that contains material exculpatory evidence, either because applicable law prohibits the disclosure or because the governmental entity from which the document was obtained insists on maintaining the confidentiality of that document, the Office of Enforcement should move the hearing officer for an order permitting the Office of Enforcement to withhold those documents.

"Material exculpatory evidence" under Rule 206(b)(2) means all information material and favorable to the respondent and should be interpreted broadly to include, among other things, information that tends to:

- Cast doubt on respondent's liability as to any essential element in any claim in the notice of charges;
- Cast doubt on the admissibility of evidence that the Office of Enforcement anticipates using in its case-in-chief;
- Cast doubt on the credibility or accuracy of any evidence that the Office of Enforcement anticipates using in its case-in-chief; or
- Diminish the degree of the respondent's culpability or the respondent's liability for civil money penalties under 12 U.S.C. § 5565(c).

Staff should err on the side of disclosure and should consult with the supervising ALD or supervising LD if there is any doubt as to whether the documents contain material exculpatory evidence. Note that Rule 206(b)(2) only applies to evidence that would be required to be produced pursuant to Rule 206(a); it thus does *not* apply to internal memoranda, notes, etc., as such documents are not within the scope of Rule 206(a)'s affirmative disclosure obligation.

MATERIAL OBTAINED FROM THIRD PARTIES SUBJECT TO A CLAIM OF CONFIDENTIALITY (OTHER THAN DOCUMENTS OBTAINED FROM STATE OR FEDERAL PARTNERS)

If any party to an adjudication proceeding (including the Office of Enforcement) intends to disclose information obtained from a third party that is subject to a claim of confidentiality, Rule 119 requires the producing party to give the third party at least 10 days' notice prior to the proposed disclosure of the information. 12C.F.R. § 1081.119(a). The third party claiming confidential status may consent to the disclosure of the material, which may be conditioned on the entry of an appropriate protective order, or may intervene in the proceeding for the limited purpose of seeking a protective order. *Id.*

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should review the Agreements Folder within the matter folder to identify any agreements governing the disclosure of materials the Office of Enforcement obtained from third parties; for example, confidentiality or non-disclosure agreements. Staff should also identify:

- Any documents or information the producing party marked "confidential," "exempt from disclosure," or some similar stamp indicating that the producing party intended to protect the confidentiality of the document;
- Any cover letters or emails the producing party included with document productions to determine whether the producing party indicated that it was seeking confidential treatment of the material; and
- Any documents Staff are otherwise aware of that are subject to a claim of confidentiality or that constitute trade secret materials.

If Staff locate documents subject to a claim of confidentiality, Staff should ascertain whether the documents are subject to one of the exemptions from mandatory disclosure set forth in Rule 206(b)(1). If any such documents are not exempt from disclosure, Staff should, as soon as practicable but in any event no later than ten days prior to producing the documents, notify the third party claiming the documents are confidential to inform them that the Office of Enforcement intends to disclose the documents.

Rule 119(a) does not provide the procedure for handling documents obtained from federal or state partners pursuant to a non-disclosure agreement. Rule 206(b)(1)(iii), addressed below, governs those documents.

MATERIAL OBTAINED FROM SUPERVISION OR OTHER OFFICES WITHIN THE BUREAU IN CONNECTION WITH THE INVESTIGATION

The affirmative disclosure obligation under Rule 206 extends to documents obtained by the Office of Enforcement prior to the institution of proceedings, from persons not employed by the Bureau, in connection with the investigation leading to the institution of proceedings. 12 C.F.R. § 1081.206(a)(1). Staff should review the section-by-section analysis of Rule 206 contained in the Federal Register for further information regarding the scope of this obligation.

The Bureau interprets its obligation to affirmatively disclose material under Rule 206 as including both records obtained by the Office of Enforcement directly from persons not employed by the Bureau, as well as documents obtained by the Office of Enforcement indirectly from persons not employed by the Bureau. For example, if the Office of Enforcement obtained information from Supervision in connection with an investigation that Supervision obtained from a person not employed by the Bureau, then the Office of Enforcement will disclose that information, subject to 12 C.F.R. § 1081.206(b). 77 FR 39070-71, 39073.

Material Obtained from Supervision

When Staff obtain documents from Supervision in the course of an investigation or when an exam-related matter is identified for possible public enforcement action, Staff should maintain those documents.

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should review any documents or information obtained from Supervision in connection with the underlying investigation to determine whether there are any documents Supervision obtained from persons not employed by the Bureau. If Staff locate such documents, Staff should include those documents in the pre-production review described in the

Bureau's eDiscovery Framework[3] and must ultimately produce those documents unless they are privileged or otherwise protected from affirmative disclosure by Rule 206(b).

Material Obtained from Other Offices Within the Bureau

When the Office of Enforcement receives documents from other offices in the course of an investigation, Staff should maintain those documents.

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should review any documents or information obtained from other offices within the Bureau in connection with the underlying investigation to determine whether there are any documents those offices obtained from persons not employed by the Bureau. If Staff locate such documents, Staff should include those documents in the pre-production review described in the Bureau's eDiscovery Framework and must ultimately produce those documents unless they are privileged or otherwise protected from affirmative disclosure by Rule 206(b).

DOCUMENTS THAT MAY BE WITHHELD UNDER RULE 206

Rule 206(b) lists several categories of documents that the Office of Enforcement may withhold notwithstanding the affirmative disclosure obligation under Rule 206(a):

- Privileged documents (12 C.F.R. § 1081.206(b)(1)(i));
- Internal memoranda, notes, or other writings prepared by a person employed by the Bureau or another governmental agency, other than examination or supervision reports, or documents subject to the work product doctrine that will not be offered into evidence (12 C.F.R. § 1081.206(b)(1)(ii));
- Documents obtained from a domestic or foreign governmental entity that is either not relevant to the proceeding or was provided on condition that the information not be disclosed (12 C.F.R. § 1081.206(b)(1)(iii));
- Documents that would disclose the identity of a confidential source (12 C.F.R. § 1081.206(b)(1)(iv));
- Documents prohibited from disclosure under applicable law (12 C.F.R. § 1081.206(b)(1)(v)); or

---

3 (b)(7)(E)

- Documents that the hearing officer has granted leave to withhold as not relevant to the subject matter of the proceeding or for good cause shown (12 C.F.R. § 1081.206(b)(1)(vi)).

Documents Obtained from State or Federal Partners Subject to Non-Disclosure Agreements or Statutes or Rules Restricting Further Disclosure (Rule 206(b)(1)(iii))

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should review the Agreements Folder within the matter folder to identify any agreements governing the disclosure of materials the Office of Enforcement obtained from state or federal law enforcement partners; for example, confidentiality or non-disclosure agreements. Staff should identify any relevant agreements and determine their applicability to documents that may be subject to Rule 206.

Rule 206(b)(1)(iii) permits the Office of Enforcement to withhold a document if it was obtained from a governmental entity on condition that the information not be disclosed. The Rule does not permit the Office of Enforcement to withhold such documents if they contain material exculpatory evidence. 12 C.F.R. § 1081.206(b)(2).

If the Office of Enforcement obtained documents from a governmental entity on condition that the documents not be disclosed, Staff should take the following steps:

1. Review the documents and, in consultation with the ALD or LD assigned to the matter, determine:

   a. Whether the documents contain material exculpatory evidence that must be produced under 12 C.F.R. § 1081.206(b)(2) and 12 C.F.R. § 1081.206(a)(1); and

   b. Whether the Office of Enforcement wishes to introduce the documents in the proceeding despite the non-disclosure or confidentiality agreement.

2. If Staff determine that the documents contain material exculpatory evidence, Staff should contact the governmental entity from which the documents were obtained to inform the entity that the Bureau's Rules do not permit the Office of Enforcement to withhold those documents and to determine whether the entity will consent to the disclosure of the documents in the proceeding.

3. If Staff determine they wish to use the documents in the proceeding (but the documents do not contain material exculpatory information), Staff should contact the entity from which the documents were obtained to determine whether the entity will consent to the disclosure of the documents, unless Staff determine, in consultation with the ALD or LD assigned to the matter, that the benefit of using the documents is outweighed by the risk that contacting the entity to make this request will be detrimental to the Bureau's relationship with the governmental entity.

4. If the entity does not consent in either of the above-referenced circumstances, or conditions its consent upon the entry of an appropriate protective order, Staff may either move for a protective order pursuant to Rule 119 and 206(a), or advise the governmental entity of its right to intervene for the limited purpose of seeking a protective order pursuant to Rule 119.

5. If the documents do not contain material exculpatory evidence and the Office of Enforcement determines that it does not wish to use the documents, or if the entity from which the documents were obtained does not consent to the disclosure, Staff should:

   a. Inform the respondent of the fact that the documents are being withheld and identify the governmental agency from whom the documents were obtained; and

   b. Inform the governmental agency that the documents will be identified as being withheld in the adjudication proceeding pursuant to Rule 206(c).

Material Disclosing the Identity of a Confidential Source (Rule 206(b)(1)(iv))

Rule 206(b)(1)(iv) permits the Office of Enforcement to withhold a document if it would disclose the identity of a confidential source. A confidential source is someone who requested that his or her identity not be disclosed, and may include whistleblowers and former employees.

When the Office of Enforcement determines that it will seek approval to bring an adjudication proceeding pursuant to the EAP, Staff should, consistent with the Bureau's eDiscovery Framework,[4] review the documents likely to be produced under

4 (b)(7)(E)

Rule 206 to determine whether any documents would disclose the identity of a confidential source. If a document would disclose the identity of a confidential source, Staff should:

1. Contact the source to determine whether the source will consent to the disclosure of the documents despite the fact that disclosure would reveal his or her identity, unless Staff determine, in consultation with the ALD or LD assigned to the matter, that contacting the source to make this request will be detrimental to the Bureau's relationship with the source.

2. If the source does not consent to the disclosure of the document, Staff should determine whether the document can be redacted in such a way that it would not disclose the identity of the confidential source.

3. If Staff determine that the document cannot be redacted, Staff should, in consultation with the ALD or LD assigned to the matter, determine whether the document contains material exculpatory evidence.

4. If Staff determine that the document contains material exculpatory evidence, Staff should:

    a. Inform the source whose identity would be revealed that the Bureau's Rules do not permit the Office of Enforcement to withhold those documents;

    b. Inform the source that the Bureau's Rules permit him or her to seek a protective order; and

    c. Move the hearing officer for an order pursuant to Rule 206(a) seeking to withhold the documents.

5. If the source does not consent, the document cannot be redacted in such a way that it would not disclose the identity of the confidential source, and the document does not contain material exculpatory evidence, the document should be withheld.

Material Prohibited from Disclosure Under Law (Rule 206(b)(1)(v))

Rule 206(b)(1)(v) permits the Office of Enforcement to withhold documents when applicable law prohibits the disclosure of the document. Though there are other sources of law that may prohibit the production of documents, the Trade Secrets Act, 18 U.S.C. § 1905, and the Bank Secrecy Act are two statutes Staff should consider when determining what documents to produce under Rule 206.

Before producing documents under Rules 206 or 207, Staff should, consistent with the Bureau's eDiscovery Framework:[5]

- Review the documents and, in consultation with the ALD or LD assigned to the matter, determine whether the Bureau is prohibited from disclosing the document under any law, including the Trade Secrets Act.
- Review the documents and, in consultation with the ALD or LD assigned to the matter, determine whether any documents prohibited from being disclosed are material exculpatory evidence that must be disclosed under Rule 206(b)(2).
- If there are documents that are prohibited from being disclosed and that also contain material exculpatory evidence, Staff should move the hearing officer for an order exempting the documents from disclosure.

Privileged Documents or Other Internal Documents Prepared by a Person Employed by the Bureau (Rule 206(b)(1)(i))

When Staff gather the documents that may be produced pursuant to Rule 206, Staff should review those documents and take reasonable steps to protect privileged documents from disclosure and production consistent with the Bureau's eDiscovery Framework. Staff should identify and protect from disclosure privileged documents and internal documents prepared by a person employed by the Bureau or another government agency (other than examination or supervision reports identified in Rule 206(a)(2)(ii)).

Rule 206(i) contains a "clawback" provision under which the disclosure of privileged information does not operate as a waiver if:

- The disclosure was inadvertent;
- The holder of the privilege took reasonable steps to prevent disclosure; and

5 (b)(7)(E)

- The holder promptly took reasonable steps to rectify the error, including notifying the other party of the claim of privilege and the basis for the claim.

See 12 C.F.R. § 1081.206(i).

Withheld Document List

Under the Rules, the Office of Enforcement is not automatically required to produce a privilege log identifying withheld documents. 12 C.F.R. § 1081.206(c). With some exceptions, however, the hearing officer can order the Office of Enforcement to produce a list of documents or categories of documents that are being withheld pursuant to paragraphs (b)(1)(i) through (v) of Rule 206, or to submit to the hearing officer any document withheld.

Though the Office of Enforcement is not automatically required to prepare and produce a privilege log, Staff should consider whether to prepare a list of withheld documents that would comply with Rule 206(c) while they are reviewing the documents before production.

Production of Witness Statements under Rule 207

As set forth in the Maintaining Matter Folders policy, for every matter folder, Staff should create a folder titled "Witness Statements and Testimony" to preserve all witness statements obtained during the course of an investigation. Before commencing an adjudication proceeding, Staff should ensure that all witness statements have been saved within this folder. If there are any documents missing, Staff should gather those missing documents and save them in the correct folder.

Rule 207 permits a respondent to move that the Office of Enforcement produce for inspection and copying any statement of any person called or to be called as a witness by the Office of Enforcement that pertains, or is expected to pertain, to his or her direct testimony and that would be required to be produced pursuant to the Jencks Act, 18 U.S.C. § 3500, if the adjudication proceeding were a criminal proceeding. 12 C.F.R. § 1081.207(a). The production shall be made at a time and place fixed by the hearing officer. *Id.* Unlike Rule 206, the production of witness statements is not automatic and, instead, the respondent is required to move for the production of these statements.

The Jencks Act does not require production of a witness's prior statement until the witness takes the stand. In ordinary cases, the Office of Enforcement should not object to voluntarily providing prehearing production of witness statements covered under Rule 207 upon motion. Submission of a witness's prior statement, however, may provide a motive for intimidation of that witness or improper contact by a respondent with the witness. Where Staff believe there is risk of improper use of a witness's prior statement, Staff should move the hearing officer to take appropriate steps to mitigate that risk. For example, Staff may move for an order delaying production of a prior statement, or prohibiting parties from communicating with particular witnesses.

Staff should consult the definition of "statement under the Jencks Act," 18 U.S.C. § 3500(e), as well case as law interpreting that definition. Generally speaking, non-verbatim notes written by an interviewing attorney or investigator that are not adopted by a witness are not "statements" under the Jencks Act and the Office of Enforcement would not have to produce those notes under Rule 207. *E.g.*, *Palermo v. United States*, 360 U.S. 343, 352 (1959) ("only those statements which could properly be called the witness' own words should be made available to the defense for purposes of impeachment"); *United States v. Valera*, 845 F.2d 923, 926 (11th Cir. 1988) (a report written by U.S. Attorney and never adopted by witness and summaries written by agent of what witness had told him "did not fall within the Jencks definition of 'statement' because neither of them was a verbatim transcription of what [the witness] had stated ... and [the witness] had adopted neither of the statements"); *United States v. Ricks*, 817 F.2d 692, 698 (11th Cir. 1987) ("FBI memoranda of witness interviews" did not fall within the Jencks Act because "the witnesses never adopted the memoranda as their own statements.").

STATEMENTS OF BUREAU PERSONNEL, INCLUDING EXAM TEAM MEMBERS AND INVESTIGATORS

Under Rule 206, reports prepared by exam team members or investigators would generally not be required to be produced because those reports would not be "documents obtained by the Office of Enforcement prior to the institution of proceeding, from persons not employed by the Bureau." 12 C.F.R. § 1081.206(a). Such reports may, however, be required to be produced under Rule 207.

In proceedings in which Bureau personnel—particularly exam team members or Enforcement investigators—may be called as witnesses, Staff should take the following steps to ensure that witness's statements have been gathered and can be produced in the event that the respondent moves for production under Rule 207(a):

1. Review the matter folder, particularly the Witness Statements and Testimony Folder, to locate any documents that may constitute statements under Rule 207 and 18 U.S.C. § 3500(e).

2. Contact the Bureau personnel to be called as a witness to determine whether he or she created other documents that may qualify as "statements" under the Jencks Act and, if so, obtain copies of those statements and save those documents in the appropriate file pursuant to the Maintaining Matter Folders policy.

3. Consult with the ALD or LD assigned to the matter to determine whether any documents are "statements" under Rule 207 and 18 U.S.C. § 3500(e).

Adjudication Process Questionnaire

This is a tool to help you plan for your administrative matter. This document should be prepared as soon as a decision is made to proceed to an adjudication proceeding. A copy should be maintained in the matter folder on SharePoint and continuously updated whenever deadlines change. The template[6] for this Excel file can be found in the Templates and Forms folder on Share.

6 (b)(7)(E)

Order Compliance Monitoring Policies

(added January 2021)

Enforcement Compliance Team Processes and Procedures

Enforcement created the Compliance Team ("CT") to centralize most of Enforcement's compliance-related work. The CT's core function is to monitor defendants'/respondents' ("defendants" for the duration of this guidance) compliance with all Enforcement-monitored orders, including by capturing, maintaining, and synthesizing information about compliance; verifying compliance representations provided by defendants; and, if likely order violations are identified, recommending and/or executing action(s) to address the violations.

Pre-Judgment Review of Draft Final Orders

The CT is responsible for reviewing all draft administrative consent orders and federal court stipulated final judgments (collectively, "Final Orders"), which are written by case teams.[1] When drafting a Final Order, the case team must use the appropriate template. Case teams should endeavor not to deviate from the template; however, when a case team recommends deviating from template language, the case team must highlight any instance of deviation and provide a justification in the draft. The case team should confer with the Compliance Attorney on any questions regarding template language or other issues regarding order construction. When the draft Final Order involves a supervised entity, the case team must also provide the appropriate Supervision region with an opportunity to provide input, consistent with SEFL processes.

The case team must submit all proposed Final Orders to the Compliance Attorney for input before submission to the Enforcement Front Office. The Compliance Attorney is responsible for maintaining and updating templates for both administrative and federal court Final Orders.

Preparation for Monitoring New Final Orders

NOTIFICATION OF SIGNED FINAL ORDER

The CT's compliance monitoring responsibilities for new Final Orders begin when a Final Order has been issued by the Bureau or entered by a Court. The case team will send an email notifying the Enforcement Front Office and CT and attach a copy of the signed order.

COMPLIANCE FOLDER STRUCTURE ON THE ENFORCEMENT SHARED DRIVE

When the CT has received a new, signed Final Order, the CT will create a folder for the order on the Enforcement shared drive. If the Final Order is a Supervision-monitored order, the CT will create the folder within the CT's "SPV Monitored Orders" folder and will save the Final Order in that folder. If the Final Order is an Enforcement-monitored order, the CT will create the folder within the CT's "ENF Monitored Orders" folder. The CT will save the Final Order in that folder and create sub-folders for the CT's ongoing monitoring work, generally for each defendant the CT will monitor.[2]

---

1 "Case team" refers to the team that worked on the underlying matter resulting in the Final Order.

2 The CT does not create sub-folders for ongoing monitoring work for Supervision-monitored orders because the CT is generally not responsible for monitoring compliance with those orders.

The sub-folders the CT will generally create for its ongoing monitoring work include, but are not limited to:

- "Compliance Materials": For submissions/communications from the defendant and communications with the case team or other stakeholders regarding compliance
- "Follow-up": For the CT's work product from recurring follow-up activities (e.g., follow-up memos, underlying resources for follow-up findings, Information Requests or other outreach to defendants or compliance stakeholders)
- "Case Team Materials" or "Background": For materials the CT compiles from the case team or other stakeholders that may be helpful to the CT's ongoing monitoring efforts (e.g., financial disclosures, investigational hearing transcripts)

COMPLIANCE TRACKING INFRASTRUCTURE IN THE COMPLIANCE DATABASE

When the CT has received a new Final Order that Enforcement is responsible for monitoring, the CT will review the Final Order and build the compliance tracking infrastructure in the Compliance Database.[3] The CT will first create a Final Order page in the Database and upload the Final Order into the "Files" area of the page. Next, the CT will create separate Defendant pages for each defendant subject to the order. After creating the Final Order and Defendant pages, the CT will use the Database's Compliance Tracker Builder functionality to create and populate an in-depth, provision-level Compliance Tracker for each defendant.[4] Among other information, the Compliance Tracker will list the provisions of the Final Order that the CT is monitoring, due dates for associated obligations, and the current compliance status. When the CT finishes drafting the Compliance Tracker and designates it as "Under Review" in the Database, the system will automatically email the case team lead attorney, directing him/her to review the Tracker for accuracy and comprehensiveness.[5] The CT will ensure that the case team has completed its review of the Tracker during the Compliance Planning Meeting if the case team has not provided feedback to the CT prior to the meeting.

COMPLIANCE PLANNING MEETING

After reviewing the order and creating the compliance tracking infrastructure in the Compliance Database, the CT will schedule a Compliance Planning Meeting with the case team lead attorney to discuss the underlying case, the Final Order, any issues the team foresees, and the compliance monitoring approach going forward.[6] These communications help inform the CT's monitoring activities for each defendant subject to the order. The Meeting gives the CT the opportunity to learn more about the underlying case, get a better sense of the unlawful actions the order is intended to prevent, the potential for recidivism, tips and best practices to determine

3 The Compliance Database is the centralized system within ENForce that the CT uses to track all ENF-monitored orders, defendants, and provisions with which defendants must comply over time.

4 The CT creates Final Order and Defendant pages in the Compliance Database for all new Final Orders so that Enforcement has a record of all Final Orders entered over time. This includes orders that Supervision is responsible for monitoring, but the CT only enters high-level information into the Database for Supervision-monitored orders and does not create the provision-level Compliance Tracker.

5 The CT relies on the "Lead Attorney" data on the Matter page in ENForce to know which attorney in ENF is the point-of-contact for all matter-related inquiries and activity. If the currently designated attorney will no longer be the POC (e.g., attorney is leaving Enforcement or changing positions), the LD or ALD must assign a new attorney as Lead.

6 Although the CT will generally send the calendar invitation for the Compliance Planning Meeting to only the case team lead attorney, the case team lead attorney may invite other case team members.

compliance with the injunctive provisions for particular defendants based on knowledge gained during the investigation, and other relevant details about the matter that may help with future compliance monitoring and enforcement, such as information about the parties, opposing counsel, and the judge. The case team should also provide the CT with any documents that might assist in compliance monitoring, such as defendants' financial statements. Any ambiguities and questions should also be addressed during this meeting. Optimally, the Compliance Planning Meeting should take place within one month of the effective date of the order.

The CT will draft a short summary of the Compliance Planning Meeting and save the summary in the CT's monitoring folder for the Final Order on Enforcement's shared drive. The CT will also enter any key notes from the Compliance Planning Meeting regarding our monitoring approach or next steps into the Compliance Database.

Compliance Monitoring

INCOMING COMPLIANCE MATERIALS

Defendants submit compliance communications and materials as instructed by the Final Order, typically via email to the Enforcement Compliance Outlook inbox and via mail. The CT is responsible for intaking, reviewing, and tracking incoming compliance materials. The CT will monitor the Enforcement Compliance inbox; review incoming submissions and communications, and address deficiencies as needed; and update the Compliance Database based on the information provided. Substantive communications and submissions will be saved in the "Compliance Materials" sub-folder for the relevant defendant(s) on the Enforcement shared drive. The CT will also route communications and submissions to the case team and other stakeholders as appropriate.

RECURRING FOLLOW-UP INVESTIGATIVE ACTIVITIES

The CT will perform recurring follow-up work on defendants to verify compliance with particular order provisions and/or uncover potential order violations. The CT will adhere to the guidance on order compliance monitoring investigative techniques detailed in Enforcement's "Law Enforcement & Investigative Techniques Manual (LEIM)."

CASE TEAM RESPONSIBILITY FOR CERTAIN COMPLIANCE MONITORING

Monetary Judgments/ Redress Plans and Execution

Case teams remain responsible for all activity related to the monetary provisions of the Final Order, including payment of judgments, redress, civil money penalties, etc. This activity includes review of Redress Plans and recommendation for non-objection by the Enforcement Director, as well as any CMP Fund memos and overseeing redress execution; however, if there is a failure to adhere to a Redress Plan or follow through on Order requirements regarding monetary relief, the case team must consult with the CT and the case team's LD as to next steps (including consideration of opening a Compliance Violation Assessment to engage in collections activity, as described in the section below, Addressing Potential Order Violations).

Compliance Plans

The case team is responsible for reviewing any Compliance Plan submitted by a defendant, working with the defendant as needed to achieve an acceptable Plan, and drafting a brief recommendation to the Enforcement Director regarding non-objection. The Compliance Attorney will review the Compliance Plan when the case team submits it to the Enforcement Front Office (or earlier if the case team has issues/questions) and will send comments within 1-2 days of receiving the case team's recommendation.

Addressing Potential Order Violations

STAKEHOLDER INPUT

If the CT becomes aware of potential order violations through compliance monitoring or other means, the CT will share its findings with the case team. This may help the CT gain additional context regarding the potential violations in addition to ideas for further investigation or other potential next steps.

The CT may also share its findings with Enforcement's Policy and Strategy Team (PST) Senior Counsel for the relevant market, other Bureau stakeholders, and/or external parties. In cases where Enforcement coordinated with local, state, or federal partners during the original investigation, the CT or case team may reach out to those partners to gain additional insight or evidence. Information sharing with external partners will be conducted pursuant to appropriate information sharing agreements and access requests.

DETERMINATION OF FURTHER ACTION

The CT will develop any evidence of potential order violations to the extent possible given its investigative options until the CT can either determine that the defendant is complying with the order or that further investigation or action is necessary.

- If the CT determines that an order violation is likely but does not warrant further action, the CT will draft a brief (one paragraph to one page) memo describing the violations and evidentiary support for the findings. The CT will send the memo to the PST Deputy, who will have three business days to object to the no-action recommendation. If the PST Deputy does not object, the CT will save the no-action memo in the CT's monitoring file for the Final Order on the Enforcement shared drive, update the Compliance Database to note the point-in-time determination, and resume recurring compliance monitoring. If the PST Deputy objects, the CT member who drafted the memo will meet with the PST Deputy to discuss the objection, and the PST Deputy will determine if further action is warranted, and if so, whether the CT should address the issue or recommend that Enforcement open a compliance investigation/compliance violation assessment ("CVA") depending on the action required.[7] A no-action decision does not foreclose future order enforcement. The CT will continue to monitor the Final Order, and if other evidence arises that constitutes

7 A CVA, as opposed to a compliance investigation, is appropriate in cases where the potential violations stem from a court order where such identified violations are solely violations of the order and do not also constitute violations of federal consumer financial protection laws that the Bureau enforces. See also infra note 8.

order violations, the CT will follow the process outlined herein.

- If the CT and/or PST Deputy determines that an order violation is likely and warrants further action, the CT may engage with the defendant to address the issue, recommend that Enforcement open a compliance investigation/CVA, or recommend other appropriate action, such as sending a warning letter or other correspondence, depending on the action required.

  The CT will evaluate its resources to determine whether it has the bandwidth to take on the necessary next steps, including a compliance investigation/CVA and any subsequent action, or whether further activities should be assigned to a Litigation Team. In determining whether an order violation warrants a compliance investigation/CVA, the CT will evaluate whether enforcement action to address the violation would further Enforcement's priorities and whether the harm caused by the violation warrants the use of Enforcement resources to conduct further investigation and potentially a contempt action.

  Factors the CT may consider include, but are not limited to: the amount and type of consumer harm potentially caused by the violative conduct; defendants' willingness to address the issue voluntarily; likelihood of recidivist behavior and other case team input; compliance status globally across orders involving a particular market; potential impact on the relevant market area; deterrent effect of Bureau action; and any other enforcement considerations. The CT should seek input from the case team, the case team's managers, and the PST.

OPENING PROCEDURES FOR COMPLIANCE INVESTIGATIONS AND CVAs

Compliance Investigation Opening Procedures

A compliance investigation, as opposed to a CVA, is generally appropriate in cases where the potential violations stem from an administrative order or a court order where such violations of the order also constitute violations of federal consumer financial protection laws that the Bureau enforces. Compliance investigations will be opened using the procedures outlined below, which are based on the procedures for opening general Enforcement investigations.

- The CT will be responsible for drafting an OIM. Consistent with the requirements of an OIM in EAP, the OIM will include a brief description of the underlying case and relevant Final Order provisions; the conduct that likely violates the Final Order and any other laws the Bureau enforces; and the evidence that supports the potential violations. The cover email for the OIM should also contain a recommendation to the Enforcement Director as to whether to use CT or Litigation Team resources to conduct the contempt investigation and potential action.

- The CT will send the draft OIM to the PST Deputy to provide notice of the potential order violations and supporting evidence.

- If the PST Deputy does not raise objections to the recommendation after three business days, the CT will provide the draft OIM to the case team and the case team's

ALD for input. The CT may also provide the draft OIM to the PST Senior Counsel for the relevant market for input as needed. In cases where the CT is not recommending that the CT handle the matter, the case team and its managers should determine whether the case team (or another attorney within the Litigation Team) wants to handle staffing for the investigation. The CT should note the staffing preference in the cover email for the OIM when it is submitted to the Enforcement Front Office. Litigation Team/PST reviewers will generally have one week to provide input before the draft OIM is re-sent to the PST Deputy for input, but the review time period may be shortened or extended depending on specific stated circumstances.

- After obtaining input from the Litigation Team, the CT will send an updated version of the OIM to the PST Deputy for input. If the PST Deputy agrees with the recommendation to open a compliance investigation, the CT will submit the OIM to the Enforcement Front Office. If there is disagreement among the PST Deputy, CT, and case team regarding the recommendation, the PST Deputy may escalate the matter to the Enforcement Front Office for a discussion and determination.

- The Enforcement Director will make the final determination about whether to approve opening a compliance investigation and if so, which resources to utilize. The Enforcement Director will choose either:
    - To assign the compliance investigation to a case team;
    - To assign the compliance investigation to the CT; or
    - To cease pursuing the compliance investigation and resume recurring monitoring.

- If the Enforcement Director approves the proposed compliance investigation, the Enforcement Front Office will send the OIM through EAP.

- Following the completion of EAP, if the compliance investigation has been approved, the Enforcement Front Office will open the investigation as a new matter in ENForce.

- The CT will update the relevant Defendant pages in the Compliance Database to note that a compliance investigation has been opened, the date on which it was opened, and the team that has been assigned. The CT will suspend its recurring monitoring of the relevant defendant(s) while the compliance investigation proceeds.

Compliance Investigations via the ARC Process

When an ARC matter contains an order violation, the CT should be notified as early as possible, optimally during the Supervisory exam. The CT will weigh in on Enforcement's view of the order violations for purposes of the ARC memo and will provide input into the Enforcement Director's ARC decision.

CVA Opening Procedures

A CVA, as opposed to a compliance investigation, is appropriate in cases where the potential violations stem from a court order where such identified violations are solely violations of the

order and do not also constitute violations of any other federal consumer financial protection law that the Bureau enforces.[8] The CVA is not a new investigation, but instead is post-judgment continuation of the existing matter.[9] CVAs are sent through EAP for notice. Otherwise, the procedures for opening a CVA, as outlined below, are similar to the procedures for opening a compliance investigation.

- The CT or case team will draft a short memo ("CVA Memo") using the established template recommending that a CVA be opened by a Litigation Team (generally the case team that litigated the original action).
- If the CT drafts the CVA Memo, the CT will send the draft CVA Memo to the PST Deputy to provide notice of the potential order violations and supporting evidence. If the PST Deputy does not raise objections to the recommendation after three days, the CT will provide the draft CVA Memo to the case team and the case team's ALD for input. (If the case team drafts the CVA Memo, the CT will send the CVA Memo to the PST Deputy for input after the CT has reviewed the memo). The CT may also provide the draft CVA Memo to the PST Senior Counsel for the relevant market for input as needed. Litigation Team/PST reviewers will generally have one week to provide input, but the review time period may be shortened or extended depending on specific stated circumstances.
- If the PST Deputy agrees with the recommendation to proceed with a CVA, the CT will submit the CVA Memo to the Enforcement Front Office. If there is disagreement among the PST Deputy, CT, and case team regarding the recommendation, the PST Deputy may escalate to the Enforcement Director for a discussion and determination.
- The Enforcement Director will make the final determination about whether to approve a CVA.
- If the Enforcement Director approves the proposed CVA, the Enforcement Front Office will send the CVA through EAP for notice purposes only.
- Following the completion of EAP, the Enforcement Front Office will open the CVA as a new matter in ENForce.
- The CT will update the relevant Defendant pages in the Compliance Database to note that a CVA has been opened, the date on which it was opened, and the team that has been assigned. The CT will suspend its recurring monitoring of the relevant defendant(s) while the CVA proceeds.

Conducting the Compliance Investigation/CVA and Action

Once the Enforcement Director approves and assigns a compliance investigation/CVA, the assigned team (either the CT or a case team) will proceed with the matter. For CVAs, the assigned

8 Because violations of Enforcement's court orders do not themselves specifically constitute violations of the CFPA standing alone, unless there is conduct that would also violate federal consumer financial protection law, Enforcement would be unable to send civil investigative demands. See 12 U.S.C. §§ 5561(1), (5), 5562(c).

9 This would include post-judgment discovery and any investigation of noncompliance for failure to pay. In administrative cases, this would be handled through the OIM process described above.

team will conduct fact-gathering activities using the terms of the Final Order (such as provisions permitting Enforcement to request compliance reports from defendants) and using post-judgment tools provided in the Federal Rules of Civil Procedure (such as Rule 45 subpoenas and Rule 69 discovery).

The assigned team should provide the CT with updates regarding the status of the compliance matter when key developments occur. If CT members are not assigned to the investigation, the assigned team should also seek input from the Compliance Team Lead on key decisions, such as whether to proceed with a contempt action administratively or in federal court.

If appropriate, the assigned team will draft a memo seeking authorization to settle or file a contempt action. The assigned team will draft any contempt filings and associated documents, including a proposed modified Final Order if necessary. The assigned team must send all authorization memos, proposed filings, and associated documents to the Compliance Team Lead for input. The assigned team will adhere to the process and guidance detailed in the Enforcement Process Blueprint when seeking settle and sue authority.

If the assigned team sought authorization to file a contempt action and was approved to proceed, the contempt litigation will proceed in the same manner as any other litigation matter. If CT members are not assigned to the litigation, the assigned team should seek the Compliance Team Lead's input on key developments and any proposed Final Order. If there is a new Final Order at the end of a contempt proceeding, the monitoring process begins again starting at the Preparation for Monitoring New Final Orders section of this guidance.

Reporting

The CT will provide a quarterly report to the Enforcement Front Office to apprise leadership of the CT's work.

Records Retention and Closing Compliance Monitoring

The Bureau's and Enforcement's National Archives and Record Administration-approved record schedules govern how long the CT must retain order-compliance records. Those record schedules are saved in the CT's "Admin & Resources" folder on the Enforcement shared drive. For quick reference regarding compliance documents, which include communications and submissions from defendants as well as work product from the CT's defendant follow-up activities: These documents are addressed by the NARA-approved "Office of Enforcement Schedule." Specifically, these documents would be included within Item 5, "Enforcement Actions." As a result, these documents should be retained for 15 years or permanently if the matter is designated as historically significant. Upon expiration of a Final Order that Enforcement is responsible for monitoring, the CT will follow the procedures set forth in the November 15, 2019 "Order Compliance Closing Procedures" to formally close compliance monitoring, including moving these CT records to the Enforcement matter folder to comply with the Enforcement records schedule. The policy is saved in the CT's "Admin & Resources" folder on the Enforcement shared drive.

Law Enforcement Partners Policies

Working with Criminal Law Enforcement Partners

Cooperating with criminal authorities and other law enforcement agencies is an important part of the Bureau's enforcement mission. The Bureau has authority to bring civil actions to enforce Federal consumer financial laws, but may not bring criminal actions, and must refer evidence of violations of federal criminal law to the Department of Justice (DOJ). Criminal referrals are handled in compliance with the Memorandum of Understanding between the Bureau and the DOJ and our internal policy on criminal referrals. The Bureau's civil authority is not compromised when the DOJ or state criminal authorities conduct a criminal investigation and/or make a determination to bring criminal charges concurrent with the Bureau's investigation and/or civil action. Nonetheless, important considerations arise when cooperating with criminal authorities, as discussed below.

Parallel Criminal Investigations

Staff should consult with a supervisor before engaging in significant discussions and written communications with criminal authorities.

Staff should not take an investigative action for which the sole aim is to benefit a parallel criminal investigation.

Staff should not affirmatively mislead the subject or potential subject of an investigation about the existence or possibility of a parallel criminal investigation or that the investigation is solely civil in nature and will not lead to criminal charges.

RESPONDING TO QUESTIONS ABOUT PARALLEL CRIMINAL INVESTIGATIONS

Staff may invite counsel or any individual to contact criminal authorities if they wish to pursue the question of whether there is a parallel criminal investigation, but do not have to identify which agencies or offices. However, if Staff is in communication with a criminal prosecutor, Staff may ask the criminal prosecutor whether Staff may direct counsel or any individual to contact the criminal prosecutor.

⚠ In most instances, you are under no affirmative obligation to disclose the existence of a parallel criminal investigation.[1] But, if counsel or an individual asks whether there is a parallel criminal investigation, you cannot give a false or misleading answer. The critical point is that you not represent or imply that there is not, or will not be, a parallel criminal investigation, because such a representation is likely to raise valid Fourth and Fifth Amendment defenses to any resulting prosecution. *See United States v. Stringer*, 521 F.3d 1189, 1199-1200 (9th Cir. 2008).

In response to a question by counsel or an individual about the existence of a parallel criminal proceeding, Staff should respond that it is the policy of the Bureau not to comment on investigations conducted by other law enforcement authorities. Staff should also refer counsel or the individual to section D of the Notice to Persons Supplying Information, "Privacy Act Statement".[2] That section states, in relevant part:

> *The information you provide will assist the Bureau in its determinations regarding violations of Federal consumer financial laws. The information will be used by and disclosed to Bureau personnel and contractors or other agents who need the information to assist in activities related to enforcement of Federal consumer financial laws. The information may also be disclosed for statutory or regulatory purposes, or pursuant to the Bureau's published Privacy Act system of records notice, to:*
>
> - *a court, magistrate, administrative tribunal, or a party in litigation;*
> - *another federal or state agency or regulatory authority;*
> - *a member of Congress; and*
> - *others as authorized by the Bureau to receive this information.*

---

1 One court has ruled that civil agencies have such an obligation. See *United States v. Scrushy*, 366 F.Supp.2d 1134 (N.D. Ala 2005).

2 (b)(7)(E)

COOPERATING WITH CRIMINAL AUTHORITIES

Staff should work cooperatively with criminal authorities, share information, and coordinate investigations with parallel criminal investigations where appropriate.

If there is an ongoing parallel criminal proceeding, Staff should consider whether to wait until the criminal proceeding has concluded before initiating a civil investigation. Similarly, Staff should consider whether to stay an ongoing investigation or civil or administrative action after learning of a parallel criminal proceeding. Staff should consult with a supervisor before making or responding to a request for a stay in civil proceedings due to a parallel criminal proceeding. In some instances, a prior conviction or plea agreement will enable Staff to negotiate a settlement without the need for a lengthy investigation. If Staff is in communication with a criminal prosecutor, Staff should consider asking the criminal prosecutor to include enough facts in the criminal plea (if a plea is entered) to find liability in the civil case.

CONDUCTING PARALLEL PROCEEDINGS

The Supreme Court recognized in *United States v. Kordel*, 397 U.S. 1, 11 (1970) that the government can conduct parallel civil and criminal proceedings without violating the Constitution, so long as the government does not act in bad faith. The Bureau may be considered to act in bad faith if it conducts a civil investigation solely for the purpose of obtaining the evidence in a criminal prosecution and does not advise the individual or his or her counsel of the planned use of the evidence solely for a criminal proceeding.[3]

As the Court of Appeals for the D.C. Circuit put it in the leading case of *SEC v. Dresser*, 628 F.2d 1368, 1377 (D.C. Cir. 1980), "effective enforcement of the securities laws require that the SEC and [the Department of] Justice be able to investigate possible violations simultaneously." Other courts have issued opinions to the same effect. *SEC v. First Fin. Grp. of Texas*, 659 F.2d 660, 666-67 (5th Cir. 1981) ("The simultaneous prosecution of civil and criminal actions is generally unobjectionable."); *Stringer*, 521 F.3d at 1191 ("There is nothing improper about the government undertaking simultaneous criminal and civil investigations...").

---

3 For a general discussion of parallel proceedings, see Gabriel L. Gonzalez, Blair G. Connelly & Elias Eliopoulos, Parallel Civil and Criminal Proceedings, 30 Am. Crim. L. Rev. 1179 (1992-1993).

The Dodd-Frank Act expressly provides that the Bureau can share information gathered in a civil investigation with other government agencies and provide information to the Department of Justice for a determination whether to institute criminal proceedings. *See* Section 1056, Title X; 12 C.F.R. §§ 1081.121 (cooperation with other agencies), 1070.43 (disclosure of confidential information to law enforcement agencies).

A civil investigation that precedes a criminal investigation or prosecution is unlikely to result in a finding that the investigation was undertaken in bad faith. *Stringer*, 521 F.3d at 1197 (finding that this sequence of events tended to "negate any likelihood that the government began the civil investigation in bad faith, as, for example, in order to obtain evidence for a criminal prosecution."). Similarly, cooperation with criminal authorities, even extensive cooperation, does not constitute bad faith. In *Stringer*, the SEC cooperated in a number of ways with the U.S. Attorney's Office that was conducting a parallel criminal investigation. The SEC offered to conduct the interviews of defendants so as to create "the best record possible" in support of "false statement cases" against them, and the AUSA instructed the SEC Staff Attorney on how best to do that. *Id.* At the AUSA's request, the SEC took defendants' depositions in the AUSA's district so that the USAO would have venue over any false statements case that might arise from the depositions. *Id.* Finally, the SEC Staff Attorney kept the existence of a criminal investigation confidential. *Id.*

BRADY OBLIGATIONS AND BECOMING A MEMBER OF THE PROSECUTION TEAM

You should be aware that criminal authorities may be constitutionally obliged to disclose to a defendant any information that you share with them and sometimes information that you collect but which you do not share with them. A criminal prosecutor has a duty to seek and disclose exculpatory and impeachment information that is material to the guilt and punishment of a criminal defendant. This information is known as *Brady* material. *See, e.g., Brady v. Maryland*, 373 U.S. 83, 87 (1963); *Kyles v. Whitley*, 514 U.S. 419, 431 (1995). In addition, a criminal prosecutor must disclose *Giglio* material, or evidence that is useful for impeachment, *i.e.*, having the potential to alter the jury's assessment of the credibility of a significant prosecution witness. *See, e.g., Giglio v. United States*, 405 U.S. 150, 154-55 (1972); *Napue v. Illinois*, 360 U.S. 264, 269 (1959) ("[J]ury's estimate of the truthfulness and reliability of a given witness may well be determinative of guilt or innocence.")

In some cases, *Brady* material may include information that you collect even if you never share that information with the criminal prosecutor. A criminal prosecutor is presumed to have knowledge of all information gathered in connection with her office's investigation of the case and "has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case." *Kyles v. Whitley*, 514 U.S. at 437; *see United States v. Payne*, 63 F.3d 1200, 1208 (2d Cir. 1995). Although a civil attorney working on a parallel civil investigation or case is not usually considered a part of the prosecution team, if you act as part of a joint investigative task force you may be considered part of the prosecution team. *See, e.g., United States v. Antone*, 603 F. 2d 566, 570 (5th Cir. 1979) (finding that "extensive cooperation between the investigative agencies" warranted imputation of state agent's knowledge to federal prosecutors). In such a case, information that you collect in a civil investigation will be subject to *Brady* obligations and must be shared with the criminal prosecutor. *See United States v. Meros*, 866 F.2d 1304, 1309 (11th Cir. 1989) (defining prosecution team as "the prosecutor or anyone over whom he has authority.").

Your knowledge of *Brady* material will not normally be imputed to the criminal prosecutor. *See United States v. Locascio*, 6 F.3d 924, 949 (2d Cir.1993) (declining to impute to the AUSAs prosecuting that action knowledge of reports prepared by FBI agents who were "uninvolved in the investigation or trial of the defendants-appellants."); *United States v. Quinn*, 445 F.2d 940, 944 (2d Cir. 1971) (refusing to impute the knowledge of a state prosecutor to an AUSA, rejecting as "completely untenable [the] position that 'knowledge of any part of the government is equivalent to knowledge on the part of this prosecutor.'"). The closer that you work with the prosecution team, however, the more likely it is that a court will deem you part of the "prosecution team" with a resultant obligation that prosecutors disclose your investigative materials under *Brady*. *Moon v. Head*, 285 F.3d 1301 (11th Cir. 2002).

Although it is the criminal prosecutor's responsibility to seek and disclose *Brady* material, to avoid any potential *Brady* issues and to assist the criminal prosecutor in seeking justice, Staff should share any material that Staff believes may implicate *Brady* or *Giglio* with the criminal prosecutor.

In addition, Staff should be aware of a criminal prosecutor's obligations to provide Jencks Act material to the defense. 18 U.S.C. § 3500. Jencks Act material includes statements of a government witness, which are discoverable after the witness has

testified on direct examination at trial. Typically, the material consists of police notes, memoranda, reports, letters, or verbatim transcripts of the witness related to the testimony or relied upon by the witness to testify at trial. Whether or not such witness statements in your possession are Jencks Act material can also depend on whether you are deemed part of the prosecution team. For example, if you take notes regarding consumer statements in a case that is ultimately set for criminal prosecution, the notes may be required to be provided to the defense.

Grand Jury Material

Before receiving information from criminal authorities, Staff should inquire whether any of the information provided comes directly or indirectly from grand jury proceedings, including subpoenas. Absent a court order, Staff should not request or receive grand jury material from any third party. If Staff inadvertently receives grand jury material, Staff should immediately contact a supervisor in order to take appropriate steps.

Staff should receive their supervisor's permission before attending a witness interview in a criminal case.

Staff should receive their supervisor's permission before seeking or receiving designation by a criminal prosecutor as a person to whom a grand jury matter may be disclosed.

The Bureau is generally not privy to grand jury matters, which are subject to confidentiality restrictions set forth in Federal Rule of Criminal Procedure 6(e) and analogous state rules of criminal procedure.

RULE 6 (E) RESTRICTIONS ON GRAND JURY MATERIAL

Under Rule 6(e), "all matter(s) occurring before the grand jury" are secret, subject to certain exceptions. Government attorneys seeking grand jury materials for use in a civil matter must obtain a court order authorizing disclosure of grand jury materials. *United States v. Sells Engineering, Inc.*, 463 U.S. 418, 442 (1983). If you require grand jury materials, you should seek a court order under Rule 6(e)(3)(C)(i), which authorizes a court to order disclosure "preliminarily to or in connection with a judicial proceeding." In most cases, you should make such a request to the court that supervised the grand jury's activities. *See Douglas Oil Co. of Cal. v. Petrol Stops*

Northwest, 441 US 211, 226 (1979). The Supreme Court has interpreted Rule 6(e) to "require a strong showing of particularized need for grand jury materials before any disclosure will be permitted." *Sells Eng'g*, 463 U.S. at 443.

Not all documents presented to a grand jury constitute "matters occurring before the grand jury." "[D]ocuments are not cloaked with secrecy merely because they are presented to a grand jury." *United States v. Lartey*, 716 F.2d 955 (2d Cir. 1983). However, the circuits are divided as to the correct standard for determining whether a document presented to the grand jury constitutes a matter occurring before the grand jury. *See United States v. Dynavac, Inc.*, 6 F.3d 1407, 1412 (9th Cir. 1993) (discussing various standards in use). The Ninth and Second Circuits have both held that business records are not matters occurring before the grand jury. *Dynavac, Inc.*, 6 F.3d at 1412 ("[W]e think that the disclosure of business records independently generated and sought for legitimate purposes would not 'seriously compromise the secrecy of the grand jury's deliberations.'"); *DiLeo v. CIR*, 959 F.2d 16, 21 (2d Cir. 1992) (holding that bank records were properly disclosed). Similarly, the Fourth Circuit has held that material gained through a search warrant is not considered grand jury material unless the search warrant is a *de facto* grand jury process. *In re Grand Jury Subpoenas*, 920 F.2d 235, 243 (4th Cir. 1990).

Due to the circuit split and the fact-intensive inquiries that many circuits use, you should carefully research the local rules and case law in the district where the grand jury sits and consult with your supervisor before possessing any document or requesting any information that has been presented to a grand jury. For more information, see the Department of Justice's Grand Jury Handbook, available at www.justice.gov.

Civil attorneys or investigators can attend interviews of witnesses in a criminal case. But there are potential issues where the witness is expected to testify before the grand jury. For example, "To have violated Rule 6(e)(2), and thus to warrant the invocation of the district court's equity powers, the agents must have disclosed to the ...investigators information revealing what had transpired, or will transpire, before the grand jury." *Blalock v. United States*, 844 F.2d 1546, 1551 (11th Cir. 1988). Therefore, you should speak to a supervisor first and weigh the value of sitting in on such an interview versus the risk of a potential Rule 6(e) challenge.

As a matter of practice, Staff should request that the criminal prosecutor provide Staff with a copy of the interview memorandum or interview report produced by the federal agent conducting the interview. You should be aware that criminal authorities

can turn over memos of interviews and summaries of investigation made by investigators and agents, even after a grand jury has been convened, as long as the documents were not presented to a grand jury. *Anaya v. United States*, 815 F.2d 1373 (10th Cir. 1987).

Finally, the prosecutor can include you on the list of people who are privy to the grand jury's operations under Rule 6(e), thus allowing the prosecutor to share and disclose grand jury information with you. However, being on this list will subject you to the grand jury secrecy rules and prohibits you from disclosing the grand jury proceedings to other Bureau Staff and anyone not on the list. Discuss with your supervisor and seriously consider the impact of being so designated, because the prohibitions on communication may interfere with the investigation or litigation of a Bureau case.

STATE LAW RESTRICTIONS ON GRAND JURY MATERIAL

States have similar rules restricting disclosure of materials presented to grand juries. *See e.g.*, N.J. Court Rule 3:6-7; Kentucky Rule of Criminal Procedure 5.24. Unlike federal grand juries, some state grand juries are also used to investigate civil matters. You cannot assume, therefore, that information shared by state civil authorities has not been presented to a grand jury. As above, you should carefully research state law in the state where the grand jury sits and consult with your supervisor before handling any documents or requesting any information that has been presented to a state grand jury.

Exchanging Confidential Information with Law Enforcement Agencies

This policy discusses the procedure Staff should follow when sharing confidential information with and receiving confidential information from local, state, federal, and tribal law enforcement agencies. In addition, this policy discusses how Staff can securely send and store confidential information. Please be aware that this policy covers only the necessary documentation and procedures for information-sharing. Guidance regarding whether and when information should be shared is found, among other places, in the policies on general referrals and criminal referrals.

Under the Bureau's Rule on Disclosure of Records and Information ("Housekeeping Rule"), 12 C.F.R. § 1070 *et seq.*, confidential information means confidential consumer complaint information, confidential investigative information (CII), and confidential supervisory information (CSI), as well as any other information that may be exempt from disclosure under the Freedom of Information Act pursuant to 5 U.S.C. § 552(b). CII is civil investigative demand material and any documentary material prepared, received, or used in an investigation or enforcement action. 12 C.F.R. § 1070.2(h). Generally speaking, CSI is information that the Bureau collects through supervisory activity.

This policy does not cover sharing non-confidential material, such as publicly available business information or materials cleared by the Bureau for use with law enforcement (*i.e.*, PowerPoints, prepared training documents, etc.). Sharing non-confidential information does not require advance approval but, depending on the source of the information, other restrictions may apply.

For technical guidelines on sending and receiving confidential information, see Securely Receiving and Transmitting Materials.

Responding to Requests for Confidential Information

Staff may receive inquiries from agencies regarding obtaining confidential information in situations in which the agency is not seeking Enforcement information and Enforcement does not have a stake in the request. In those cases, Staff should direct the agency to contact the Bureau's Office of Intergovernmental Affairs for further guidance. If Enforcement information is sought, the request involves a potential joint

investigation, and/or Enforcement has any equities in providing information to the agency, Staff will determine what procedure applies to the information-sharing and guide the agency through the process.

SHARING CONFIDENTIAL INFORMATION WITH A LAW ENFORCEMENT AGENCY

Disclosing any confidential information—orally or in writing—to a law enforcement agency should be discussed with and approved by your ALD in advance. The Bureau's Housekeeping Rule, 12 C.F.R. § 1070 *et seq.*, governs both discussing confidential information with law enforcement agencies in summary fashion and responding to requests from law enforcement agencies for confidential information. In most cases, Legal Division approval will be necessary before sharing any written confidential material.

DISCUSSING CONFIDENTIAL INFORMATION WITH OTHER LAW ENFORCEMENT AGENCIES

Under 12 C.F.R. § 1070.45(a)(5), Staff may share confidential information with law enforcement agencies in summary form *to the extent necessary* to notify the agencies of potential violations of laws subject to their jurisdiction.

Staff may use the affirmative disclosure provision to summarize confidential information, but not to share copies of confidential written documents with another law enforcement agency. The summary disclosure is meant to facilitate, not obviate, the need for agencies to follow the access letter procedure in 12 C.F.R. § 1070.43(b).

Under Section 1070.45(a)(5), Staff may describe a matter with sufficient clarity to allow another law enforcement agency to determine whether it has relevant information to share with Enforcement or if it might be interested in obtaining more information. This description may include such things as entity names, background facts, and laws potentially at issue.

STEP- BY- STEP PROCESS FOR SHARING CONFIDENTIAL INFORMATION

Law enforcement agencies will almost always have to follow 12 C.F.R. § 1070.43(b) to obtain confidential information—even if they are signatories to memoranda of understanding (MOUs) or common interest agreements with the Bureau. Please see the discussion below regarding the agencies who, in some circumstances, might be exempt from this process.

Under the access letter procedure set forth in 12 C.F.R. § 1070.43(b), Enforcement may disclose confidential information to a federal or state agency upon the Legal Division's approval of a written request from the agency that:

- Describes the kinds of information sought and, where possible, the particular documents to which access is sought;
- States the law enforcement purpose for which the information will be used;
- Identifies the agency's legal authority for requesting the information, i.e., the agency's jurisdiction over the matter or entity to which information pertains;
- States whether the requested information may be subject to further disclosure under any applicable law or regulation, such as a state FOIA law, and, if so, can the agency assert any arguments or exemptions to prevent such disclosure; and
- Commits the agency to maintaining the requested confidential information in a manner that conforms to the standards that apply to federal agencies for the protection of the confidentiality of personally identifiable information and for data security and integrity.

Staff have four responsibilities with respect to the access request process:

1. Assisting the requesting agency with completing the letter, if needed;
2. Submitting the letter and accompanying materials to the Legal Division;
3. Preparing any materials approved by the Legal Division for disclosure; and
4. Transmitting the confidential materials to the agency securely.

Assisting the Agency with Completing an Access Request Letter

Staff should provide a template access request letter to an agency that plans to request confidential information. A modified template access request letter is available if the agency is seeking CSI. Both templates are available on SharePoint in the Information Sharing[1] folder.

---

1 (b)(7)(E)

Submitting the Access Request Letter to the Legal Division

Staff should ask the requesting agency to address the request letter to the Legal Division, but submit it to Staff. After receiving the letter, Staff should send an email to the Legal Division with the access request letter and any other relevant documents attached. The email should also address the following 10 questions and items:

1. If you know, does the requestor need the information within any particular timeframe?

2. Do you anticipate working with the requestor on a matter related to the information sought? If so, please describe Enforcement's interest in conducting the potential joint investigation and explain whether sharing the requested information is vital to the potential joint investigation. If not, please explain the Bureau's interest in sharing the information.

3. Do you plan on entering into a common interest agreement with the requestor related to a matter relevant to the information sought? If you have already done so, please provide a copy of the common interest agreement.

4. Please describe the nature of the investigation in which we obtained the information. If you know, please also describe the nature of the investigation for which the information is sought.

5. Please describe the types of information requested, from whom the information was obtained, and how the information was obtained (*e.g.*, financial statements, personnel files, and consumer complaints obtained via CID and voluntary requests to Acme Corp, the subject of an ongoing Enforcement investigation).

6. Does the information requested come from any Bureau component outside Enforcement?

7.

    a. Does the information requested come from an entity currently under examination?

    b. Does the information come from an entity subject to our supervisory authority?

c. Is there any reason that the requested information could otherwise be considered supervisory information?

8. Aside from our Housekeeping Rule, are there any restrictions on our ability or procedures we must follow to disclose the information? For example, is any of the information subject to a protective order, confidentiality agreement, or any type of agreement with another agency? Even if no agreement exists, did the source of the information submit a request that we not further disclose the information? If so, please provide that request.

9. Does Enforcement recommend that the Legal Division grant the request? If not, please explain. In addition, please explain if Enforcement recommends any limitations on granting the request, has concerns about the disclosure of the information, or would like restrictions on how the information may be used.

10. Please state whether Enforcement believes that compliance with the information-sharing request would be burdensome. For example, are the materials already identified? Will they be easy to produce?

Based upon the answers to these questions and the information set forth in the request letter, the Legal Division will determine whether the Bureau is authorized to grant the request. Please note that, depending on the context, the Legal Division may seek additional information to facilitate its determination.

Staff should note that requests for CSI will receive closer scrutiny than other requests. Pursuant to Section 1022(c)(6)(C)(ii) of the Dodd-Frank Act, the Bureau has discretion to share CSI only with an agency that has jurisdiction over the covered person or service provider to which the information pertains. In addition, pursuant to Bureau Bulletin 12-01, the Bureau "will not routinely share confidential supervisory information with agencies that are not engaged in supervision." When a non-supervisory agency, such as a state attorney general, seeks access to CSI, the Legal Division will evaluate the strength of the law enforcement interest at stake in consultation with Enforcement. The Legal Division will also consult Supervision to determine the supervisory implications of sharing the information, if any.

The Legal Division will issue a written letter granting or denying an agency's access request letter. The Legal Division will send Staff a copy of that letter, which will set forth any limitations or conditions that the Legal Division places on the disclosure of the requested information.

Preparing and Securely Transmitting Approved Materials to a Third Party

If the Legal Division approves the disclosure of confidential information, Staff is responsible for executing the disclosure through the following procedure.

1. Staff should stamp all materials to be produced with the footer: "Confidential Information; Property of the Consumer Financial Protection Bureau."

2. In addition, Staff should maintain an electronic copy of the approval letter, along with the transmitted materials, in an appropriately designated subfolder in the case folder on the shared drive, *e.g.*, "Materials Provided to DOJ."

3. Staff should send the requested materials in a format that provides a reasonable level of security for the data, as described in Securely Receiving and Transmitting Materials.

Please be aware that the Legal Division's approval of an agency's request to access the Bureau's confidential information does not imply permission to also utilize the confidential information in court or in another law enforcement proceeding, even if the agency and Enforcement are engaged in a joint or parallel investigation. An agency must separately submit a request to the Legal Division to utilize the Bureau's confidential information in court or in another law enforcement proceeding. In appropriate circumstances, the Legal Division may require the requesting agency to file the confidential information under seal or to obtain a protective order prior to using the confidential information in the proceeding. The Legal Division is available to assist with or respond to any questions or concerns raised by the requesting agency regarding the access request process, particularly any follow-up requests by the agency to utilize disclosed information in a law enforcement proceeding. If you believe the Legal Division should grant anything other than full use of shared information, please speak to your ALD about the best way to proceed.

JOINT INVESTIGATIONS AND STANDING ACCESS REQUESTS

In some circumstances, particularly when Enforcement and an agency have a joint investigation or litigation, it may be impractical for the agency to submit an access request letter each time Enforcement has new information relevant to a matter. In those situations, the agency can submit a written request under 12 C.F.R. § 1070.43(b) that seeks information related to a subject or matter on a standing basis, as permitted by 12 C.F.R. § 1070.43(d).

COMMON INTEREST AGREEMENTS AND PROTECTION OF WORK PRODUC T

If Staff wish to share Enforcement work product with an agency in the instance of a joint investigation or action, Staff should propose that the Bureau and the agency enter into a common interest agreement specific to that investigation or action.
A common interest agreement provides greater protection and flexibility for the ongoing exchange of work product between the Bureau and the agency. The Legal Division has approved a model common interest agreement,[2] available in the Common Interest Agreements folder on SharePoint, that may be used for this purpose. Please be aware that the agency will still have to submit an information access request letter to receive confidential information. To avoid any confusion
about whether the agency will receive confidential information, the best practice is for Staff to ensure the access request is submitted and approved prior to entering into a common interest agreement.

SPECIAL INFORMATION- SHARING ISSUES RELATED TO THE CSBS, FEDERAL PRUDENTIAL REGULATORS, FAIR LENDING INVESTIGATIONS, FTC , AND DEPARTMENT OF EDUCATION

Certain information requests from a small group of federal and state agencies may be governed by MOUs that the Bureau has entered into with the agencies authorizing the bilateral sharing of certain information or a statute requiring the sharing of certain information. If Staff receive a request involving any of the agencies set forth below, they should consult their ALD or the Legal Division to determine whether one of the authorization MOUs or statutes apply and, if so, the procedure for complying with the MOU or statute. While this list may change (a more detailed list[3] can be found on the Bureau wiki), the impacted requests and agencies are:

---

2 (b)(7)(E)

3 (b)(7)(E)

- CSI or personal consumer information requests from a CSBS MOU signatory;[4]
- Requests for any confidential information from the OCC, FDIC, Federal Reserve Board, NCUA, and HUD;
- Exchanges of fair lending investigatory materials with DOJ's Civil Rights Division or among the DOJ's Civil Rights Division, the FTC, and HUD;
- Enforcement information requests from the FTC and/or notifications regarding certain activities;
- Sharing consumer complaint information with the Department of Education; and
- Evidence of criminal violations that we send to DOJ.

The Bureau has entered into a number of MOUs with federal, state, local, and tribal law enforcement agencies that address the mechanics of information-sharing. These MOUs do not replace the access request procedure described above. There are a small number of MOUs between the Bureau and other law enforcement agencies, however, that authorize information-sharing outside the 12 C.F.R. § 1070.43(b) procedure. Navigating the requirements of these MOUs can be difficult and will generally be done in consultation with the Legal Division or according to previous direction from the Legal Division. A list of all of the MOUs that the Bureau has entered into is available on the MOU wiki page.[6]

DATA BREACHES

Staff should immediately report to their supervisor, the Legal Division, and the Chief Information Security Officer, any instance in which Staff know or have reason to believe that:

- Confidential information has been accessed, used, or disseminated internally or disclosed externally without proper authorization or in violation of these procedures or has been lost or stolen; or

4 (b)(7)(E)

5

- An agency with which Staff have shared confidential information has violated the terms of its access or of the Bureau's confidentiality regulations, including by further disclosing the information without permission or using it for purposes other than those specified by the Bureau.

Receiving Information from a Law Enforcement Agency

The procedures below should be used for the receipt of any type of material that an agency wishes to share. Please note that if the agency wishes to send the Bureau consumer complaints to process through Consumer Response, the agency should contact Consumer Response directly.

ESTABLISHING PROTECTIONS FOR SHARED INFORMATION

Before receiving information from a law enforcement agency, Staff should establish— in writing—how the agency wants the information handled and any limitations on using the information. Staff may do this in a letter to the agency requesting the materials. Sample access letters sent by the Bureau to other agencies are kept on the shared drive.[6]

Some agencies have entered into memoranda of understanding or common interest agreements with the Bureau that detail how any information disclosed by the agency should be treated. A list of all of the MOUs that the Bureau has entered into, along with links to some of the actual documents, is available on the wiki.[7]

Common interest agreements are available on SharePoint.[8] If none of these mechanisms apply, Staff should send the ownership disclaimer below to the agency, prior to receiving any materials.

> *The information below describes how the Bureau will treat your materials. Please acknowledge receipt of this information prior to sending materials to the Bureau.*
>
> *Any materials sent to the Bureau remain your property and we will maintain them in a manner identifying them as such. In the event that we receive any legally enforceable demand or request for the materials or if*

6 (b)(7)(E)

7 (b)(7)(E)

8 (b)(7)(E)

they are subject to an affirmative disclosure obligation, we will promptly inform you in writing and provide a copy of the demand or request or description of the obligation.

If the request is made pursuant to the Freedom of Information Act, the Privacy Act, or a state analogue, we will inform the requester that the materials may not be disclosed as they are your property and any request for the materials is properly directed to you.

If the request or demand or affirmative disclosure obligation is not pursuant to these statutes, we will consult with you before complying and give you a reasonable opportunity to respond. We will also assert all reasonable and appropriate legal exemptions or privileges that you may reasonably request. In addition, we will consent to any motion you make to intervene in any action to preserve, protect, and maintain the confidentiality of the materials.

We are not prevented, however, from complying with a legally valid and enforceable order of a court of competent jurisdiction, an order issued by a federal Administrative Law Judge or, if compliance is deemed compulsory, a request or demand from a duly authorized committee of the United States Senate or House of Representatives.

STEP- BY- STEP PROCESS FOR RECEIVING MATERIAL S FROM A LAW ENFORCEMENT AGENCY

Whenever Staff plan to receive information from an agency, they should:

1. Confirm how the Bureau will treat the provided materials. This is done by sending an access request to the agency; confirming in writing that the agency is a signatory to an MOU or common interest agreement with the Bureau; or emailing the ownership disclaimer to the agency.

2. Ask the agency to send the materials in a format that provides a reasonable level of security for the data.

3. If the materials are coming in an electronic format, request a secure folder on the shared network drive from the Help Desk (202-435-7777) at least 24 hours prior to anticipated receipt. Please review the guidance below for more information on secure storage of information.

4. Upon receipt, immediately place the information received in an electronic format in the secured folder. Nothing should be stored in the secured folder, aside from materials provided by the agency. If the materials are in hard copy, they should be placed in a separate file in a locked file cabinet.

5. Label the information with the name of the sending agency, the date sent, and any restrictions on using the information, *i.e.*, "FTC Information Subject to 1/1/13 MOU; Do Not Disclose without Authorization."

Before further disclosing any information provided by the agency, Staff should have written approval from the agency or confirmation from the agency in writing that it does not deem the provided information confidential. Unless prohibited by law or previously agreed otherwise, this approval or confirmation must be sought for any disclosure of another agency's information, regardless of whether the disclosure is discretionary or in the context of an access request, subpoena, discovery request, affirmative obligation, or other compulsory request. If the agency is a signatory to a memorandum of understanding with the Bureau or a common interest agreement related to the information, Staff should follow the notification requirements in those documents.

Further Questions

Talk to your supervisor or use the points of contact[9] on the Enforcement wiki page if you have any further questions.

9 (b)(7)(E)

Criminal Referrals

The Bureau is required by 12 U.S.C. § 5566 to refer to the U.S. Department of Justice evidence it obtains that "any person...has engaged in conduct that may constitute a violation of federal criminal law." This process describes the flow of such referrals within the Office of Enforcement and does not address the broader Bureau policy on criminal referrals.

Processing Potential Criminal Referrals Within Enforcement

When Staff encounters credible information about potential criminal conduct, they should bring it to the attention of the Criminal Coordinator in consultation with their supervisor. The Criminal Coordinator (in consultation with management) will evaluate whether the information involved contains:

- Credible evidence;
- Possible violations of criminal law (federal or other);
- Violations that are within the Office of Enforcement's jurisdiction; and/or
- Connections to any ongoing Enforcement matter.

The Criminal Coordinator will consult with the Enforcement Director/Principal Deputy before transmitting any referral.

All referrals under this policy will be copied to the DOJ Office of the Inspector General (OIG).

Pursuant to 12 U.S.C. § 5566, material that constitutes evidence of criminal conduct may be transmitted to the appropriate criminal authorities without an access request. Sharing any other information must be done under 12 C.F.R. § 1070.43(b), which governs the sharing of confidential Bureau information.

INFORMATION RELATED TO AN ONGOING ENFORCEMENT MATTER

Direct Referrals

Enforcement may make direct referrals to particular offices or divisions of USAOs or DOJ of matters relating to an ongoing Enforcement investigation where Enforcement seeks to work jointly with that office or division. Such direct referrals should be made in consultation with the team's LD, the Criminal Coordinator, and the Enforcement Director/Principal Deputy.

The Enforcement team should keep the Criminal Coordinator apprised of all such referrals, including the transmission of any evidence or documents pursuant to a criminal referral, for purposes of tracking the referral.

Other Referrals

Where Enforcement comes into possession of information relating to potential criminal conduct as part of an ongoing investigation or examination, but where such information will not require close coordination with DOJ/USAO following the referral (*i.e.*, where the matter is collateral to the Enforcement matter) the Criminal Coordinator will receive approval of the Enforcement Director/Principal Deputy prior to forwarding any such information to DOJ/OIG. To the extent that the referral would be appropriate for a particular office or division of the USAOs or DOJ, the Criminal Coordinator may make a direct referral to that office or division.

INFORMATION NOT RELATED TO AN ONGOING ENFORCEMENT MATTER

When the information does not relate to an ongoing matter, the Criminal Coordinator, in conjunction with the relevant Issue Team, will evaluate whether Enforcement should investigate further.

When it is determined that Enforcement will not investigate the information, the Criminal Coordinator will forward to the DOJ POCs and copy OIG and any relevant Enforcement Supervisor where the information appears to be credible and indicates potential criminal conduct.

Communications with Subjects Regarding Referrals

Bureau personnel should not have any communications with subjects regarding the existence of, or status of, a criminal referral. This does not prohibit communicating to a subject that their conduct is in clear violation of criminal law in certain circumstances where it is deemed necessary by the Director or Principal Deputy of Enforcement.

In particular, Staff generally should not make any promises or representations regarding any potential action that the Bureau or the receiving criminal authority might take or has taken in response to the information provided.

The Office of Enforcement should not condition any agreements with a subject on the transmittal of a referral.

Recordkeeping

Enforcement attorneys will forward to the Criminal Coordinator any correspondence from the Bureau related to initiating the referral and from the receiving agency acknowledging the referral. The Criminal Coordinator will keep a record of any referral and a copy of any correspondence initiating or acknowledging the referral. The referral will also be logged in the Leads Database. The Criminal Coordinator will be responsible for forwarding any such correspondence and other relevant materials to the Legal Division, which is responsible for keeping records regarding all criminal referrals by the Bureau.

Civil Referrals—Incoming and Outgoing

Incoming referrals from other law enforcement agencies can serve as a valuable resource for the Office of Enforcement in identifying potential legal violations. Outgoing referrals occur when the Office of Enforcement determines that evidence would be appropriately referred to another agency for evaluation and possible law enforcement action. This policy addresses both types of referrals.

This policy does not apply to re-routing tips or unsubstantiated leads to the appropriate agency, which should generally be handled by the appropriate Issue Team and logged in the Leads Database. This policy also does not address referrals of evidence that any person has engaged in conduct that may constitute a violation of federal criminal law. Such referrals should be handled under the Enforcement process on referring criminal violations to the Department of Justice. The civil referrals policy does not cover referrals made by other SEFL offices, such as Fair Lending referrals
to the Department of Justice of a pattern or practice of discrimination or Office of Supervision referrals.

Receiving Referrals from Law Enforcement Partners

Staff receiving an incoming referral from another law enforcement agency should not make any promises or representations regarding any potential action that the Bureau might take in response to the information provided. If the referral is a Whistleblower tip, Staff should refer to the policy on Handling Law Enforcement Tip Calls and Emails.

If the referral is not received directly by the Issue Team, Staff receiving the incoming referral should forward a copy to the appropriate Issue Team facilitator.

The Issue Team should document receipt of any referral in the Leads Database. Either the Issue Team or Staff receiving the referral should acknowledge receiving the referral to the law enforcement agency that sent it.

After review of the referral, if a staff member recommends the referral be subject to further investigation, they will follow the policy for Opening an Enforcement Matter by completing the Recommendation for Assignment of a Matter Memorandum[1] or

---

1 (b)(7)(E)
(b)(7)(E)

an Opening Investigation Memo.[2] If a staff member does not recommend further investigation, the Issue Team may recommend it, following the same procedure above.

The determination whether to recommend further investigation should be documented in the Enforcement Leads Database.

Any written correspondence pertaining to referrals should be housed on SharePoint in a location to be managed by the paralegal for the Policy and Strategy Team (PST Paralegal).

Staff evaluating the referral should consider the factors listed in the policy for Opening an Enforcement Matter in addition to the following special factors:

- The source of the referral;
- Whether other authorities, including federal or state agencies or regulators, are already investigating the conduct or might be better suited to do so than the Bureau; and
- Whether the Bureau is uniquely situated to address the potential violation.
- If the referral relates to a supervised entity, notify the appropriate POC in the region.

REFERRALS MADE PURSUANT TO SEC TION 1024 (C)(2) OR SEC TION 1025(C)(2)

⚠ If the referring agency specifically states that the referral is made pursuant to Section 1024(c)(2) or Section 1025(c)(2) or recommends, in writing, that the Bureau initiate an enforcement proceeding, the decision to open the matter must be made **within 120 days of receipt of the referral.**

The Issue Team facilitator is responsible for calendaring the deadline for a response and following up, as necessary, to ensure that the deadline is met.

If neither the Issue Team nor a staff member recommends opening a matter, the Issue Team facilitator will send a summary of the referral to the Deputy Enforcement Director for Policy and Strategy (PST Deputy) with a sufficient amount of time for

---

2 (b)(7)(E)
(b)(7)(E)

review before the expiration of the 120 day period. If the PST Deputy believes that a matter should be opened, the Issue Team will follow the procedure policy for Opening an Enforcement Matter by completing the Recommendation for Assignment of a Matter Memorandum or an Opening Investigation Memo.

The Issue Team facilitator is responsible for notifying the referring agency of the decision whether to open a matter in writing within 120 days of receipt of the referral.

Whether the decision is to open a matter or not, the Issue Team facilitator will provide the SEFL Front Office with a summary of the referral and a copy of the notification to the referring agency. The SEFL Front Office will coordinate SEFL review of the referral for general awareness and potential use as field market intelligence.

Making Referrals to Law Enforcement Partners

Whether in the course of conducting a research matter or an investigation, or by some other manner, Staff may uncover reliable information about a potential violation of state and/or federal law that might be more appropriately addressed by another law enforcement agency.

Before making a referral to another law enforcement agency, including the Internal Revenue Service, Staff should seek input from the relevant Issue Team, obtain approval for the referral from their Litigation Deputy, and confirm with the Enforcement Front Office that no other offices should be consulted or copied on the referral. Referrals should be made in writing to the appropriate agency.

Staff must ensure that all referrals are made in accordance with federal law, including the Bureau's confidentiality regulations at 12 C.F.R. 1070.40 *et seq.*, and the Right to Financial Privacy Act, 12 U.S.C. 3401 *et seq.*, as well as the Bureau's internal policies on information sharing, including the policy on Exchanging Information with Law Enforcement Partners, SEFL Staff Memorandum 2014-01, SEFL Policies and Procedures for Sharing Confidential Supervisory Information and Confidential Investigative Information with External Partners. Consult with the Legal Division as necessary.

All document productions must be properly logged and encrypted. See Outgoing Productions. Submit the referral to the PST Paralegal for documentation in the referrals spreadsheet.

NOTE FOR SECTION 5516 (D)(2) REFERRALS TO PRUDENTIAL REGULATORS REGARDING SMALLER DEPOSITORY INSTITUTIONS AND CREDIT UNIONS

Pursuant to 12 U.S.C. § 5516(d)(2), when Staff has reason to believe that an insured depository institution with total assets of $10,000,000 or less, or an insured credit union with total assets of $10,000,000 or less, has engaged in a material violation of a federal consumer financial law, the Bureau shall notify the institution's prudential regulator in writing and recommend that the prudential regulator take appropriate action. The prudential regulator has 60 days to respond to the recommendation.
In these cases, these additional steps should be taken, in addition to following the procedure above:

- Confirm that the matter rises to the level of a formal referral. For purposes of Section 5516(d)(2), "reason to believe" means the Bureau has enough information to support the filing of a complaint. A "material violation" is a violation substantial enough that the prudential regulator would consider it relevant to its decision-making. Information that does not meet the standard for a formal referral may still be sent to the appropriate prudential regulator. Consult your ALD or the relevant Issue Team for more information.
- After obtaining approval for sending the referral from the Enforcement Litigation Deputy, but prior to actually sending the referral, provide a copy of the draft referral to the SEFL Front Office, which will help determine if any other information or notifications are necessary.
- Calendar the date by which a written response is required under Section 1026(d)(2)(B) (60 days from the date Bureau sent the referral).

- Follow up with the prudential regulator by email 60 days after sending the referral, copying the SEFL Front Office and sending the SEFL Front Office a copy of the response, if any.
- Submit all follow-up correspondence to the PST Paralegal for documentation in the referrals spreadsheet.

Bureau Policy on Review and Response to Section 1042 Notices Submitted by State Attorneys General or State Regulators

Section 1042 of the Consumer Financial Protection Act (CFPA) provides state attorneys general and state regulators independent authority to bring actions or administrative proceedings to enforce the provisions of the CFPA or regulations issued thereunder, except that state attorneys general may bring actions against national banks or federal savings associations only to enforce regulations issued under the CFPA. 12 U.S.C. § 5552(a).[1]

Ten calendar days before initiating any such action or proceeding, the state attorney general or state regulator must provide a copy of the proposed complaint to the Bureau, as well as a notice describing:

- The court or body in which the action will be initiated;
- The identity of the parties;
- The nature of the action;
- The anticipated date of the action;
- The alleged facts underlying the action;
- The name, email address, and phone number of a state official who can consult regarding the matter;
- A determination of whether there exists a need to coordinate the prosecution of the action or proceeding to avoid interference with any action, including a rulemaking, of the Bureau or any other federal agency; and
- A statement regarding any limitations on the disclosure of the substance of the matter or the fact of the notice outside of the recipient agency. Id. § 5552(b)(1); 12 C.F.R. § 1082.1(a), (c).

Such notice may be delayed until the initiation of the matter if prior notice is not practicable, or otherwise for good cause. 12 U.S.C. § 5552(b)(1)(B); 12 C.F.R. § 1082.1(b). In the event the notice is delayed until after the initiation of the

---

1 Please contact the Legal Division with any questions about the interpretation of this provision.

proceeding, the notice should also contain: a description of any proceedings in the action to date, including any orders issued; the case or matter number assigned to the action or proceeding; any information regarding scheduled court or administrative proceedings; and a complete and unredacted copy of any document filed in the proceeding to date. 12 C.F.R. § 1082.1(c)(3), (4).

Upon receipt of a notice described above, the Bureau may intervene in the action as a party; upon intervening, remove the action to the appropriate United States district court, if it was not originally brought there, and be heard on all matters arising in the action; appeal any order or judgment to the same extent as any party; and otherwise participate in the proceeding as appropriate. 12 U.S.C. § 5552(b)(2); 12 C.F.R.
§ 1082.1(d).

Bureau Review of Section 1042 Notices

Notices described above are required to be sent by email to the Bureau's Executive Secretary and its Office of Enforcement. 12 C.F.R. § 1082.1(a)(2). Upon receipt of such notices, the Executive Secretary shall immediately distribute the notice and any attachment to the Legal Division and the Office of Intergovernmental Affairs, with
a copy to the Office of Enforcement. If the Office of Enforcement receives a notice that is not also sent to the Executive Secretary, or if the Executive Secretary fails to promptly distribute the notice as described above, the Office of Enforcement will be responsible for distributing the notice and copying the Executive Secretary.

Within five calendar days of the receipt of any notice and its attachments, assigned staff from interested divisions will consult with one another, other relevant staff members, and relevant managers, in order to arrive at a consensus regarding the appropriate course of action. The appropriate course of action may include, but is not limited to, one or more of the following:

- Consultation with the relevant state official to express concern or disagreement with any proposed interpretation of federal consumer financial law or any course of action;
- Consultation with other federal agencies, as appropriate;
- Immediate intervention; and/or
- A decision to monitor the proceeding to determine whether future intervention or amicus participation is warranted.

The Bureau's position shall be communicated to the state official as soon as possible after consensus is reached. The Office of Enforcement will be primarily responsible for communicating the Bureau's position to the relevant state official, but it should copy the assigned staff of the Legal Division in all correspondence with the relevant state official and the Office of Intergovernmental Affairs, in appropriate circumstances. The Legal Division shall maintain all files related to a notice or proceeding in electronic format in a separate folder.

Intervention in a matter will require Director authorization pursuant to the existing Enforcement Action Process. Amicus participation in a matter will require authorization through the existing Amicus Working Group process. The Legal Division, in coordination with the Office of Enforcement, will monitor developments in matters brought by a state official under section 1042. Significant developments will be communicated to relevant staff and managers and, if appropriate, to the Director in the form of an information memorandum.

In emergency situations in which the Bureau is not afforded the standard 10 calendar days, review of a notice and its attachments should follow the same process under an agreed upon time frame appropriate for the circumstances.

Procedure for Reviewing Section 1042 and MARS Rule Notices

This procedure complements the Bureau Policy on Review and Response to Section 1042 Notices Submitted by State Attorneys General or State Regulators. Specifically, this procedure details the role of the Office of Enforcement in reviewing and responding to Section 1042 and Mortgage Assistance Relief Services (MARS) Rule notices.

Section 1042 requires state attorneys general and regulators send notice of potential actions under the CFPA or regulations promulgated thereunder to Enforcement@cfpb.gov, which is monitored by the Enforcement Front Office, and ExecSec@cfpb.gov. When the Enforcement Front Office receives a Section 1042 notice, it will send the notice to the individual on the Enforcement Policy and Strategy Team (PST) assigned to maintaining state attorney general relationships (AG contact), unless another point of contact for reviewing the notices has been established. The Enforcement Front Office or the AG contact will also forward the notices to the Senior Team. The AG contact will review the notice and send it, as well as any additional information relevant to the action or relationship, to the Legal Division's Section 1042 point of contact. If the notice came directly from the state and it does not appear that it was sent to ExecSec@cfpb.gov, the notice will also be sent to the Assistant Director and Deputy Assistant Director of the Office of Intergovernmental Affairs and the Office of the Executive Secretary. If the notice pertains to a statute or regulation that requires notice to another agency, it will also be sent to the point of contact at that agency.

Within five days of receipt, the Legal Division will review the notice and notify the AG contact about any potential conflicts with Bureau precedent or interpretation of the CFPA and the proposed Bureau response. The AG contact will discuss the notice and the Legal Division's review with the Deputy Director and Assistant Deputy Director for Enforcement Policy and Strategy to determine if there are issues that should be raised with other Bureau components. In addition, the AG contact will forward the notice to the appropriate issue team lead.

If Enforcement and Legal do not intend to raise any substantive issues with the state, the PST AG contact will send the state attorney general or regulator a letter confirming receipt of the notice, asking for the state to send us a file-stamped version of the complaint, and reminding the state to keep the Bureau in the loop on any

discovery disputes, dispositive motions, or court rulings related to the CFPA claim. The PST AG contact will copy IGA and the Office of the Executive Secretary on the email sending this correspondence.

To the extent there are substantive issues with the notice or any comments related to the notice, the AG contact will call the state attorney general or regulator and discuss the matter orally. The Legal Division may participate in this call, if they wish to do so.

The draft and final notices, as well as any other materials received from the state, will be kept in the following folder on the shared drive: (b)(7)(E)

(b)(7)(E)

The PST paralegal or admin will ensure that the notice is logged on the notice tracking spreadsheet.[1] In conjunction with the Legal Division, the AG contact will stay informed about the progress of the state attorney general or regulator's action. The PST paralegal or admin will ensure that the notice is logged on the notice tracking spreadsheet. In conjunction with the Legal Division, the AG contact will stay informed about the progress of the state attorney general or regulator's matter and inform the Deputy Director and Assistant Deputy Director for Enforcement Policy and Strategy and Assistant Director and Deputy Assistant Director of the Office of Intergovernmental Affairs of any significant developments. The AG contact will also provide any requested information to the Executive Secretary for the Bureau's Semi-Annual Report.

As with required notice for CFPA claims, the MARS Rule also requires notice to the Bureau under 12 U.S.C. § 5538. When the Enforcement Front Office receives notice that a state attorney general is filing an action asserting a claim under the MARS Rule, it will forward the notice to the AG contact for review. The AG contact will review the notice and determine whether the Bureau or FTC has a pending matter involving the subject of the proposed state attorney general action. The AG contact will send the notice, as well as any additional information relevant to the action or relationship, to the Legal Division's Section 1042 point of contact and the PST counsel assigned to debt relief. If the notice came directly from the state and it does not appear that it was sent to ExecSec@cfpb.gov, the notice will also be sent to the Assistant Director and Deputy Assistant Director of the Office of Intergovernmental Affairs and the Office of the Executive Secretary.

---

1 (b)(7)(E)

Within five days of receipt, the Legal Division and PST debt relief counsel will review the notice and notify the AG contact about any potential conflicts with Bureau precedent or interpretation of the MARS Rule. If Legal and the PST debt relief counsel do not raise any substantive issues, the PST AG contact will send the state attorney general or regulator a letter confirming receipt of the notice, asking for the state to send us a file-stamped version of the complaint, and reminding the state to keep the Bureau in the loop on any discovery disputes, dispositive motions, or court rulings related to the MARS Rule claim. Enforcement will copy IGA and the Office of the Executive Secretary on the email sending this correspondence. The PST AG contact will also send a copy of the notice and the Bureau's response to the FTC.

To the extent there are substantive issues with the notice or any comments related to the notice, the AG contact and PST debt relief counsel will call the state attorney general or regulator and discuss the matter orally. The Legal Division may participate in this call, if they wish to do so. Materials related to the notice will be logged and tracked in the same manner as Section 1042 notices.

Part 2: Practice Guidance

DISCLAIMER:
These Practice Guidance documents are intended to facilitate your work in the Office of Enforcement. They are not official policies or procedures of the Office, but rather represent recommended best practices. They are meant to be followed at your discretion in light of the specific circumstances surrounding the particular investigation.

Ethical Guidance Related to Obtaining Information from Consumer Response

Consumer Response Investigators may occasionally contact attorneys with questions involving a person or entity that is currently the subject of an Enforcement matter.

Staff may not direct, order, or instruct Consumer Response Investigators to contact the subject of a complaint or obtain materials from the subject of a complaint. If Staff provide any opinion to Consumer Response Investigators regarding follow-up conversations or obtaining documentation from the subject of a complaint, Staff should clearly state that the advice is just an opinion, which the Investigators are in no way obligated to follow.

You are not prohibited from providing advice to investigators in Consumer Response under Rule 4.2 of the Model Rules of Professional Conduct, as long as you do not *direct* investigators to communicate with or request materials from a company. Ethical concerns are not raised when you provide *advice* to Consumer Response investigators about issues in consumer complaints, even if the company is the subject of an Enforcement matter. Advice may consist of opinions about whether a legal violation has occurred and what documents might be relevant to that analysis. You may also obtain information received as part of a Consumer Response investigation as long as the information was not obtained at your direction. If you have any questions about ethics rules, please contact the Ethics Office of the Legal Division at EthicsHelp@cfpb.gov.

Requesting CSI from OCC

(updated January 2019)

The following process is to be used when staff requests information that might constitute confidential supervisory information from a bank. The first step is to make a written request to the bank for the information. Presumably, this request could be a civil investigative demand or a voluntary request in lieu of a CID. The request should say that we understand that some of the information we are seeking may be OCC non-public information, and that we request that the bank request permission from the OCC to release the information to the us. We should advise the bank that, pursuant to 12 C.F.R. Part IV, it should direct its request to Greg Taylor, Director of Litigation, Office of the Comptroller of the Currency, 400 7th Street, SW, Washington, DC 20219. We should copy the OCC Enforcement Director Monica Freas on the request.

The OCC would then authorize the bank to share its information with the us (and require the bank to provide the OCC with an inventory of documents provided to us for their tracking purposes). The OCC would send a separate letter to us authorizing the release pursuant to Part IV, including restrictions on our use and disclosure of the information. Because we are the Enforcement Office conducting an investigation (as opposed to a supervisory examination), the letter would not apply to the bank's privileged information (attorney-client, work product).

The Enforcement POC for purposes of receiving the OCC letter authorizing the release of information is the Enforcement Director.

When such a request is made to a bank, and/or when any response is received from the OCC, please notify the Enforcement Front Office via the Senior Counsel to the Director.

Securely Receiving and Transmitting Materials

Ways to Transmit Information Securely

The methods listed below are acceptable ways to send or receive information, listed in order of preference.

ELECTRONIC TRANSMISSION

For sensitive information sent electronically, either the transmission should be encrypted or the data itself should be encrypted. Sending restricted data in encrypted, password-protected attachments is acceptable as long as the password is communicated separately, securely and, ideally, in an alternative method (*e.g.*, by phone, in person, or in the mail). The password should never be sent in the email containing the attachment.

REMOVABLE MEDIA

Sensitive information should not be on removable media unless the data is encrypted. The Bureau does not accept all types of removable media. Staff should confirm the acceptability of the removable media with the eLitigation Support Specialists team prior to receiving the information.

ACCEPTABLE PHYSICAL DELIVERY METHODS

Physically mailing hard copies of sensitive information should only be done using the U.S. Postal Service's First Class Mail, Priority Mail, or an accountable commercial delivery service (*e.g.*, DHL), with the documents sealed in an opaque envelope or container. If possible, use a receipted delivery service (*i.e.*, Return Receipt, Certified, or Registered mail) or a tracking service to ensure secure delivery is made to the appropriate recipient, or contact the intended recipient to confirm receipt.

FACSIMILE

Senders transmitting via facsimile should use a cover sheet that states that the fax includes sensitive data and clearly indicates the recipient. The sender should also confirm receipt.

Advice to Law Enforcement Agencies on the Secure Transmission of Information

Although the Bureau does not require that law enforcement use a particular method of secure transmission, you may offer general guidance on best practices. You may wish to include the following statement in your correspondence with the agency that is sending you information:

> *We ask that you send us the information in a format that provides a reasonable level of security for the data while it is in transit. While we do not require that you use any particular method, examples of reasonable security measures include using:*
>
> - *A password-protected Zip file;*
> - *An encrypted email using ZixSelect;*
> - *Certified mail; or*
> - *An encrypted form of removable media, such as a CD or DVD.*
>
> *The Bureau has certain limits on removable media, so please contact me if you would like to use that option or if you have any other questions about secure methods of transmitting data.*

Shared Information Should be Securely Stored

Staff should create an access-restricted folder to store shared electronic information or, if information is shared in paper form, store it in a locked location. The Help Desk will apply security restrictions to a folder, but Staff should first create a folder in the location the information will be stored. The folder name should indicate the owner of the information, *i.e.*, (b)(7)(E)

(b)(7)(E) . If there is a common interest agreement, MOU, or access letter that governs treatment of the shared information, that document should be kept in the folder. Access to this folder should be restricted to a designated subset of Bureau employees who have a bona fide need for the information to carry out their

assigned job responsibilities. To apply the security restrictions, the Help Desk will need to know the file location and a list of Bureau employees with need-to-know and specific access permissions for the data (read, write, etc.).

Further Questions

Talk to your supervisor or use the points of contact[1] on the Enforcement wiki page if you have any further questions.

1 (b)(7)(E)

Outgoing Productions

The production of documents to parties outside of the Bureau, most often in the form of electronically stored information, arises in three situations:

1. Discovery in administrative proceedings and litigation,
2. The sharing of documents with partner federal agencies and states, and
3. The retention of consulting and litigation experts. These productions raise a number of legal and security issues. Staff should follow a consistent framework for managing outgoing productions in order to comply with legal obligations and security of Bureau information.

Protecting Bureau Information

The Bureau has a legal responsibility to safeguard personally identifiable information (PII), confidential supervisory information (CSI), and confidential investigative information (CII). Definitions for these types of information can be found in the Handbook for Sensitive Information.[1] In particular, 12 C.F.R. 1070.41 provides that, except as provided by law, no employee of the Bureau shall disclose CSI or CII. Further, the Bureau Acceptable Use Policy[2] requires that employees maintain the security of Bureau information and only share such information as specifically authorized, such as sharing information pursuant to an MOU or providing such information in discovery.

You should be familiar with the types of information held by the Bureau, including PII, CSI, and CII and the requirement to safeguard such information under 12 C.F.R. 1070.41. You should only direct the production of information outside the Bureau as specifically authorized in your matter through the administrative rules, federal discovery procedures, or an MOU.

When sharing Bureau information with an expert, attorneys must ensure that before any information is shared, the expert has signed a non-disclosure agreement. Sharing Bureau information with experts also raises legal concerns. Federal Rule of Civil Procedure 26(a)(2)(B) requires that a litigant produce to the opposing party all "facts

1 (b)(7)(E)

2

or data considered" by an expert who will testify at trial in formulating the expert's opinion. Fed. R. Civ. P. 26(b)(4)(D) provides that similar information need not be disclosed to the opposing party when it is provided to a non-testifying (consulting) expert (*United States v. Second Chance Body Armor, Inc.*, 288 F.R.D. 222 (D.D.C. 2012)), and that information is treated as work product under Fed. R. Civ. P. 26(b)(3)(A) (*Apple v. Amazon*, 2013 WL 1320760 *1 (N.D. Cal. April 1, 2013)). If a consulting expert becomes a testifying expert, work product may still serve to protect from disclosure those facts or data considered by the expert when the expert was acting in the role of a consulting expert. However, work-product may only be asserted as to materials that do not pertain to the subject matter of which the expert testifies (*SEC v. Reyes*, 2007 WL 963422, *2 (N.D. Cal. March 30, 2007)). Whether the materials relate to the subject matter to which the expert will testify is determined from the content of the documents themselves. *Id.*

As a best practice in investigations, Enforcement Staff need to keep an accurate list of all documents provided to any expert in order to comply with the clear mandate of the Fed. R. Civ. P. that those documents must be disclosed if the expert is to testify. This list should also be maintained with regard to consulting experts because they may become testifying experts. When an expert wears two hats as both a consulting and a testifying expert, the documents provided to the expert will need to be analyzed to determine what must be disclosed to the opposing party. When sharing documents with experts and consultants, attorneys should be aware that, for security reasons, access to Bureau systems cannot be granted to an expert or consultant.

In order to meet these legal and security obligations and best practices, Enforcement Staff must be accountable for the production of any Bureau information by tracking what, when, and to whom such information is provided. This accountability is ensured by following the procedures set forth below.

If the case team anticipates any outgoing production, the team should contact the eDiscovery distribution list as early as possible to ensure there is adequate time to create productions. There are certain trigger points where the need for outgoing productions becomes almost certain and the case team should initiate these procedures (*e.g.*, when a decision is made to hire an expert, or when a decision is made to file an administrative notice of charges or complaint in district court).

Prepare the Production

The case team creates a record of the documents to be produced in Clearwell or Relativity by tagging the documents. If the case team is not using a review platform, they will create a manual list of the documents to be produced.

After the tagging is complete or the list of documents is created, the case team sends an email to the e-Litigation Support Specialist assigned to the matter and the eDiscovery distribution list (DL_CFPB_eDiscoveryIT@cfpb.gov) with that information, requesting that a production be created. In that email the case team should specify the prefix for the application of Bates numbers to that production. This is a new Bates number for purposes of this production and will be different from and in addition to any Bates numbers already existing on the documents.

The e-Litigation Support Specialist assigned to the matter will create an outbound production request in EINForce and have the production prepared, including applying the production-specific prefix Bates numbers, and copied to the appropriate media.

Production Format

All outgoing productions will generally be provided on encrypted physical media (DVDs, hard drives, thumb drives) pursuant to the following procedures:

- The eDiscovery Team will have the information properly marked to give notice to the recipient of the sensitive nature and ownership of the information. Each production will have the media stamped (and each document if possible) with language that states: "BCFP Property; disclosure governed by 12 C.F.R. Part 1070."
- An electronic copy of the production will be created by the eDiscovery Team and maintained in a folder in Relativity or Clearwell or on a shared drive. A physical copy of the production media will be retained by T&I in case additional copies are needed.
- The e-Litigation Support Specialist will provide a copy of the production on the physical media to the case team and will provide the password for the physical media under separate cover.
- The case team is responsible for delivering the physical media using a delivery method that can be tracked (*e.g.*, UPS).

- The case team should provide the password to the recipient by separate email or other delivery method from that used to deliver the physical media.

- The case team paralegal is responsible for uploading the outgoing production tracking label to the ENForce recipient page found on the case detail screen.

Under certain exigent circumstances, productions can be made through email using encrypted files pursuant to the following procedures:

- The case team obtains approval of an ALD to use email.

- The case team consults with the assigned e-Litigation Support Specialist to obtain the production in the proper electronic form and to ensure that the outgoing email is sent using the proper encryption to secure the integrity of the production.

For further details on delivering materials, see Securely Receiving and Transmitting Materials.

Part 3: Administrative Policies

Conference and Training Attendance Policy

(updated January 2019)

In support of their work at the Bureau, Office of Enforcement Staff may attend conferences and trainings to sharpen skills and substantive knowledge, enhance relationships with key stakeholders, and stay on top of new and cutting-edge developments in our sphere. Accordingly, Staff may attend conferences within the parameters described in this policy.

Staff may determine what conferences to attend in accordance with this policy, but may only attend conferences that their supervisor approves and must be relevant to their work. Staff are encouraged to provide readouts from the conference to the Enforcement Front Office.

Conference registration will be handled by a Legal Assistant designated by the Chief of Staff. Staff should indicate their interest in attending a conference to the designated Legal Assistant no later than 30 days before the conference registration deadline. Failure to indicate interest within 30 days may complicate procurement of conference fees and may compromise one's ability to attend a conference.

Conference attendance will be presumptively capped in three ways:

- No person may incur more than $3,500 in costs associated with conference attendance during a single fiscal year (October 1 to September 30). This includes all costs associated with conference attendance (registration fees, travel, hotel, etc.).
- No person may spend more than six business days attending conferences during a single fiscal year.
- No more than 10 people from the team may attend any conference.

The Chief of Staff may grant exceptions to any of these presumptive caps in specific circumstances when appropriate and justified. The caps will be modified as appropriate for those who have roles which specifically necessitate greater participation in conferences (*e.g.*, for people with significant outreach responsibilities).

Staff are responsible for ensuring that they comply with these caps and that their conference costs and attendance are tracked on the speaking engagement/ conference attendance tracking spreadsheet.

This policy should be observed in accordance with Bureau-wide policies on training.

Staff should be attentive to any ethical restrictions on conference participation or activity.

Whenever applicable, Staff should obtain CLE credit for conferences attended.

The limit on team participation in any conference will be managed on a "first come, first served" approach with sign-ups maintained by the designated Legal Assistant. To the extent 10 team members are already registered for a conference and there is a particular need to have one or more individuals attend the conference who are not registered, swaps will be negotiated or additional slots will be authorized.

The Office of Enforcement's Public Speaking Policy governs Staff participation in conferences as speakers, panelists, etc. Attendance at conferences in such capacity on the day of the speaking engagement will not count against the caps above. Further, if a supervisor specifically requests that a team member attend a particular conference, that conference will not count against the caps above for that team member.

Public Speaking Policy

The Office of Enforcement recognizes the value of Staff periodically making public presentations. This policy explains how decisions will be made about public speaking opportunities. It applies to speaking invitations directed to Staff and similar opportunities they identify.

Staff receiving speaking invitations or identifying speaking opportunities that might benefit the Office of Enforcement and/or the Bureau should notify his or her supervisor and the Chief of Staff.

Supervisors will decide whether invitations should be accepted or presentation opportunities should be pursued, according to the factors described below.

If it is determined that someone from the Office of Enforcement should make the presentation, that person, in coordination with his or her supervisor, should coordinate with the Bureau's Office of External Affairs before committing to any speaking engagement.

Remarks should be cleared by the speaker's supervisor or another member of the senior team. When speaking, Staff should first offer a disclaimer that the remarks do not represent official Bureau views.

Costs of the conference and travel will be paid for by the Bureau. The sponsoring entity may not reimburse the speaker, but it may waive the fee for the event on the day the speaking occurs.

The day on which a person speaks does not count against his or her "conference days," and any costs associated with the speaking engagement itself (*e.g.*, airfare, hotel for day before/of speaking engagement) do not count against his or her annual conference attendance budget.

It is the responsibility of the person who receives a speaking invitation to ensure that an appropriate response to the invitation is made. It is the responsibility of the person who speaks to log the engagement on the speaking engagement/conference attendance tracking spreadsheet.

Supervisors will use the following factors in deciding whether an invitation should be accepted:

- Whether accepting the invitation promotes the mission of the Office of Enforcement and/or the Bureau;
- Whether the event provides an opportunity for the Office of Enforcement to build relationships with partners or relevant constituencies;
- Whether the topic to be discussed relates to an articulated enforcement priority or presents an opportunity to discuss an enforcement initiative; and
- What resource investments are associated with accepting the invitation in terms of working time spent, travel costs, admission fees, etc.

The person who receives an invitation to speak (or identifies a speaking opportunity) will not automatically be selected to make the presentation. Rather, supervisors will consider the following factors in determining who should speak:

- Ability to perform this task well, taking into account experience working on the particular issues to be discussed, and interest and involvement in similar/ related projects;
- Time to perform this task without undue interference with other work.
- Other public speaking opportunities;
- Receipt of the invitation to speak and interest in making the presentation; and
- The extent to which the invitation is only for the individual to whom it was directed.

Enforcement Attorney Hiring Process

Posting

Generally, Enforcement will hire Enforcement Attorneys through USA Jobs postings.

We will request a resume and cover letter from all applicants. Applicants who are asked to come back for a second-round interview will be asked to provide a writing sample.

Candidates will be hired for the office, rather than for specific litigation teams. When new hires are assigned start dates, the Litigation Deputies and the Front Office will determine which team the attorneys join.

Resume Review

For each posting, a resume review group will be assembled to review resumes.

The resume review group will be composed of five to eight attorney volunteers from the team, with the number dependent on the volume of applications. Litigation Deputies may suggest attorneys to participate in resume review. The Chief of Staff will select attorneys to participate. The resume review group will participate in diversity and structured-interview training before reviewing resumes.

The resume review group will consider the following in recommending candidates to be interviewed:

- The Enforcement Attorney position description
- The expectations for attorneys at each level in the Office of Enforcement
- The qualifications of the individual candidates, with particular attention paid to the following attributes:
    - Litigation and investigatory experience
    - Legal experience generally
    - Consumer law experience
    - Academic achievement
    - Clerkship(s)

- Demonstrated commitment to public service
- Interest in the Bureau's mission
- Any other skill or expertise identified by the office at a particular time

The resume review group will recommend candidates to interview. The Chief of Staff, in consultation with the Litigation Deputies, the Principal Deputy, and the Enforcement Director, will select the final group to be interviewed.

The number of candidates to interview will depend on the number of vacancies to be filled.

Interviews

Candidates will participate in structured interviews.

For each posting, an interview group will be assembled to interview candidates. The interview review group will be composed of eight attorney volunteers from the team. Litigation Deputies may suggest attorneys to participate in interviews. The Chief of Staff will select attorneys to participate. The interview group will participate in diversity and structured-interview training before conducting interviews. Managers participating in interviews will also complete these trainings.

Interviews will be structured as follows:

- 45 minutes with three members of the interview group.
- 45 minutes with an LD, an ALD, and the Chief of Staff.
- The first group will ask Interview Questions Set 1 (to be provided to interviewers).
- The second group will ask Interview Questions Set 2 (to be provided to interviewers).

Interviewers will complete interview packets immediately after the interview. Interviewers will meet as a group during the week that the interview occurs to discuss the candidate(s) interviewed. Interviewers will recommend candidates to return for a call-back interview. The Chief of Staff, in consultation with the Litigation Deputies, the Principal Director, and the Enforcement Director, will select candidates for call-back interviews.

Call-back interviews will be structured as follows:

- 30 minutes with the Enforcement Director (and Principal Deputy, if available).
- 30 minutes with any LD who has a vacancy and who did not meet the candidate during the first round of interviews.
- Both interviews will be conducted without set questions.

Final hiring decisions will be made by the Chief of Staff, in consultation with the Enforcement Director, the Principal Deputy, and the LDs.

Internal Candidates

Candidates who are already employed by the Bureau, but not the Office of Enforcement, will apply and interview according to the process described above.

Candidates who are already employed by the Office of Enforcement and who wish to apply to vacancy announcements for regional offices will notify the Chief of Staff of their interest by submitting a resume and cover letter. These candidates will be interviewed only by management and considered in advance of external candidates who apply to the posting.

Reserve Pool

If we end up with more candidates we wish to hire than spaces available, we will maintain a list of candidates to contact in the future when vacancies arise. The Chief of Staff will contact these candidates to let them know that they remain in the reserve pool.

Intern Use of Writing Samples

We encourage Enforcement interns to seek out written work. If interns are particularly interested in creating something that can be used as a writing sample, they should talk to the intern coordinators about obtaining assignments conducive to developing this work product.

The following guidelines apply to use of writing samples created during internships in the Office of Enforcement:

- It is generally not OK to use as a writing sample any memo discussing the following:
    - Bureau authority or jurisdiction
        - Statutes of Limitation or Retroactivity
            - The use of prosecutorial discretion
        - Discussions where the law *in a particular area of interest to the Bureau and our constituencies* is unclear and the author advocates a particular viewpoint
        - Memos that clearly identify a particular investigation or pending case
- It is generally OK to use as a writing sample any memo discussing the following:
    - Black letter law
    - An analysis of law and fact that is non-controversial or so specific to the particular facts presented that it would be unlikely to have general applicability to other matters
    - A discussion of process, federal or administrative procedure, or ancillary legal issues (*e.g.*, rules of evidence, FOIA)

When someone who has worked as an intern in the Office of Enforcement would like to use their own written work product created during their internship as a writing sample for a future opportunity, he or she should do the following:

- Talk to the attorney who assigned the project to get a general sense of whether the memo contemplated would be appropriate for a writing sample, based on the guidelines above and the attorney's knowledge of the matter for which the memo was created (Enforcement Attorneys may consider consulting with ALDs if they are unsure about what to recommend).
- Redact any case/investigation-identifying information, names, facts, application of law to facts, etc.
- Prepare the document on blank or personal (not Bureau) letterhead.
- Include the following header on the document:
  This writing sample reflects work performed by the author during an internship at the Consumer Financial Protection Bureau. It has not been edited by any employee of the Bureau. The views expressed herein are the author's only, and have not been adopted by the Bureau or any of its employees.
- Ask the Enforcement intern coordinator(s) to confirm with the supervising ALD that he or she is comfortable with the memo being used as a writing sample.

For More Information:

Mailing Address:
Consumer Financial Protection Bureau
PO Box 4503
Iowa City, IA 52244

Phone:
(855) 411-CFPB | (855) 411-2372
TTY/TDD: (855) 729-CFPB | (855) 729-2372

8 a.m. to 8 p.m. ET, Monday through Friday