Privacy and Civil Liberties Impact Assessment for the Office of Financial Research (OFR) Use of Board of Governors of the Federal Reserve System's Comprehensive Capital Analysis and Review (CCAR) Data

September 28, 2016

Reviewing Official
Ryan Law
Acting Deputy Assistant Secretary for Privacy, Transparency, and Records
Department of the Treasury

Bureau/Office Certifying Official
Wesley Fravel
Senior Information Technology Specialist - Privacy
Office of Financial Research
Bureau Privacy and Civil Liberties Officer

Section 1.0: Introduction

It is the policy of the Department of the Treasury (hereinafter "Treasury" or "Department") and its Bureaus to conduct a Privacy and Civil Liberties Impact Assessment (hereinafter "PCLIA") when Personally Identifiable Information (hereinafter "PII") is maintained in a system or by a project. PCLIAs are required for all systems and projects that collect, maintain, or disseminate PII, regardless of the manner in which the information is retrieved.

This assessment is being completed pursuant to Section 208 of the E-Government Act of 2002 (hereinafter "E-Gov Act"), 44 U.S.C. § 3501, Office of the Management and Budget (hereinafter "OMB") Memorandum 03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," and Treasury Directive 25-07, "Privacy and Civil Liberties Impact Assessment (PCLIA)," which requires Treasury Offices and Bureaus to conduct a PCLIA before:

1. developing or procuring information technology (hereinafter "IT") systems or projects that collect, maintain or disseminate PII from or about members of the public, or

2. initiating, a new collection of information that: a) will be collected, maintained, or disseminated using IT; and b) includes any PII permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons. Agencies, instrumentalities or employees of the federal government are not included.

This PCLIA provides the following information regarding the system or project:
(1) an overview of its purpose and functions;
(2) a description of the information collected;
(3) a description of the how information is maintained, used and shared;
(4) an assessment of whether the system or project is in compliance with federal requirements that support information privacy; and
(5) an overview of the redress/complaint procedures available to individuals who may be affected by the use or sharing of information by the system or project.

This PCLIA is for the OFR's Analytical Environment (OFRAE). The OFRAE was previously documented in the Privacy Impact Assessment (PIA), Office of Financial Research Analytical Environment Privacy Impact Assessment, published in October 2014. OFR is conducting this revised PCLIA to evaluate new privacy implications associated with introducing additional IT capabilities to the OFRAE.

Section 2.0: Definitions

Agency – means any entity that falls within the definition of the term "executive agency", as defined in section 102 of title 31, United States Code, or "agency", as defined in section 3502 of title 44, United States Code.

Certifying Official – The Bureau Privacy and Civil Liberties Officer(s) who certify that all requirements in TD and TD P 25-07 have been completed so a PCLIA can be reviewed and approved by the Treasury Deputy Assistant Secretary for Privacy, Transparency and Records.

Collect (including "collection") – means the retrieval, receipt, gathering or acquisition of any PII and its storage or presence in a Treasury system. This term should be given its broadest possible meaning.

Contractors and service providers – include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications.

Data mining – The term "data mining" means a program involving pattern-based queries, searches, or other analyses of 1 or more electronic databases, where-- (A) a department or agency of the Federal Government, or a non-Federal entity acting on behalf of the Federal Government, is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals; (B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and (C) the purpose of the queries, searches, or other analyses is not solely-- (i) the detection of fraud, waste, or abuse in a Government agency or program; or (ii) the security of a Government computer system.

Disclosure – When it is clear from its usage that the term "disclosure" refers to records provided to the public in response to a request under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act, its application should be limited in that manner. Otherwise, the term should be interpreted as synonymous with the terms "sharing" and "dissemination" as defined in this manual.

Dissemination – as used in this manual is synonymous with the terms "sharing" and "disclosure" (unless it is clear from the context that the use of the term "disclosure" refers to a FOIA/Privacy Act disclosure).

E-Government – the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery.

Federal information system – a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information owned or under the control of a federal agency, whether automated or manual.

Final rule – After the Notice of proposed rulemaking (NPRM) comment period closes, the agency reviews and analyzes the comments received (if any). The agency has the option-to proceed with the rulemaking as proposed, issue a new or modified proposal or withdraw the proposal before reaching its final decision. The agency can also make any revisions to the supporting analyses contained in the NPRM (e.g., to address a concern raised by a member of the public in response to the NPRM).

Government information – information created, collected, used, maintained, processed, disseminated, or disposed of by or for the Federal Government.

Individual – means a citizen of the United States or an alien lawfully admitted for permanent residence. If a question does not specifically inquire about or an issue does not clearly involve a Privacy Act system of records, the term should be given its common, everyday meaning. In certain contexts, the term individual may also include citizens of other countries who are covered by the terms of an international or other agreement that involves information stored in the system or used by the project.

Information – means any representation of knowledge such as facts, data, or opinions in any medium or form, regardless of its physical form or characteristics. This term should be given the broadest possible meaning. This term includes, but is not limit to, information contained in a Privacy Act system of records.

Information technology (IT) – any equipment or interconnected system or subsystem of equipment, used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use: (i) of that equipment; or (ii) of that equipment to a significant extent in the performance of a service or the furnishing of a product. It includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services), and related resources; but does not include any equipment acquired by a federal contractor incidental to a federal contract. Clinger-Cohen Act of 1996, 40 U.S.C. § 11101(6).

Major Information system – embraces "large" and "sensitive" information systems and means "a system or project that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources." OMB Circular A-130, Section 6.u. This definition includes all systems that contain PII and are rated as "MODERATE or HIGH impact" under Federal Information Processing Standard 199.

National Security systems – a telecommunications or information system operated by the federal government, the function, operation or use of which involves: (1) intelligence activities, (2) cryptologic activities related to national security, (3) command and control of military forces, (4) equipment that is an integral part of a weapon or weapons systems, or (5) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management. Clinger-Cohen Act of 1996, 40 U.S.C. § 11103.

Notice of proposed rulemaking (NPRM) – the Privacy Act (Section (J) and (k)) allow agencies to use the rulemaking process to exempt particular systems of records from some of the requirements in the Act. This process is often, referred to as "notice-and-comment rulemaking." The agency publishes an NPRM to notify the public that the agency is proposing a rule and provides an opportunity for the public to comment on the proposal before the agency can issue a Final rule.

Personally Identifiable Information (PII) – "means, any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying

information that is linked or linkable to a specific individual. The definition of this term also incorporates by reference the definition of PII in OMB Memorandum 06-19[1] and the definition of term "Information in Identifiable Form" as defined in § 208(d)[2] of the E-Government Act of 2002, Pub. L.107-347, 116 Stat. 2899 and as further defined in OMB M 03-22.[3]

Privacy and Civil Liberties Impact Assessment (PCLIA) – a PCLIA is:

(1) a *process* conducted to: (a) identify privacy and civil liberties risks in systems, programs and other activities that maintain PII; (b) ensure that information systems**,** programs and other activities comply with legal, regulatory, and policy requirements; (c) analyze the privacy and civil liberties risks identified; (d) identify remedies, protections and alternative or additional privacy controls necessary to mitigate those risks; and (e) provide notice to the public of privacy and civil liberties protection practices.
(2) a *document* that catalogues the outcome of that privacy and civil liberties risk assessment process.

Protected Information – as the term is used in this PCLIA, has the same definition given to that term in TD 25-10, Section 4.

Privacy Act Record – any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, the individual's education, financial transactions, medical history, and criminal or employment history and that contains the individual's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Reviewing Official – The Deputy Assistant Secretary, Privacy, Transparency and Records who reviews and approves all PCLIAs as part of their duties as a direct report to the Treasury Senior Agency Official for Privacy.

---

1 "Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

2 "Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means."

3 "Information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors.)"

Routine Use – with respect to the disclosure of a record outside of the Department of the Treasury (i.e., external sharing), the use of such record for a purpose which is compatible with the purpose for which it was collected.

Sharing – any Treasury initiated distribution of information to government employees or agency contractors or grantees, including intra- or inter-agency transfers or exchanges of Treasury information regardless of whether it is covered by the Privacy Act. It does not include responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act. It is synonymous with the term "dissemination" as used in this assessment. It is also synonymous with the term "disclosure" as used in this assessment unless it is clear from the context in which the term is used that it refers to disclosure to the public in response to a request for agency records under the Freedom of Information Act (5 U.S.C. 552) or the Privacy Act.

System – as the term used in this manual, includes both federal information systems and information technology.

System of Records – a group of any records (as defined in the Privacy Act) under the control of Treasury from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

System of Records Notice – Each agency that maintains a system of records shall publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include: (A) the name and location of the system; (B) the categories of individuals on whom records are maintained in the system; (C) the categories of records maintained in the system; (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use; (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records; (F) the title and business address of the agency official who is responsible for the system of records; (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him; (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and (I) the categories of sources of records in the system.

System Owner – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Section 3.0: System Overview

In achieving its mission of improving the quality, transparency, and accessibility of financial data and information, the OFR regularly engages in information sharing requests with other Federal agencies. Acquired data are processed by applications and databases within the OFR Analytical Environment, or OFRAE. In general, these data are used for trend analysis in the aggregate, including identifying macro-level risks and trends in financial markets.

OFR previously addressed its OFRAE and certain datasets stored on it that include personally identifiable information (PII) in the Privacy and Civil Liberties Impact Assessment (PCLIA) for that system. As discussed in that PCLIA, in cases where OFR identifies unique privacy considerations

associated with a particular dataset, it will conduct a separate PCLIA specific to that dataset. You can read more about the OFRAE here.

One such dataset that OFR has identified as critical to fulfilling its research mission is The Board of Governors of the Federal Reserve System's (the "Board") Capital Assessment and Stress Testing Information (Forms FR Y-14) used in the Comprehensive Capital Analysis and Review (CCAR), or what is more commonly known as the stress testing and capital planning process. For the purposes of this document, the data are collectively referred to as "CCAR data". These data are submitted by institutions to the Board per regulation, and will be used by OFR to carry out its statutory mandate to evaluate stress tests and other initiatives outlined in OFR's stress testing program.

OFR has requested the CCAR data from the Board pursuant to Sections 153 and 154 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Act) in order to create work product related to financial stability including conducting financial research and analyses, and preparing reports, memoranda, working papers, agent based modeling and interdependency modeling.

Information included in the CCAR data includes both aggregate and loan level information about regulated institutions' capital position. The loan level data, submitted via Form FR Y-14M through one of four schedules (A, B, C, D), includes:

Schedule A: Domestic First Lien Closed-end 1-4 Family Residential Loan Data; Schedule B: Domestic Home Equity Loan and Home Equity Line Data; Schedule C: Address Matching Loan Level Data:

- Loan number (or a reference number used in lieu of the loan number given it meets the requirements outlined by the Board)
- Date the loan originally closed (loan closing date);
- First payment date;
- Property (to which the loan applies) street address, including city, state, and five digit ZIP code);
- Property census tract (2010)
- Original loan amount;
- Original property value (at time of loan origination) rounded to the nearest whole number;
- Original loan to value (LTV) ratio (amount of loan divided by value of the property);
- Debt to income ratios (DTI) of borrower used to determine how much the borrower qualifies for, and at time of loan origination
- Borrower credit score at time of origination and at time of reporting;
- Occupancy status of mortgaged property (e.g. primary residence, second home, investment, etc.);
- Credit class assigned by the lender at time of origination;
- Loan type (e.g. FHA, VA, Conventional, etc.)
- Lien position (at origination) (e.g. first, second, etc.)
- Product (loan/mortgage) type (e.g. fixed 30, fixed 15, ARM 10, etc.);
- Loan purpose (e.g. purchase; refinance; home improvement, etc.);
- Mortgage insurance coverage percent (for loans with mortgage coverage insurance);
- Property type (e.g. condo, townhouse, single family, etc.);

- Whether the loan has a “balloon payment” and the number of months between the loan closing date and the due date for the balloon payment;
- Whether the loan is a “buy down”;
- Whether the loan is “interest only”;
- Whether additional recourse (beyond possession of the property) is available to the loan owner in the event of default;
- Information about the loan’s interest rate, including the initial rate, the initial rate period, the periodic interest rate reset period, the rate caps and floors, etc.;
- Information about the loan’s original terms, including total months, interest rate, interest type (fixed or variable), and scheduled principle and interest;
- Whether the loan has a pre-payment penalty and, if so, the terms;
- Borrower bankruptcy history, including “chapter” or type (e.g. chapter 9, chapter 11, etc.) ;
- Current loan information, including interest rate, remaining term (in months), next payment date, outstanding loan balance (principal), and current payment (principal and interest amount);
- Information relating to whether the loan has been modified or extended (including the terms of such modifications or extensions), is in default or foreclosure, or subject to the servicer’s loss mitigation procedures;
- Payment delinquency history for the loan (90 days past due in the previous 12 months);
- Borrower’s mailing address.

Schedule D: Domestic Credit Card Data Collection:

- Reference number used in lieu of the actual account number for the credit card;
- Customer ID for cardholders with multiple accounts;
- State of the billing address of the cardholder;
- Five digit ZIP code of the billing address of the cardholder;
- Credit card type (e.g. general purpose; private label; business card; corporate card);
- Product type (e.g. gas card, co-branded for retail or services, student, etc.);
- Lending type (e.g. consumer bank card, consumer charge card, etc.);
- Whether the account is revolving;
- “Network ID” (e.g. Visa, MasterCard, American Express, etc.);
- Whether the card is secured by collateral;
- “Loan Channel” or, the method of solicitation used to acquire the account;
- Whether an outstanding balance exists on the card and the total of that balance;
- Any portion of the balance, or amount subject to rates below or above the accounts normal purchase APR (e.g. promotional rate, cash advance rate, penalty pricing, etc.);
- Average daily balance;
- Rewards associated with the account, including types and the total rewards cash for the account;
- Account cycle end date;
- Whether the cardholder has other non-credit card banking relationships with the reporting bank and the nature of those relationships (e.g. deposit, mortgage, auto, student loans, etc.);
- Whether multiple cards are associated with the account, the total number of authorized users, or if the account is a joint account;

- Cardholder's income at origination and as updated (current) and income source (e.g. individual, household, other);
- Credit score of cardholder at origination and as updated (refreshed), including date of most recent score;
- Original and current credit limit;
- Payment information, including minimum due, total due, next payment due date, and actual payment amount(s);
- Delinquency information including total past due, days past due, and whether the account has ever been more than 60 days past due in the previous three years, charge off(s), amounts, and reasons;
- Fees and costs information including interest type (i.e. fixed or variable), purchase APR, finance charges, fee types (e.g. annual, monthly, etc.) and amounts;
- Account status (i.e. open, closed, active, inactive);
- Total amounts charged in the reporting period, including purchase amount, cash advance amount, balance transfer amount, and convenience check amount;
- Bankruptcy history of the cardholder;
- Probability of default for the account;
- Whether the cardholder is enrolled in any special repayment, restructuring, or workout programs or receiving any benefits under a debt suspension or cancellation program, or if the account is currently frozen or was closed due to potential fraud.

A complete list of the data points collected in the FR Y-14 schedules is available on the Board's website, www.federalreserve.gov.

While the CCAR data does not include directly identifiable PII associated with each loan, the mortgage information and the address matching schedule can be used in conjunction with each other to tie loan-level information with specific property addresses, and it is possible that the mortgage or credit card data may, when combined with other existing data sets, including publicly available information, be used to identify an individual borrower. As such, OFR considers these data to be PII as in accordance with Treasury policy and guidance from the Office of Management and Budget (OMB).

OFR is conducting this Privacy and Civil Liberties Impact Assessment to evaluate the general privacy impact(s) and risk(s) associated with the maintenance and use of these data for research purposes.

Number of Individuals Maintained in the System or Project		
☐ 0 – 999	☐ 1000 – 9,999	☐ 10,000 – 99,999
☐ 100,000 – 499,999	☐ 500,000 – 999,999	☒ 1,00,000+*

**Please note, this number is an estimate only. While OFR believes the number to be at or near 1,000,000 lines of mortgages and credit cards included in the data set, due to the nature of the data, it impossible to differentiate the number of "unique" records, as they have been stripped of direct-identifiers that would link them to a unique individual.*

Section 3.2: Purpose Specification

CCAR data provided to OFR by the Board are used by OFR in support of its research mission. Generally, such data will be used to identify macro-level risks and trends in financial markets. Data

may be used in developing OFR work product, in accordance with the provisions of the information sharing agreement between OFR and the Board for use of the CCAR data.

Section 3.3: Authority to Collect

The statutory authority for operating this system or performing this project is:

Statute	Description
Dodd-Frank Wall Street Reform Act and Consumer Protection Act (Pub.L. 111–203, H.R. 4173), Section 153.	Establishes the OFR, outlines its mission, and authorizes the OFR Director to manage administrative functions of the office. Specifically, subsection 154 (b) "Data Center" provides that the Data Center, on behalf of the Council, shall collect, validate, and maintain all data necessary to carry out the duties of the Data Center, as described in this part. The data assembled shall be obtained from member agencies, commercial data providers, publicly available data sources, and financial entities under subparagraph (B).

Section 4.0: Information Collection

Section 4.1: Relevant and Necessary

The Privacy Act requires "each agency that maintains a system of records [to] maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be fulfilled by statute or by executive order of the President." See 5 U.S.C. § 552a(e)(1).

The Privacy Act allows federal agencies to exempt records from the relevant and necessary requirement if certain conditions are met. This includes issuing a Notice of Proposed Rulemaking (hereinafter "NPRM") to solicit public opinions on the proposed exemption and issuing a Final rule after addressing any concerns raised by the public in response to the NPRM. It is possible for some, but not all, of the records maintained in the system or by the project to be exempted from the Privacy Act through the NPRM/Final rule process.

Section 4.1(a) Please check all of the following that are true:

1. ☒ None of the PII maintained in the system or by the project is part of a Privacy Act system of records;
2. ☐ All of the PII maintained in the system or by the project is part of a system of records and none of it is exempt from the Privacy Act relevant and necessary requirement;
3. ☐ All of the PII maintained in the system or by the project is part of a system of records and all of it is exempt from the Privacy Act relevant and necessary requirement;

4. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and the records to which the Privacy Act applies are exempt from the relevant and necessary requirement; and 5. ☐ Some, but not all, of the PII maintained in the system or by the project is part of a system of records and none of the records to which the Privacy Act applies are exempt from the relevant and necessary requirement.
Section 4.1(b) ☐ Yes ☐ No ☒ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, was an assessment conducted prior to collection (e.g., during Paperwork Reduction Act analysis) to determine which PII types (see Section 4.2 below) were relevant and necessary to meet the system's or project's mission requirements?
Section 4.1(c) ☐ Yes ☐ No ☒ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is the PII limited to only that which is relevant and necessary to meet the system's or project's mission requirements?
Section 4.1(d) ☐ Yes ☐ No ☒ N/A With respect to PII maintained in the system or by the project that is subject to the Privacy Act's relevant and necessary requirement, is there a process to continuously reevaluate and ensure that the PII remains relevant and necessary?
Explanation for Answers in Sections 4.1(a) thru 4.1(d): Information included in the CCAR dataset is not retrieved by personal identifier and is therefore not subject to the requirements of the Privacy Act. Further, PII included in the dataset was originally collected by the Board in accordance with rules, procedures, and processes specific to the Board, including an assessment to determine which PII types are relevant and necessary.

Section 4.2: PII and/or information types or groupings

To perform their various missions, federal agencies must necessarily collect various types of information. The checked boxes below represent the types of information maintained in the system or by the project. Information identified below is used by the system or project to fulfill the purpose stated in Section 3.3 – Authority to Collect.

Biographical/General Information Regarding Individuals		
☐ Name	☐ Gender	☐ Group/Organization Membership
☐ Birth Date	☐ Race/Ethnicity	☐ Military Service Information
☒ Home Physical Mailing Address	☐ Citizenship	☒ Marital Status
☐ Personal Cell Number	☐ Nationality	☐ Mother's Maiden Name
☐ Personal Home Phone or Fax Number	☐ Country of Birth	☐ Spouse Information
☐ Personal e-mail address	☐ City or County of Birth	☐ Children Information
☐ Alias (including nickname)	☐ Immigration Status	☐ Information about other relatives.

☐ Education Information	☐ Religion/Religious Preference	☐ References or other information about an individual's friends, associates or acquaintances.
☒ Personal Financial Information (including loan information)* ** Such information includes loan and credit card information which does not include direct identifiers and is aggregated and used for trend analysis to identify macro-level risks and trends in financial markets. See Section 3, System Overview for a discussion of these data points.*	☐ Passport Information	☐ Global Positioning System (GPS)/Location Data
☐ Sexual Orientation	☐ User names, avatars etc.	☐ Secure Digital (SD) Card or Other Data stored on a card or other technology
☐ Cell tower records (e.g., logs. user location, time etc.)	☐ Contact lists and directories	☐ Other (please describe):
☐ Network communications data	☐ Device settings or preferences (e.g., security level, sharing options, ringtones).	☐ Other (please describe):
☐ Other (please describe):	☐ Other (please describe):	

Identifying Numbers Assigned to Individuals	
☐ Full Social Security number	☐ Personal Bank Account Number
☐ Truncated Social Security Number (e.g., last 4 digits)	☐ Health Plan Beneficiary Number
☐ Employee Identification Number	☐ Credit Card Number
☐ Taxpayer Identification Number	☐ Patient ID Number
☐ File/Case ID Number	☐ Vehicle Identification Number
☐ Alien Registration Number	☐ Driver's License Number
☐ Personal device identifiers or serial numbers	☐ License Plate Number
☐ Internet Protocol (IP) Address (where known to belong to an individual or unknown whether the IP address belongs to an individual or organization)	☐ Professional License Number
☐ Other (please describe):_____	

Medical/Emergency Information Regarding Individuals

☐ Medical/Health Information	☐ Worker's Compensation Act Information	☐ Patient ID Number
☐ Mental Health Information	☐ Disability Information	☐ Emergency Contact Information (e.g., a third party to contact in case of emergency)
☐ Other (please describe): _____		

Biometrics/Distinguishing Features/Characteristics of Individuals		
☐ Physical description/ characteristics (e.g., hair, eye color, weight, height, sex, gender etc.)	☐ Signatures	☐ Vascular scans
☐ Fingerprints	☐ Photos	☐ Retina/Iris Scans
☐ Palm prints	☐ Video	☐ Dental Profile
☐ Voice audio recording	☐ Scars, marks, tattoos	☐ DNA Sample or Profile
☐ Other (please describe): _____	☐ Other (please describe): _____	☐ Other (please describe): _____

Specific Information/File Types That Include Information Regarding Individuals		
☐ Taxpayer Information/Tax Return Information	☐ Law Enforcement Information	☐ Security Clearance Information
☐ Civil/Criminal History Information/Police Records	☐ National Security/Classified Information	☐ Bank Secrecy Act Information
☐ Protected Information (as defined in Treasury Directive 25-10)	☐ Case files	☐ Personnel Files
☐ Information provided under a confidentiality agreement	☐ Information subject to the terms of an international or other agreement	☐ Other (please describe): _____

Audit Log and Security Monitoring Information		
☐ User ID assigned to a user of Treasury IT	☐ Date and time an individual accesses a facility, system, or other IT	☐ Files accessed by a user of Treasury IT
☐ Passwords generated by a user of Treasury IT	☐ Internet or other queries run by a user of Treasury IT	☐ Contents of files accessed by a user of Treasury IT
☐ Video of individuals derived from security cameras	☐ Biometric information used to access Treasury facilities or IT	☐ Public Key Information.

☐ Information revealing an individual's presence in a particular location as derived from security token/key fob, employee identification card scanners or other IT or devices	☐ Still photos of individuals derived from security cameras.	☐ Other (please describe): _____

Other	
☐ Other (please describe): ____	☐ Other (please describe): _____
☐ Other (please describe): _____	☐ Other (please describe): _____

Section 4.3: Sources of information and the method and manner of collection

Information is provided by the Board per an agreement between the Board and the OFR. CCAR data is submitted by institutions to the Board per regulation, on a quarterly basis, using the procedures and reporting forms created and maintained by the Board.

CCAR Data Received by OFR from the Board	**N/A**	**N/A**	**N/A**
Specific PII identified in Section 4.2 that was acquired from this source: Personal financial information, including loan and credit card information which does not include direct identifiers and is used for trend analysis to identify macro-level risks and trends in financial markets, as outlined in Section 3 of this PCLIA.	**Specific PII identified in Section 4.2 that was acquired from this source:**	**Specific PII identified in Section 4.2 that was acquired from this source:**	**Specific PII identified in Section 4.2 that was acquired from this source:**
Manner in which information is acquired from source by the Treasury project/system: (select all that apply):	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**	**Manner in which information is acquired from source by the Treasury project/system: (select all that apply):**
☐ From a paper or electronic form	☐ From a paper or electronic form	☐ From a paper or electronic form	☐ From a paper or electronic form

provided to individuals, the public or members of a particular group Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	provided to individuals, the public or members of a particular group Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	provided to individuals, the public or members of a particular group Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____	provided to individuals, the public or members of a particular group Please identify the form name (or description) and/or number (e.g., OMB Control Number): _____
☐ Received in paper format other than a form.	☐ Received in paper format other than a form.	☐ Received in paper format other than a form.	☐ Received in paper format other than a form.
☐ Delivered to the project on disk or other portable device and uploaded to the system.	☐ Delivered to the project on disk or other portable device and uploaded to the system.	☐ Delivered to the project on disk or other portable device and uploaded to the system.	☐ Delivered to the project on disk or other portable device and uploaded to the system.
☐ Accessed and downloaded or otherwise acquired via the internet	☐ Accessed and downloaded or otherwise acquired via the internet	☐ Accessed and downloaded or otherwise acquired via the internet	☐ Accessed and downloaded or otherwise acquired via the internet
☐ Email	☒ Email	☐ Email	☐ Email
☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.	☐ Scanned documents uploaded to the system.
☒ Bulk transfer	☐ Bulk transfer	☐ Bulk transfer	☐ Bulk transfer
☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).	☐ Extracted from particular technology (e.g., radio frequency identification data (RFID) devices, video or photographic cameras, biometric collection devices).
☐ Fax	☐ Fax	☐ Fax	☐ Fax
☐ Extracted from notes of a phone interview or face to face contact	☐ Extracted from notes of a phone interview or face to face contact	☐ Extracted from notes of a phone interview or face to face contact	☐ Extracted from notes of a phone interview or face to face contact

☐ Other: Please describe:	☐ Other: Please describe: _____	☐ Other: Please describe:	☐ Other: Please describe: _____
☐ Other: Please describe: _____	☐ Other: Please describe: _____	☐ Other: Please describe: _____	☐ Other: Please describe: _____

Section 4.4: Privacy and/or civil liberties risks related to collection

Notice of Authority, Principal Uses, Routine Uses and Effect of not Providing Information

When federal agencies use a form to obtain information from an individual that will be maintained in a system of records, they must inform the individual of the following: "(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information." See 5 U.S.C § 522a.(e)(3).

Section 4.4(a) ☐ Yes ☒ No Is any of the PII maintained in the system or by the project collected directly from an individual?

Section 4.4(b) ☐ Yes ☐ No ☒ N/A Was the information collected from the individual using a form (paper or electronic)?

Section 4.4(c) ☒ N/A Was the individual notified (on the form in which the PII was collected or on a separate form that can be retained by the individual) about the following at the point where the information was collected (e.g., in a form or on a website).

☐ The authority (whether granted by statute, or by Executive order of the President) which authorizes the solicitation of the information.
☐ Whether disclosure of such information is mandatory or voluntary.
☐ The principal purpose or purposes for which the information is intended to be used.
☐ The individuals or organizations outside of Treasury with whom the information may be/ will be shared.
☐ The effects on the individual, if any, if they decide not to provide all or any part of the requested information.

Explanation for Answers in Sections 4.4(a) thru 4.4(c): Information included in the CCAR data is collected by the Board from regulated institutions in accordance with rules, procedures, and processes specific to the Board.

Use of Social Security Numbers

Social Security numbers (hereinafter "SSN") are commonly used by identity thieves to commit fraudulent acts against individuals. Therefore, as a matter of policy, federal agencies are required to eliminate the use of SSNs (subject to certain exceptions).

In addition, the Privacy Act, as amended, provides that: "It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number." Pub. L. No. 93–579, § 7. This provision does not apply to: (1) any disclosure required by federal statute; or (2) any disclosure of an SSN to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. See Pub. L. 93–579, § 7(a)(2)(A)-(B).

Section 4.4(d) ☐ Yes ☒ No ☐ N/A Does the system or project maintain SSNs?

Section 4.4(e) ☐ Yes ☐ No ☒ N/A Were steps taken to explore alternatives to the use of SSNs as a personal identifier in the system or project and were any resulting actions taken to eliminate unnecessary uses?

Section 4.4(f) ☐ Yes ☐ No ☒ N/A Will individuals be denied any right, benefit, or privilege provided by law because of such individual's refusal to disclose their SSN?

☐ SSN disclosure is required by Federal statute;
☐ the SSN is disclosed to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, and disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual; or
☐ when the information is collected, individuals are given notice whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

Explanation for Answers in Sections 4.4(d) thru 4.4(f): The CCAR data does not include SSNs.

First Amendment Activities

The Privacy Act requires that federal agencies "maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." See 5 U.S.C. § 552a.(e)(7).

Section 4.4(g) ☐ Yes ☒ No Does the system or project maintain any information describing how any individual exercises their rights guaranteed by the First Amendment?

☐ The individual about whom the information was collected or maintained expressly authorizes its collection/maintenance.

☐ The information maintained is pertinent to and within the scope of an authorized law enforcement activity. ☐ There is a statute that expressly authorizes its collection.
Explanation for the Answer to Section 4.4(g): The CCAR data does not contain any information describing how any individual exercises their rights guaranteed by the First Amendment.

Section 5.0: Maintenance, use and sharing of the information

The following sections require a clear description of the system's or project's use(s) of information.

Section 5.1: Describe how and why the system or project uses the information it collects and maintains

Please describe all of the uses of the information types and groupings collected and maintained by the system or project (see Section 4.2), including a discussion of why the information is used for this purpose and how it relates to the mission of the bureau or office that owns the system.

The CCAR data provided by the Board to OFR is used by OFR to carry out its statutory mandate to evaluate stress tests and other initiatives outlined in OFR's stress testing program. Personal financial information, including loan information, included in the CCAR data does not include direct-identifiers and is used for trend analysis to identify macro-level risks and trends in financial markets in accordance with OFR's research-based mission.

Collecting Information Directly from the Individual When Using it to Make Adverse Determinations About Them

The Privacy Act requires that federal agencies "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." See 5 U.S.C. § 552a.(e)(2).

Section 5.1(a) ☐ Yes ☒ No Is it possible that the information maintained in the system or by the project may be used by Treasury to make an adverse determination about an individual's rights, benefits, and privileges under Federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)? **Section 5.1(b)** ☐ Yes ☒ No Is it possible that Treasury will share information maintained in the system or by the project with a third party external to the Department that will use the information to make an adverse determination about an individual's rights, benefits, and privileges under Federal programs? **Section 5.1(c)** ☐ Yes ☐ No ☒ N/A If information could potentially be used to make an adverse determination about an individual's rights, benefits, and privileges under Federal

programs, does the system or project collect information (to the greatest extent practicable) directly from the individual?
Explanation of the Answer to Section(s) 5.1(a) through 5.1(c): Information included in the CCAR data is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Data Mining

As required by Section 804 of the Implementing the 9/11 Commission Recommendations Act of 2007 (hereinafter "9-11 Commission Act"), Treasury reports annually to Congress on its data mining activities. For a comprehensive overview of Treasury's data mining activities, please review the Department's Annual Privacy reports available at: http://www.treasury.gov/privacy/annual-reports.

Section 5.1(d) ☐ Yes ☒ No Is information maintained in the system or by the project used to conduct "data-mining" activities as that term is defined in the Implementing the 9-11 Commission Act?
Explanation of the Answer to Section 5.1(d): Information contained in the CCAR data is not used to conduct "data-mining" activities as that term is defined in the Implementing the 9/11 Commission Act.

Section 5.2: Ensuring accuracy, completeness, and timeliness of information collected, maintained, and shared

Exemption from Accuracy, Relevance, Timeliness, and Completeness Requirements

The Privacy Act requires that federal agencies: "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." See 5 U.S.C § 552a.(e)(5). If a particular system of records meets certain requirements (including the NPRM process discussed above), an agency may exempt the system of records (or a portion of the records) from this requirement.

Section 5.2(a) ☐ Yes ☒ No Is all or any portion of the information maintained in the system or by the project (a) part of a system of records and (b) exempt from the accuracy, relevance, timeliness, and completeness requirements in sections (e)(5) of the Privacy Act?
Explanation of the Answer to Section 5.2(a): Information included in the CCAR data is not retrieved by personal identifier and is therefore not subject to the requirements of the Privacy Act.

Computer Matching

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act for the purpose of imposing additional requirements when Privacy Act systems of records are used in computer matching programs.

Pursuant to the Privacy Act, as amended, there are two distinct types of matching programs. The first type of matching program involves the computerized comparison of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records. This type of matching program may be conducted for any purpose. The second type of matching program involves the computerized comparison of two or more automated systems of records or a system of records with non-federal records. The purpose of this type of matching program must be for the purpose of eligibility determinations or compliance requirements for applicants, recipients, beneficiaries, participants, or providers of services for payments or in-kind assistance under federal benefit programs, or recouping payments or delinquent debts under such federal benefit programs. See 5 U.S.C. § 522a.(a)(8).

Matching programs must be conducted pursuant to a matching agreement between the source and recipient agencies. The matching agreement describes the purpose and procedures of the matching and establishes protections for matching records.

Section 5.2(b) ☐ Yes ☒ No Is any of the information maintained in the system or by the project (a) part of a system of records and (b) used as part of a matching program?

Section 5.2(c) ☐ Yes ☐ No ☒ N/A Is there a matching agreement in place that contains the information required by Section (o) of the Privacy Act?

Section 5.2(d) ☐ Yes ☐ No ☒ N/A Are assessments made regarding the accuracy of the records that will be used in the matching program? See 5 U.S.C § 552a.(o)(J).

Section 5.2(e) ☐ Yes ☐ No ☒ N/A Does the bureau or office that owns the system or project independently verify the information, provide the individual notice and an opportunity to contest the findings, or obtain Data Integrity Board approval in accordance with Section (p) of the Privacy Act before taking adverse action against the individual?

Explanation of Answers to Sections 5.2(b) through 5.2(e): Information included in the CCAR data is not subject to or part of a matching program.

Ensuring Fairness in Making Adverse Determinations About Individuals

Federal agencies are required to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination." See 5 U.S.C. § 552a(e)(5). This requirement also applies when merging records from two or more sources where the merged records are used by the agency to make any determination about any individual.

Section 5.2(f) ☐ Yes ☐ No ☒ N/A With respect to the information maintained in the system or by the project, are steps taken to ensure all information used to make a determination about an individual is maintained with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination?

Explanation of the Answer to Section 5.2(f): Information included in the CCAR data is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Merging Information About Individuals
Section 5.2(g) ☒ Yes ☐ No Is information maintained in the system or by the project merged with electronic or non-electronic information from internal or external sources (e.g., other files or systems)? **Section 5.2(h)** ☐ Yes ☒ No ☐ N/A Once merged, is the information used in making determinations about individuals (e.g., decisions about whether the individual will receive a financial benefit or payment, get a clearance or access to a Treasury facility, obtain employment with Treasury, etc.)? **Section 5.2(i)** ☐ Yes ☐ No ☒ N/A Are there documented policies or procedures for how information is merged? **Section 5.2(j)** ☐ Yes ☐ No ☒ N/A Do the documented policies or procedures address how to proceed when not all of the information being merged matches a particular individual (i.e., partial matches)? **Section 5.2(k)** ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make a determination about an individual, are steps taken to ensure the accuracy, relevance, timeliness, and completeness of the information as is reasonably necessary to assure fairness to the individual?
Explanation of Answers to Sections 5.2(g) through 5.2(k): Information included in the CCAR data may be merged with other existing OFR datasets to form aggregate datasets for research purposes. While these datasets may contain PII, they do not include direct-identifiers and are primarily used for trend analysis in the aggregate. Research is done across the datasets to identify macro-level risks and trends in financial markets, not to identify or make determinations about individuals. Further, per the agreement between OFR and the Board for use of the CCAR data, OFR employees are prohibited from any efforts to combine the CCAR data with other data in order to identify unique individuals.

Policies and Standard Operating Procedures or Technical Solutions Designed to Ensure Information Accuracy, Completeness, and Timeliness
Section 5.2(l) ☐ Yes ☐ No ☒ N/A If information maintained in the system or by the project is used to make any determination about an individual (regardless of whether it is an exempt system of records), are there documented policies or standard operating procedures for the system or project that address the accuracy, completeness, and timeliness of the information? **Section 5.2(m)** ☐ Yes ☒ No Does the system or project use any software or other technical solutions designed to improve the accuracy, completeness, and timeliness of the information

used to make an adverse determination about an individual's rights, benefits, and/or privileges (regardless of if it is an exempt system of records)?

Explanation of the Answer to Sections 5.2(l) and 5.2(m): Information included in the CCAR data is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs. Processes and procedures governing data, including PII are described below in Section 5.2(n).

Accuracy, Completeness, and Timeliness of Information Received from the Source

Section 5.2(n) ☒ Yes ☐ No Did the bureau or office receive any guarantee, assurance, or other information from any information source(s) regarding the accuracy, relevance, timeliness and completeness of the information maintained in the system or by the project?

Explanation of the Answer to Sections 5.2(n): Prior to obtaining a dataset, data standards are established which specify the format in which the OFR expects to receive the data that it has procured or acquired. Extract, transform, and load (ETL) processes are developed such that accuracy and completeness are validated during the ETL process to verify that data has been received according to procurement and data management specifications. ETL processes are performed when data is received from a third party to extract the data needed for financial research purposes, transform the data in the required format for loading into OFR systems, and loading the standardized format into OFR systems for further analysis. ETL processes are developed such that if data is received in an unexpected format or with unexpected data included, the ETL process will fail and coordination with the vendor will be required to move forward with the data intake process.

In the case of information included in the CCAR data, this information is collected directly by the Board from regulated entities in accordance with the policies and procedures governing data collection by the Board. As such, the data is considered accurate, relevant, and timely as it relates to the information's purpose in facilitating OFR's research mission.

As outlined above, information included in the CCAR data is used to identify macro-level risks and trends in financial markets, not to identify or make determinations about individuals, thus, the question of accuracy, timeliness and relevance as it relates to a particular individual do not pose a risk.

Disseminating Notice of Corrections or Amendments to PII

Section 5.2(o) ☐ Yes ☐ No ☒ N/A Where feasible and appropriate, is there a process in place for disseminating corrections of or amendments to the PII maintained in the system or by the project to all internal and external information-sharing partners?

Section 5.2(p) ☐Yes ☐ No ☒ N/A Where feasible and appropriate, does the process for disseminating corrections or amendments include notifying the individual whose information is corrected or amended?

Explanation of the Answer to Sections 5.2(o) and 5.2(p): Because it is not retrieved by personal identifier, information included in the CCAR data is not subject to the requirements of the Privacy Act. Further, per the agreement between the Board and OFR, OFR is prohibited from disseminating or sharing CCAR data. PII included in the CCAR data is not collected directly from individuals, but by the Board from regulated entities in accordance with the procedures and policies governing the Board's collection of such information. Any updates, amendments, or other changes to information included in the CCAR data would be the responsibility of the Board.

Section 5.3: Information sharing within the Department of the Treasury

Internal Information Sharing
Section 5.3(a) ☒ Yes ☐ No Is PII maintained in the system or by the project shared with other Treasury bureaus or offices? **Section 5.3(b)** ☒ Yes ☐ No Does the Treasury bureau or office that receives the PII limit access to those Treasury officers and employees who have a need for the PII in the performance of their official duties (i.e., those who have a "need to know")?
Explanation of the Answer to Sections 5.3(a): Per the agreement between the Board and OFR for the use of the CCAR data, OFR is prohibited from sharing information included in the dataset except as provided in the Agreement. OFR will grant access to the dataset on a need-to-know basis, to: (i) OFR employees whose job duties include using the dataset to perform research; and (ii) Federal Stability Oversight Council staff on a need-to-know basis. OFR also has information security access procedures and policies in place for confidential information, including PII.

Memorandum of Understanding/Other Agreements Limiting Treasury's Internal Use/Disclosure of PII
Section 5.3(c) ☒ Yes ☐ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency that provided the information to the Treasury or subject to an international agreement or treaty) that limits or places conditions on Treasury's internal use, maintenance, handling or disclosure of the PII?

Internal Information Sharing Chart

Internal Recipient's Name (e.g., bureau or office)	OFR
Purpose of the Sharing	OFR and FSOC staff may request access to CCAR data for purposes consistent with OFR's and FSOC's research mission and statutory authority. Data access requests are reviewed and approved in accordance with OFR user access policies and guidelines. Data shared internally is based on specific, discrete user access requests and such

	access is based on a demonstrable need-to-know in support of a specific business function or request.
PII Shared	PII shared is limited to that which is necessary for a specific business purpose or request as described above in "Purpose of Sharing." Use of such information is governed by the agreement between the OFR and the Board for use of CCAR data.
Applicable Statutory or Regulatory or Restrictions on Information Shared	OFR has a statutory obligation under the Dodd-Frank Act (Act) to protect confidential data from unauthorized disclosure. In addition, the CCAR data is subject to the parameters and restrictions contained in data sharing agreement.
Applicable Restrictions Imposed by Agreement on Information Shared (e.g., by Treasury agreement with the party that provided the information to Treasury)	The agreement between the OFR and the Board for OFR's use of the CCAR data contains provisions related to the access, use and disclosure of the data and other information provided under the agreement. Additionally, specific provisions around PII include completing a Privacy and Civil Liberties Impact Assessment and restrictions around re-identification of individuals whose information is included in the dataset. A copy of the agreement is maintained on file by the OFR Chief Counsel.
Name and Description of MOU or Other Agreement Restricting Treasury's Internal Use, Maintenance, Handling or Sharing of PII Received	Request for Capital Assessments and Stress Testing Information Collection (CCAR data) dated May 27, 2016.
Method of PII Transfer (e.g., paper/ oral disclosures/ magnetic disk/portable device/email fax/other (please describe if other)	Data is transferred via secure electronic means per the OFR's data onboarding process.
Explanation for Responses in the Internal Information Sharing Chart: See above.	

Section 5.4: Information sharing with external (i.e., outside Treasury) organizations and individuals

External Information Sharing
Section 5.4(a) ☐ Yes ☒ No Is PII maintained in the system or by the project shared with agencies, organizations, or individuals external to Treasury?

Explanation of the Answer to Section 5.2(a): Information included in the CCAR data is not shared with agencies, organizations, or individuals external to the OFR or Treasury.

Accounting of Disclosures

Section 5.4(b) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you maintain a paper or electronic log or other record of the date, nature, and purpose of each disclosure (not including intra-agency disclosures and FOIA disclosures) of a record to any person or to another agency (outside of Treasury) and the name and address of the person or agency to whom the disclosure is made? See 5 U.S.C § 552a.(c).

Section 5.4(c) ☐ Yes ☐ No ☒ N/A If you do not keep a running tabulation of every disclosure at the time it is made, are you able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to Privacy Act requests in a timely fashion?

Section 5.4(d) ☐ Yes ☐ No ☒ N/A With respect to records maintained in the system or by the project that are subject to the Privacy Act, do you retain the log or other record of the date, nature, and purpose of each disclosure, for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made?

Section 5.4(e) ☐ Yes ☒ No With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to make the accounting available to the individual named in the record?

Section 5.4(f) ☐ Yes ☒ No With respect to records maintained in the system or by the project that are subject to the Privacy Act, does your bureau or office exempt the system of records (as allowed by the Privacy Act in certain circumstances) from the requirement to inform any person or other agency about any correction or notation of dispute made by the agency of any record that has been disclosed to the person or agency if an accounting of the disclosure was made?

Explanation of Answers to Sections 5.4(b) through 5.4(f): Because it is not retrieved by personal identifier, information included in the CCAR data is not subject to the requirements of the Privacy Act and is not shared with agencies, organizations, or individuals external to the OFR or Treasury.

Statutory or Regulatory Restrictions on Disclosure

Section 5.4(g) ☒ Yes ☐ No In addition to the Privacy Act, are there any other statutory or regulatory restrictions (e.g., 26 U.S.C § 6103 limits disclosure of tax returns and return information) on the sharing of any of the information or records maintained in the system or by the project?

Explanation of the Answer to Section 5.4(g): Federal statutes, including the Dodd-Frank Act, require the OFR to maintain and preserve the confidentiality of information received from third parties. Additionally, information included in the CCAR data is considered confidential supervisory information of the Board and may also in part be subject to the Trade Secrets Act which would prohibit disclosure.

Memorandum of Understanding Related to External Sharing
Section 5.4(h) ☐ Yes ☒ No ☐ N/A Does Treasury (including bureaus and offices) have an MOU, or any other type of agreement, with any external agencies, organizations, or individuals with which/whom it shares PII maintained in the system or by the project?
Explanation of the Answer to Section 5.4(h): Information included in the CCAR data, including PII, is not shared with agencies, organizations, or individuals external to the OFR or Treasury.

Memorandum of Understanding Limiting Treasury's Use or Disclosure of PII
Section 5.4(i) ☒ Yes ☐ No ☐ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement (e.g., agreement with another federal or state agency, an international agreement or treaty or contract with private vendor) that limits or places conditions on Treasury's internal use or external (i.e., outside Treasury) sharing of the PII?
Explanation of the Answer to Section 5.4(i): The CCAR data is subject to an MOU between the OFR and the Board. See Section 5.3(c) for more information.

Memorandum of Understanding Limiting External Party's Use or Disclosure of PII
Section 5.4(j) ☐ Yes ☐ No ☒ N/A Is any of the PII maintained in the system or by the project subject to the requirements of a Memorandum of Understanding or other agreement in which Treasury limits or places conditions on an external party's use, maintenance, handling or disclosure of PII shared by Treasury?
Explanation of the Answer to Section 5.4(j): Information included in the CCAR data is subject to the agreement in place between the OFR and the Board as described in Section 5.3(c). Pursuant to that agreement, OFR is prohibited from sharing information included in the CCAR data with agencies, organizations, or individuals external to the OFR or Treasury without the prior consent of the Board.

External Information Sharing Chart				
Section 5.4(k) ☒ N/A				
External Recipient's Name	N/A			
Purpose of the Sharing	N/A			
PII Shared	N/A			
Content of Applicable Routine Use/Citation to the SORN	N/A			
Applicable Statutory or Regulatory or	N/A			

Restrictions on Information Shared				
Name and Description of Relevant MOUs or Other Agreements Containing Sharing Restrictions Imposed on Treasury by an External Source or Providing/Originating Agency (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A			
Name and Description of Relevant MOUs or Other Agreements Containing Restrictions Imposed by Treasury on External Sharing Partner (including description of restrictions imposed on use, maintenance, and disclosure of PII)	N/A			
Method(s) Used to Transfer PII (e.g., paper/ oral disclosures/ magnetic disk/portable device/email fax/other (please describe if other)	N/A			

Obtaining Consent Prior to New Disclosures Not Included in the SORN
Section 5.4(l) ☐ Yes ☐ No ☒ N/A Is the individual's consent obtained, where feasible and appropriate, prior to any **new** disclosures of previously collected records in a system of records (those not expressly authorized by the Privacy Act or contained in the published SORN (e.g., in the routine uses))?
Explanation of the Answer to Section 5.4(l): As previously discussed, information included in the CCAR data is not subject to the requirements of the Privacy Act and is not shared with agencies, organizations, or individuals external to the OFR or Treasury.

Section 6.0: Legal compliance with Federal information management requirements

Responses to the questions below address the practical, policy and legal consequences of failing to comply with one or more of the following federal information management requirements (to the

extent required) and how those risks were or are being mitigated: (1) The Privacy Act System of Records Notice Requirement; (2) the Paperwork Reduction Act; (3) the Federal Records Act; (4) the E-Gov Act security requirements; and (5) Section 508 of the Rehabilitation Act of 1973.

Section 6.1: Privacy Act System of Records Notice (SORN)

For all collections of PII that meet certain requirements, the Privacy Act requires that the agency publish a SORN in the *Federal Register*.

System of Records
Section 6.1(a) ☐ Yes ☒ No ☐ N/A Does the system or project retrieve records about an individual using an identifying number, symbol, or other identifying particular assigned to the individual? (see items selected in Section 4.2 above) **Section 6.1(b)** ☐ Yes ☐ No ☒ N/A Was a SORN published in the *Federal Register* for this system of records?
Explanation of the Answers to Sections 6.1(a) and 6.1(b): Information included in the CCAR data is not retrieved by personal identifier and is therefore not subject to the requirements of the Privacy Act.

Section 6.2: The Paperwork Reduction Act

The PRA requires OMB approval before a federal agency may collect standardized data from 10 or more respondents within a 12 month period. OMB requires agencies to conduct a PIA (a Treasury PCLIA) when initiating, consistent with the PRA, a new electronic collection of [personally identifiable information] for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).

Paperwork Reduction Act Compliance
Section 6.2(a) ☒ Yes ☐ No Does the system or project maintain information obtained from individuals and organizations who are not federal personnel or an agency of the Federal government (i.e., outside the federal government)? **Section 6.2(b)** ☒ Yes ☐ No ☐ N/A Does the project or system involve a new collection of information in identifiable form for 10 or more persons from outside the Federal government? **Section 6.2(c)** ☒ Yes ☐ No ☐ N/A Did the project or system complete an Information Collection Request (hereinafter "ICR") and receive OMB approval?
Explanation of the Answers to Sections 6.2(a) through 6.2(c): Information included in the CCAR data was originally collected by the Board from regulated entities, in accordance with the rules, policies, and procedures governing the collection of such information. Information is collected using the Board's CCAR data report forms, which received OMB approval (OMB No. 7100-0341) and are available on the Board's website.

Section 6.3: Records Management - NARA/Federal Records Act Requirements

Records retention schedules determine the maximum amount of time necessary to retain information in order to meet the needs of the project or system. Information is generally either disposed of or sent to the NARA for permanent retention upon expiration of this period.

NARA Records Retention Requirements
Section 6.3(a) ☐ Yes ☒ No Has the Archivist of the United States approved a retention schedule for the records maintained in the system or by the project? **Section 6.3(b)** ☐ Yes ☒ No Do General Records Schedules (hereinafter "GRS") apply to the records maintained in the system or by the project? **Section 6.3(c)** ☒ Yes ☐ No ☐ N/A If the Archivist of the United States has not approved a retention schedule for the records maintained in the system or by the project and records are not covered by a GRS, has a draft retention schedule been developed for the records used in this project or system? **Section 6.3(d)** ☐ Yes ☒ No Have all applicable Treasury officials approved a draft retention schedule for the records used in this project or system?
Explanation of the Answers to Sections 6.3(a) through 6.3(d): The CCAR data is currently on a disposition hold as the Boards' records officials review the retention of all supervision records. Upon completion of scheduling for these records, OFR will work with the Board to ensure its own schedule mirrors the Board's.

Section 6.4: E-Government Act/NIST Compliance

The completion of Federal Information Security Management Act (hereinafter "FISMA") Security Assessment & Authorization process is required before a federal information system may receive Authority to Operate (hereinafter "ATO"). Different security requirements apply to National Security Systems.

Federal Information System Subject to FISMA Security Assessment and Authorization
Section 6.4(a) ☐ Yes ☐ No ☒ N/A Is the system a federal information system subject to FISMA requirements? **Section 6.4(b)** ☐ Yes ☐ No ☒ N/A Has the system or project, if applicable, undergone a Security Assessment and Authorization and received Authority to Operate?
Explanation of the Answers to Sections 6.4 (a) and 6.4(b): The CCAR data is an information collection and not an information system. However, the dataset will be stored within the Core Data Repository within the OFRAE, which is a FISMA system. The OFRAE has been categorized as a FIPS 199 moderate system and NIST 800-53 controls are configured in accordance with a FIPS 199 moderate baseline. The system was granted an Authority to Operate (ATO) effective 3/6/2014. The ATO expires on 3/6/2017.

Access Controls and Security Requirements
Section 6.4(c) ☒ Yes ☐ No Does the system or project include access controls to ensure limited access to information maintained by the system or project?
Explanation of the Answer to Section 6.4(c): Access to data will be granted on an as-needed, least-privilege basis through the approval workflow outlined in the OFR Access Control Procedures. Multiple layers of approval are required prior to granting access to data or systems at the OFR. Access controls are enforced by the OFR Information Security Team. Only authorized personnel have access to monitoring tools. The central log management tool that OFR is utilizing will enforce access controls. The OFRAE is categorized as a FIPS 199 moderate system and NIST SP 800-53 controls are configured in accordance with a FIPS 199 moderate baseline. Employees are trained annually on the laws and policies governing the collection, use, maintenance and dissemination of PII. Employees are also required to agree to and acknowledge by signature "Rules of Behavior" governing appropriate use of OFR Information Technology and OFR information. OFR also works closely with the Treasury Office of Privacy, Transparency and Records on all issues related to PII.

Security Risks in Manner of Collection
Section 6.4(d) ☒ Yes ☐ No In Section 4.3 above, you identified the sources for information used in the system or project and the method and manner of collection. Were any security, privacy, or civil liberties risks identified with respect to the manner in which the information is collected from the source(s)?
Explanation of the Answer to Section 6.4(d): There are privacy risks associated with participation and notice. Individuals may not understand that their information is being collected, and may have limited opportunities for correcting or amending their information. Information used by OFR for research purposes and received from third parties, including the CCAR data received from the Board, presents a low level of risk. In these instances, OFR does not use such information to make determinations about specific individuals, and such information is either collected without any direct-identifiers, or stripped of such identifiers, and are used for trend analysis in the aggregate. Research is done across the datasets to identify macro-level risks and trends in financial markets, but not related to individuals. As such, while data accuracy is less relevant, notice opportunities may be limited. That said, to foster transparency and reduce residual risk, OFR is outlining its receipt and use of such data in this PCLIA.

Security Controls When Sharing Internally or Externally
Section 6.4(e) ☐ Yes ☐ No ☒ N/A Are all Treasury/bureau security requirements met in the method of transferring information (e.g., bulk transfer, direct access by recipient, portable disk, paper) from the Treasury project or system to internal or external parties?
Explanation of the Answer to Section 6.4(e): Information included in the CCAR data is not shared with agencies, organizations, or individuals external to the OFR or Treasury.

Monitoring of Individuals
Section 6.4(f) ☐ Yes ☒ No Will this system or project have the capability to identify, locate, and monitor individuals or groups of people?
Explanation of the Answer to Section 6.4(f): Information included in the CCAR data does not contain any direct-identifiers and are used for trend analysis in the aggregate rather than identifying specific individuals. Further, per the agreement between OFR and the Board for use of the CCAR data, OFR employees are prohibited from any efforts to combine the CCAR data with other data in order to identify particular individuals. While the system (OFRAE) in which the CCAR data will be housed does not have the capability to identify, locate, or monitor individuals or groups of people, it does monitor users of the system for security, auditing, and functionality purposes.

Audit Trails
Section 6.4(g) ☒ Yes ☐ No Are audit trails regularly reviewed to ensure appropriate use, handling, and disclosure of PII maintained in the system or by the project inside or outside of the Department?
Explanation of the Answer to Section 6.4(g): The OFRAE, the system in which the CCAR data will be maintained, captures audit logs of employees, government contractors, and subcontractors using the OFRAE to ensure its proper use. Monitoring is done in accordance with internal OFR information system audit and accountability procedures. Event logs and log management tools are secure and access is limited to authorized staff only. Audit logs and audit settings at the OFR may not be tampered with, deleted, or disrupted. Any changes must be approved by the OFR Change Control Board (CCB) through a formal review of a configuration change request.

Section 6.5: Section 508 of the Rehabilitation Act of 1973 Compliance

When federal agencies develop, procure, maintain or use Electronic and Information Technology (hereinafter "EIT"), Section 508 of the Rehabilitation Act of 1973 (as amended in 1998) requires that individuals with disabilities (including federal employees) must have access and use (including privacy policies and directives as well as redress opportunities) that is comparable to that which is available to individuals who do not have disabilities.

Applicability of the Rehabilitation Act
Section 6.5(a) ☐ Yes ☒ No Will the project or system involve the development, procurement, maintenance or use of EIT as that term is defined in Section 508 of the Rehabilitation Act of 1973 (as amended in 1998)?

Compliance With the Rehabilitation Act
Section 6.5(b) ☐ Yes ☐ No ☒ N/A Does the system or project comply with all Section 508 requirements, thus ensuring that individuals with disabilities (including federal employees) have access and use (including access to privacy and civil liberties policies) that is comparable to that which is available to individuals who do not have disabilities?

Explanation of the Answer to Section 6.5(b): OFR has addressed the issue of Section 508 compliance for the OFRAE, the system in which the CCAR data will be maintained, in the PCLIA for the OFRAE.

Section 7.0: Redress

Freedom of Information Act and Privacy Act Redress
Section 7.0(a) ☒ Yes ☐ No Does the agency have a published process in place by which individuals may seek information and redress under the Freedom of Information Act and Privacy Act?
Explanation for Answer in Section 7.0(a): The Treasury FOIA Regulations can be found at 31 CFR Part 1, Subpart A. However, please note that information included in the CCAR data is not subject to the Privacy Act.

Privacy Act Access Exemption
Section 7.0(b) ☐ Yes ☒ No Was any of the information that is maintained in system of records and used in the system or project exempted from the access provisions of the Privacy Act?
Explanation of the Answer to Section 7.0(b): Information included in the CCAR data is not retrieved by personal identifier, and there is not subject to the Privacy Act.

Additional Redress Mechanisms
Section 7.0(c) ☐ Yes ☒ No With respect to information maintained by the project or system (whether or not it is covered by the Privacy Act), does the bureau or office that owns the project or system have any additional mechanisms other than Privacy Act and FOIA remedies (e.g., a customer satisfaction unit; a complaint process) by which an individual may request access to and/or amendment of their information and/or contest adverse determinations about denial of their rights, benefits, and privileges under Federal programs (e.g., decisions about whether the individual will receive a financial benefit, get a clearance or access to a Treasury facility, obtain employment with Treasury etc.)?
Explanation of the Answer to Section 7.0(c): Information included in the CCAR data is not used to make determinations about an individual's rights, benefits, or privileges under Federal programs.

Responsible Officials

Jill Cetina
Associate Director, Policy Studies
Office of Financial Research
U.S. Department of the Treasury

John Talbot
Chief Technology Officier
Office of Financial Research
U.S. Department of the Treasury

Cornelius Crowley
Deputy Director and Chief Data Officer
Office of Financial Research
U.S. Department of the Treasury

Ryan Law
Acting Deputy Assistant Secretary for
Privacy, Transparency, and Records
U.S. Department of the Treasury

Approval Signature

John R. Talbot
Digitally signed by John R. Talbot
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Departmental Offices, ou=People, serialNumber=630785, cn=John R. Talbot
Date: 2016.10.19 10:35:31 -04'00'

John Talbot
Chief Technology Officer
Office of Financial Research
U.S. Department of the Treasury

Digitally signed by Ryan A. Law
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Departmental Offices, ou=People, serialNumber=716338, cn=Ryan A. Law
Date: 2016.10.31 12:07:49 -04'00'

Ryan Law
Acting Deputy Assistant Secretary for
Privacy, Transparency and Records
U.S. Department of the Treasury

Jill K. Cetina
Digitally signed by Jill K. Cetina
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Departmental Offices, ou=People, serialNumber=200924, cn=Jill K. Cetina
Date: 2016.10.06 12:48:42 -04'00'

Jill Cetina
Associate Director, Policy Studies
Office of Financial Research
U.S. Department of the Treasury

Cornelius E. Crowley
Digitally signed by Cornelius E. Crowley
DN: c=US, o=U.S. Government, ou=Department of the Treasury, ou=Departmental Offices, ou=People, serialNumber=653985, cn=Cornelius E. Crowley
Date: 2016.10.17 12:24:40 -04'00'

Cornelius Crowley
Deputy Director and Chief Data Officer
Office of Financial Research
U.S. Department of the Treasury