JULY 2022

Annual Report of the Council of Inspectors General on Financial Oversight

Message from the Chair

In 2020 and 2021, the Federal Government enacted unprecedented levels of financial assistance and stimulus programs to provide much needed relief to individuals, families, and businesses in response to the Coronavirus Disease 2019 (COVID-19) pandemic. In keeping with its mission, the Council of Inspectors General on Financial Oversight (CIGFO), which is authorized to oversee Financial Stability Oversight Council (FSOC) operations, continues to monitor the ongoing response of FSOC and its member agencies related to the public health and financial crisis.

We are also mindful of new and evolving risks and challenges that could cause stress to the stability of the U.S. financial system. This past year, FSOC issued its report on climate-related financial risk in response to Executive Order 14030, *Climate-related Financial Risk*, and a report on digital assets required by Executive Order 14067, *Ensuring Responsible Development of Digital Assets* is expected in the fall of 2022. Meanwhile, the war in Ukraine has the potential to pose new challenges to financial stability that warrant monitoring by FSOC and its member agencies.

To accomplish CIGFO's oversight and monitoring activities, it has, since 2011, established working groups that are comprised of staff from the CIGFO member Inspector General offices to conduct reviews of FSOC operations. CIGFO relies on these working groups to fulfill its mission. In 2020, CIGFO approved a working group to compile forward-looking guidance for FSOC and its members to consider in preparing for a crisis. This project is expected to be completed in the summer of 2022. In 2021, CIGFO approved another working group to review FSOC's response to Executive Order 14030, *Climate-related Financial Risk*, which is expected to be completed in the fall of 2022.

CIGFO's monitoring activities also include sharing financial regulatory information which enhance the knowledge and insight of its members about specific issues related to members' current and future work. For example, during its quarterly meetings, CIGFO members discussed FinTech companies and the regulatory challenges these companies pose to federal regulators; Executive Orders 14030 and 14067; as well as legislative activities that could impact the financial regulatory system.

In the coming year, CIGFO members will continue, through their individual and joint work, to help strengthen the financial system by oversight of FSOC and its Federal member agencies.

/s/

Rich Delmar
Acting Chair, Council of Inspectors General on Financial Oversight
Deputy Inspector General, Department of the Treasury

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Table of Contents

THIS PAGE IS INTENTIONALLY LEFT BLANK.

Council of Inspectors General on Financial Oversight

The Council of Inspectors General on Financial Oversight (CIGFO) was established by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), and meets on a quarterly basis to facilitate the sharing of information among Inspectors General. The CIGFO members discuss the ongoing work of each Inspector General who is a member of the Council, with a focus on concerns that may apply to the broader financial sector, and exchange ideas about ways to improve financial oversight. The CIGFO publishes an annual report that includes separate sections within the exclusive editorial control of each Inspector General. Those sections describe the concerns and recommendations of each Inspector General and a discussion of ongoing and completed work.

During the course of the year, the CIGFO continued to monitor coordination efforts among and between Financial Stability Oversight Council (FSOC) members. Specifically, CIGFO members were briefed on and/or discussed the following:

- Financial Technology (FinTech) companies and recent developments regarding bank charters and regulatory challenges
- Office of the Comptroller of the Currency – current priorities and key issues which may have broader implications within CIGFO's lines of oversight
- Intelligence Community Inspector General – results of an audit of the implementation of the Cybersecurity Information Sharing Act of 2015
- Legislative matters of interest, including budget resolution and statutory debt limit constraints
- Executive Order 14030 – *Climate-related Financial Risk* and *A Roadmap to Build a Climate-Resilient Economy*
- FSOC's report on *Climate-related Financial Risk*
- Executive Order 14067 – *Ensuring Responsible Development of Digital Assets*

The Council of Inspectors General on Financial Oversight Reports

The Dodd-Frank Act authorizes CIGFO to convene a working group, by a majority vote, for the purpose of evaluating the effectiveness and internal operations of the FSOC.

To date, CIGFO has issued the following reports—

- 2012 - *Audit of the Financial Stability Oversight Council's Controls over Non-public Information*
- 2013 - *Audit of the Financial Stability Oversight Council's Designation of Financial Market Utilities*
- 2014 - *Audit of the Financial Stability Oversight Council's Compliance with Its Transparency Policy*
- 2015 - *Audit of the Financial Stability Oversight Council's Monitoring of Interest Rate Risk to the Financial System*
- 2017 - *Audit of the Financial Stability Oversight Council's Efforts to Promote Market Discipline*
- 2017 - *Corrective Action Verification of FSOC's Implementation of CIGFO's Audit Recommendations in the 2013 Audit of FSOC's Financial Market Utility Designation Process*
- 2018 - *Top Management and Performance Challenges Facing Financial Regulatory Organizations*
- 2019 - *Audit of the Financial Stability Oversight Council's Monitoring of International Financial Regulatory Proposals and Developments*
- 2019 - *Top Management and Performance Challenges Facing Financial-Sector Regulatory Organizations*
- 2020 - *Survey of FSOC and its Federal Member Agencies' Efforts to Implement the Cybersecurity Act of 2015*
- 2020 - *Council of Inspectors General on Financial Oversight Presidential Transition Handbook*

The corrective actions described by FSOC, with respect to the audits listed above, met the intent of our recommendations, and may be subject to verification in future CIGFO working group reviews.

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Office of Inspector General Board of Governors of the Federal Reserve System and Bureau of Consumer Financial Protection

We provide independent oversight by conducting audits, inspections, evaluations, investigations, and other reviews of the programs and operations of the Board of Governors of the Federal Reserve System and the Bureau of Consumer Financial Protection and demonstrate leadership by making recommendations to improve economy, efficiency, and effectiveness, and by preventing and detecting fraud, waste, and abuse.

Background

Congress established our office as an independent oversight authority for the Board, the government agency component of the broader Federal Reserve System, and the Bureau.

Under the authority of the Inspector General Act of 1978, as amended (IG Act), we conduct independent and objective audits, inspections, evaluations, investigations, and other reviews related to the programs and operations of the Board and the Bureau.

- We make recommendations to improve economy, efficiency, and effectiveness, and we prevent and detect fraud, waste, and abuse.
- We share our findings and make corrective action recommendations to the Board and the Bureau; we do not manage agency programs or implement changes.
- We keep the Board chair, the Bureau director, and Congress fully informed of our findings and corrective action recommendations, as well as the agencies' progress in implementing corrective action.

In addition to the duties set forth in the IG Act, Congress has mandated additional responsibilities for our office. Section 38(k) of the Federal Deposit Insurance Act (FDI Act) requires us to review failed financial institutions supervised by the Board that result in a material loss to the Deposit Insurance Fund (DIF) and produce a report within 6 months. The Dodd-Frank Wall Street Reform and Consumer Protection Act amended section 38(k) of the FDI Act by raising the materiality threshold and requiring us to report on the results of any nonmaterial losses to the DIF that exhibit unusual circumstances warranting an in-depth review.

Section 211(f) of the Dodd-Frank Act also requires us to review the Board's supervision of any covered financial company that is placed into receivership under title II of the act and produce a report that evaluates the effectiveness of the Board's supervision, identifies any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommends appropriate administrative or legislative action.

The Federal Information Security Modernization Act of 2014 (FISMA) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In a manner consistent with FISMA requirements, we perform annual independent reviews of the Board's and the Bureau's information security programs and practices, including testing the effectiveness of security controls and techniques for selected information systems.

Section 15010 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act established the Pandemic Response Accountability Committee (PRAC) within the Council of the Inspectors General on Integrity and Efficiency (CIGIE). PRAC is required to conduct and coordinate oversight of covered funds and the coronavirus response in order to detect and prevent fraud, waste, abuse, and mismanagement and identify major risks that cut across programs and agency boundaries. PRAC is also required to submit reports related to its oversight work to relevant federal agencies, the president, and appropriate congressional committees. The CIGIE chair named our inspector general as a member of PRAC, and as such, we participate in PRAC meetings, conduct PRAC oversight activities, and contribute to PRAC reporting responsibilities.

The economic disruptions caused by the COVID-19 pandemic resulted in an abrupt shock to financial markets and affected many credit channels relied on by households, businesses, and state and local governments. In response, the Board took steps to support the flow of credit to U.S. households and businesses. Notably, the Board used its emergency lending authority under section 13(3) of the Federal Reserve Act to create lending programs that ensure liquidity in financial markets and provide lending support to various sectors of the economy. In addition, the Bureau has continued to play a vital role throughout the pandemic by enforcing federal consumer protection laws and protecting consumers from abuse.

OIG Reports and Other Products Related to the Broader Financial Sector

In accordance with section 989E(a)(2)(B) of the Dodd-Frank Act, the following highlights the completed and ongoing work of our office, with a focus on issues that may apply to the broader financial sector.

COMPLETED WORK

Major Management Challenges for the Board and the Bureau

Although not required by statute, we biennially report on the major management challenges facing the Board and the Bureau. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the Bureau's accomplishment of their strategic objectives.

Among other items, we identified four major management challenges for the Board that apply to the financial sector in 2021:

- Designing and Operationalizing Emergency Lending Programs to Address the Economic Effects of the COVID-19 Pandemic
- Enhancing Organizational Governance and Risk Management
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Remaining Adaptable to External Developments While Supervising Financial Institutions

Among other items, we identified two major management challenges for the Bureau that apply to the financial sector in 2021:

- Remaining Adaptable to External Developments While Continuing to Refine the Supervision and Enforcement Strategy

- Managing Consumer Complaints

Results of Analytical Testing of the Board's Publicly Reported Data for the Main Street Lending Program, April 14, 2021

In response to the economic effects of the COVID-19 pandemic, the Board established several emergency lending programs and facilities to provide loans to employers, certain businesses, and communities across the country. The Board established the Main Street Lending Program (MSLP) to support lending to small and medium-sized for-profit businesses and nonprofit organizations that were unable to access the Paycheck Protection Program (PPP) or that required additional financial support after receiving a PPP loan. The MSLP ended on January 8, 2021.

In February 2021, we announced an evaluation of third-party cybersecurity risk management processes for vendors supporting the MSLP and the Secondary Market Corporate Credit Facility (SMCCF). During our planning work for this evaluation, we checked the accuracy and completeness of specific demographic data to identify invalid city-state combinations. We also determined the accuracy of specific MSLP transaction disclosure data.

We identified several inaccurate city and state data points affecting a limited number of published loan transactions for the MSLP. After informing Board and System officials of these inaccuracies, they took immediate steps to address them and to update the Board's public reporting.

Results of Analytical Testing of the Board's Publicly Reported Data for the Secondary Market Corporate Credit Facility, July 14, 2021

In response to the economic effects of the COVID-19 pandemic, the Board established several emergency lending programs and facilities to provide loans to employers, certain businesses, and communities across the country. The Board established two facilities to support credit to large employers: the Primary Market Corporate Credit Facility for new bond and loan issuance and the SMCCF to provide liquidity for outstanding corporate bonds. The Board designed the SMCCF to create a portfolio that tracked a broad, diversified market index of U.S. corporate bonds.

In February 2021, we announced an evaluation of third-party cybersecurity risk management processes for vendors supporting the MSLP and the SMCCF. During our planning work for this evaluation, we identified transactions that appeared to have been documented twice in each of the SMCCF transaction-specific disclosures published from January through April 2021. In addition, we identified instances in each of the publicly reported transaction-specific disclosures published from January through April 2021 in which transactions for partial bond redemptions were not clearly labeled and did not include redemption amounts.

After informing Board and Federal Reserve Bank of New York (FRB New York) officials of these duplicate entries, they took immediate steps to strengthen internal review processes to ensure that these transactions are appropriately recorded in the SMCCF public disclosure data.

The Board Can Improve the Efficiency and Effectiveness of Certain Aspects of Its Consumer Compliance Examination and Enforcement Action Issuance Processes, OIG Report 2021-SR-B-012, October 6, 2021

The Board delegates to each Federal Reserve Bank the authority to supervise certain financial institutions located within the Reserve Bank's district. Reserve Bank consumer compliance examination staff help execute the Board's consumer compliance supervision program, and the Board's Division of Consumer and Community Affairs (DCCA) oversees these delegated responsibilities. DCCA's *Consumer Compliance Handbook* describes Unfair or Deceptive Acts or Practices (UDAP) and fair lending as two of the most significant consumer compliance risk areas for financial institutions. We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action issuance processes, including the processes pertaining to UDAP and fair lending matters.

DCCA can improve the efficiency and effectiveness of the UDAP review processes by developing formal performance goals and target time frames, establishing criteria for when DCCA must review a potential UDAP matter, and providing guidance and training to Reserve Bank consumer compliance supervision personnel. Although DCCA has recently made efforts to improve the timeliness of the fair lending review processes by establishing new performance measures and targets as well as refining the criteria for delegating certain fair lending reviews to the Reserve Banks, DCCA can further enhance these processes by developing additional training to help acclimate Reserve Bank staff and examiners to their newly delegated roles and responsibilities. In addition, DCCA should assess the staffing structure and approach of its Fair Lending Enforcement and UDAP Enforcement sections. Finally, DCCA can enhance transparency in the UDAP and fair lending examination and enforcement action issuance processes by clarifying expectations for communicating with key stakeholders.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's and the Reserve Banks' consumer compliance examination and enforcement action issuance processes for UDAP and fair lending matters. The Board concurred with our recommendations.

The Board Has Effective Processes to Collect, Aggregate, Validate, and Report CARES Act Lending Program Data, OIG Report 2022-FMIC-B-004, February 28, 2022

The COVID-19 pandemic disrupted economic activity in the United States, which affected many sectors of the financial system. In response to the pandemic, the Board established lending programs under the CARES Act to support state and local governments and businesses of all sizes. The Board is required by statute to report on any outstanding loan or guarantee programs once every 30 days. We assessed the Board's processes for collecting, aggregating, validating, and reporting data related to its CARES Act lending programs.

The Board meets its CARES Act reporting requirements; voluntarily reports transaction-specific data; and publishes complete and accurate data, with the exception of some immaterial inaccuracies. Although the Board established and documented processes for collecting, aggregating, validating, and reporting CARES Act lending program data, it can improve the documentation of a key decision related to how it gains assurance that the publicly reported transaction-specific data are accurate and complete.

While the Board's decision to publish transaction-specific data exceeded applicable statutory requirements for publishing aggregate-level data on the lending programs, we identified additional opportunities to enhance transparency and reduce the potential to report immaterial inaccuracies in the supplemental data, which would further the Board's long-term objective to increase the public's understanding of its activities.

Our report contains recommendations designed to help the Board quickly establish processes for reporting on lending programs under similar future circumstances. The Board concurred with our recommendations, and one recommendation was closed, based on actions taken by the Board, upon issuance of this report.

The Bureau Can Improve Aspects of Its Quality Management Program for Supervision Activities, OIG Report 2021-SR-C-016, November 1, 2021

Within the Bureau's Division of Supervision, Enforcement and Fair Lending (SEFL), the Office of Supervision Examinations (OSE) is responsible for supervising and examining institutions' compliance with federal consumer financial laws. OSE's Oversight team is responsible for developing and supporting the supervision program and manages the Quality Management Program (QMP) for supervision activities. We assessed the design and effectiveness of SEFL's QMP for supervision activities.

SEFL can improve the effectiveness of its QMP for supervision activities by finalizing the updates to existing and draft QMP policies, procedures, and guidance and considering increasing SEFL leadership involvement in formal program oversight. Additionally, OSE should enhance aspects of the QMP's quality control review processes, assess the program's current staffing level and structure, formalize its training program, and enhance the reporting and distribution of its quality assurance results.

Our report contains recommendations designed to enhance the effectiveness of SEFL's QMP for supervision activities. The Bureau concurred with our recommendations.

The Bureau Can Further Enhance Certain Aspects of Its Approach to Supervising Nondepository Institutions, OIG Report 2021-SR-C-017, December 8, 2021

The Bureau's SEFL is responsible for ensuring compliance with federal consumer financial laws by supervising market participants and initiating enforcement actions when appropriate. The Dodd-Frank Act authorizes the Bureau to supervise depository institutions and their affiliates with more than $10 billion in total assets and certain nondepository institutions. We assessed SEFL's approach to supervising nondepository institutions.

SEFL applies consistent examination procedures to depository and nondepository institutions and uses the same approach to follow up on Matters Requiring Attention. These approaches help to ensure that the Bureau consistently supervises these two types of financial institutions. SEFL can, however, further improve its approach to supervising nondepository institutions. Specifically, SEFL has issued consumer compliance ratings to nondepository institutions less frequently than to depository institutions and faces challenges gathering information to identify the total population of nondepository institutions within the Bureau's jurisdiction. We also found that limited staffing levels in SEFL's OSE constrain the Bureau's ability to examine nondepository institutions. Lastly, SEFL's guidance lacked definitions for tracking certain examination data, and we identified inconsistent and missing data in SEFL's system of record.

Our report contains recommendations designed to further enhance the Bureau's approach to supervising nondepository institutions. The Bureau concurred with our recommendations.

ONGOING WORK

Evaluation of the Board's Processes for Reviewing and Approving Supervisory Proposals

The Board plays a significant role in supervising and regulating U.S. financial institutions. Through its oversight, the Board seeks to ensure that the institutions it supervises operate in a safe and sound manner and comply with applicable federal laws and regulations. Key aspects of the Board Division of Supervision and Regulation's mission include developing and implementing effective supervisory policy and guidance for supervised financial institutions. Board governors may be involved in reviewing and approving supervisory proposals addressing various matters, such as certain supervisory policy and guidance and aspects of the supervisory stress testing program. We are assessing the effectiveness of the Board's processes for reviewing and approving supervisory proposals. Our focus is on the Board's practices for determining which supervisory proposals and activities warrant consultation and approval by the governors. Our scope includes proposals related to supervisory policy and guidance as well as the supervisory stress testing program.

Monitoring of the Federal Reserve's Lending Programs

In response to the economic effects of the COVID-19 pandemic, the Federal Reserve created new lending programs to provide loans to employers, certain businesses, and communities across the country to support the U.S. economy. Specifically, the following programs have been created: the MSLP, the Paycheck Protection Program Liquidity Facility, the Municipal Liquidity Facility, the Primary Market Corporate Credit Facility, and the SMCCF. We initiated an active monitoring effort of these programs to gain an understanding of the operational, governance, reputational, and financial matters associated with them. Through this monitoring effort, we will refine our focus on the programs and identify areas for future audits or evaluations. Some of the topics we are considering include the design, operation, governance, and oversight of the lending programs; data collection and reporting associated with the programs; and the effect of the programs on the Board's supervision and regulation activities.

Evaluation of the Board's Statistical Assessment of Bank Risk and Bank Exams Tailored to Risk Processes

The Board uses various models to inform risk-based examination decisions. The Board's Statistical Assessment of Bank Risk (SABR) surveillance models and processes inform the agency's watch list, which highlights state member banks and holding companies with emerging financial weaknesses and flags institutions in the initial phases of financial deterioration. The Board uses the Bank Exams Tailored to Risk (BETR) processes to assess the level of risk at a state member bank, which allows supervisory personnel to tailor examination procedures to the size, complexity, and risk profile of the institution. We are assessing the effectiveness of the model risk management processes pertaining to SABR and BETR.

Evaluation of the Board's and the Federal Reserve Banks' Ethics Programs Pertaining to Personal Investment and Trading Activities

As the central bank of the United States, the Board must maintain impartiality and avoid even the appearance of conflicts of interest to inspire public trust in the nation's financial system. The Board recently announced a broad set of new investment and trading rules that, among other things, will prohibit the purchase of individual securities, restrict active trading, and increase the timeliness of reporting and public disclosure. We are assessing the design and effectiveness of these new rules as well as the Board's and the Reserve Banks' approach to monitoring personal investment and trading activities for possible conflicts of interest.

Evaluation of the Board's Oversight of FRB New York's Vendor Selection and Management Processes Related to Its Emergency Lending Facilities

As part of its emergency lending program, FRB New York operated six emergency lending facilities, five of which were supported by multiple vendor contracts. FRB New York awarded some of its emergency lending program–related contracts noncompetitively because of the exigent circumstances, and other contracts pose potential conflict-of-interest risks to the System. FRB New York's reliance on vendors highlights the importance of its monitoring of vendor performance. We are assessing the Board's and FRB New York's processes related to vendor selection and management for FRB New York's emergency lending programs.

Evaluation of the Federal Reserve System's Loan Purchases and Administration for Its MSLP

In response to the COVID-19 pandemic, the System established the MSLP—composed of five different lending facilities—to facilitate lending to small and medium-sized for-profit and nonprofit organizations. Through the MSLP, the Federal Reserve Bank of Boston (FRB Boston) purchased 1,830 loans amounting to approximately $17.5 billion from lenders; the majority of these loans were purchased during the last 2 months of the program. Following the purchase of the loans, FRB Boston is now responsible for administering the loans, including assessing overall credit risk and identifying substandard loans. FRB Boston leveraged third-party vendors to support both loan purchases and loan administration. We are assessing the MSLP's processes for loan purchases and loan administration, including the design, implementation, and operating effectiveness of internal controls.

Evaluation of Third-Party Cybersecurity Risk Management Processes for Vendors Supporting the Main Street Lending Program (MSLP) and the Secondary Market Corporate Credit Facility (SMCCF)

In response to the economic effects of the COVID-19 pandemic, the Board created new lending programs and facilities to provide loans to employers, certain businesses, and communities across the country to support the U.S. economy. To support the implementation of specific programs and facilities, the Federal Reserve Banks have contracted with third-party vendors for various services, such as administrative, custodial, legal, design, and investment management services. These vendors provide data generated from the operations and management of the facilities to the Reserve Banks, who then provide the data to the Board. We are evaluating the effectiveness of the risk management processes designed to ensure that effective information security and data integrity controls are implemented by third parties supporting the administration of the MSLP and the SMCCF.

Office of Inspector General Commodity Futures Trading Commission

The CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate.

Background

The CFTC OIG was created in 1989 in accordance with the 1988 amendments to the Inspector General Act of 1978 (P.L. 95-452). OIG was established as an independent unit to:

- Promote economy, efficiency and effectiveness in the administration of CFTC programs and operations and detect and prevent fraud, waste and abuse in such programs and operations;
- Conduct and supervise audits and, where necessary, investigations relating to the administration of CFTC programs and operations;
- Review existing and proposed legislation, regulations and exchange rules and make recommendations concerning their impact on the economy and efficiency of CFTC programs and operations or the prevention and detection of fraud and abuse;
- Recommend policies for, and conduct, supervise, or coordinate other activities carried out or financed by such establishment for the purpose of promoting economy and efficiency in the administration of, or preventing and detecting fraud and abuse in, its programs and operations; and
- Keep the Commission and Congress fully informed about any problems or deficiencies in the administration of CFTC programs and operations and provide recommendations for correction of these problems or deficiencies.

CFTC OIG operates independently of the Agency and has not experienced interference from the CFTC Chairman in connection with the conduct of any investigation, inspection, evaluation, review, or audit, and our investigations have been pursued regardless of the rank or party affiliation of the target.[1] The CFTC OIG consists of the Inspector General, the Deputy Inspector General/Chief Counsel, the Assistant Inspector General for Auditing, the Assistant Inspector General for Investigations (vacant), two Attorney-Advisors, two Auditors, and one Senior Program Analyst. The CFTC OIG obtains additional audit, investigative, and administrative assistance through contracts and agreements.

1 The Inspector General Act of 1978, as amended, states: "Neither the head of the establishment nor the officer next in rank below such head shall prevent or prohibit the Inspector General from initiating, carrying out, or completing any audit or investigation…." 5 U.S.C. App. 3 sec. 3(a).

Role in Financial Oversight

The CFTC OIG has no direct statutory duties related to oversight of the futures, swaps and derivatives markets; rather, the CFTC OIG acts as an independent Office within the CFTC that conducts audits, investigations, reviews, inspections, and other activities designed to identify fraud, waste, and abuse in connection with CFTC programs and operations, and makes recommendations and referrals as appropriate. The CFTC's yearly financial statement and Customer Protection Fund audits are conducted by an independent public accounting firm, with OIG oversight.

Recent, Current or Ongoing Work in Financial Oversight

In addition to our work on CIGFO projects described elsewhere in this report, and our detail of a senior OIG Program Analyst to the U.S. Department of the Treasury to assist development of an interagency committee to address Household Resilience to Climate Change, CFTC OIG started the following projects during the past year:

2021-I-4 Pay Protection Program Proactive Investigation

In May 2021, OIG began a proactive investigation (2021-I-4) in coordination with CIGIE's Pandemic Response Accountability Committee (PRAC), CIGIE's Pandemic Analytics Center for Excellence, and the Small Business Administration, involving multiple phases. The first Phase identified CFTC employees who had obtained PPP loans and whether proper authorization for outside business activities had been obtained. CFTC OIG made recommendations to the Agency to improve the business processes and disclosures concerning outside business activities. Phase II and Phase III involve potential oversight issues. The Phase II and Phase III objectives are to:

- Identify CFTC registrants who have received PPP loans, with the potential goal of recommending that CFTC increase oversight efforts to assure CFTC's no-action relief is followed properly, if warranted, as well as other potential recommendations with regard to the oversight of registrants who have received PPP loans (including issues, if any, indicating potential systemic impact), and indicia of fraud in connection with the PPP loans identified.
- Identify CFTC contractors who obtained PPP loans to identify any indicia of fraud or potential reputational risks to the Agency.

OIG contracted with a third-party vendor to provide analytic support to examine the millions of records received in this investigation. OIG has shared its findings and has collaborated with other CIGFO OIGs on investigative methods to maximize the value of this investigation to the oversight community.

White Paper Evaluating CFTC Experience with Digital Assets

Digital assets—including, among other things, cryptocurrency—have been widely adopted and used by both market participants and ordinary consumers. The CFTC has played an active role in the digital asset space, offering information to the public in the form of education and guidance as well as prosecuting digital asset-related conduct that violates the Commodity Exchange Act. This white paper will provide a general background of the digital asset market, the CFTC's participation in the digital asset market, an overview of CFTC staff views and experience with digital assets, and potential recommendations for future CFTC engagement. This project began during the Summer of 2021.

Office of Inspector General
Federal Deposit Insurance Corporation

The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency.

Background

The Federal Deposit Insurance Corporation (FDIC) was created by the Congress in 1933 as an independent Agency to maintain stability in the Nation's banking system by insuring deposits and independently regulating state-chartered, non-member banks. The FDIC insures $9.73 trillion in deposits at about 4,840 banks and savings associations, and promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The Deposit Insurance Fund balance totaled $123.1 billion as of December 31, 2021.

The FDIC is the primary Federal regulator for approximately 3,120 of the insured institutions. An equally important role for the FDIC is as Receiver for failed institutions; the FDIC is responsible for resolving the institution and managing and disposing of its remaining assets.

The Office of Inspector General (OIG) at the FDIC is an independent and objective oversight unit established under the Inspector General (IG) Act of 1978, as amended. Our mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the Agency. We pursued audits, evaluations, and other reviews throughout the year in carrying out this mission. Of particular interest for this CIGFO report, our audit and evaluation work covered topics such as Sharing of Threat Information, Terminations of Bank Secrecy Act/Anti-Money Laundering Consent Orders, and Supply Chain Risk Management.

Importantly, and in connection with matters affecting the financial sector, in February 2022, our Office also published its assessment of the Top Management and Performance Challenges Facing the FDIC. Our Top Management and Performance Challenges document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, in accordance with the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 10, 2021).

In addition to the above activities related to the broader financial sector, our Office conducted significant investigations into criminal and administrative matters involving sophisticated, complex multi-million-dollar frauds. These schemes involve bank fraud, embezzlement, money laundering, currency exchange manipulation, and other crimes involving banks, executives, directors, officials, insiders, and financial professionals. We are also working to detect and investigate cyber-criminal cases that threaten the banks and banking sector. Our cases reflect the cooperative efforts of other OIGs, U.S. Attorneys' Offices, FDIC Divisions and Offices, and others in the law enforcement community throughout the country. These working partnerships contribute to ensuring the continued safety and soundness of the Nation's banks and help ensure integrity in the FDIC's programs and activities.

Our Office also continues to play a key role in the investigation of individuals and organized groups perpetrating fraud through the Paycheck Protection Program (PPP) under the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and American Rescue Plan (ARP). To date, we have opened 169 cases associated with fraud in the CARES Act and ARP programs. We strongly support the Pandemic Response Accountability Committee's Fraud Task Force and the Department of Justice's COVID-19 Fraud Enforcement Task Force. We will continue to work in close collaboration with our law enforcement partners.

The FDIC OIG also played a key role over the past year as Co-Lead of the CIGFO Working Group that developed forward-looking guidance for the Financial Stability Oversight Council and its member agencies to consider in preparing for and managing future crises. (Guidance in Preparing for and Managing Crises.)

FDIC OIG Audits and Evaluations Made Significant Recommendations for Improvements to the FDIC

During the 12-month period ending March 31, 2022, the FDIC OIG issued 11 audit and evaluation products and made 89 recommendations to strengthen controls in FDIC programs and operations. In the write-ups below, we discuss three significant reviews, as they cover issues relevant to the broader financial sector.

Sharing of Threat Information to Guide the Supervision of Financial Institutions

Banks face a wide range of threats to their operations, including cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters. The consequences of these threats may significantly affect the safety and soundness of numerous financial institutions -- as well as the stability of the Nation's financial system.

Therefore, it is important that the FDIC develop policies, processes, and procedures to ensure that vital threat information is shared with its personnel – such as FDIC policymakers, bank examiners, supervisory personnel, and Regional Office staff – so that the data may be used in an actionable and timely manner. Our Office conducted a review to determine whether the FDIC had established effective and efficient processes to share threat information with its personnel. We identified several weaknesses in the FDIC's sharing of threat information and reported on those during the reporting period.

We found that the FDIC did not establish effective governance processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. Specifically, the FDIC:

- Did not establish a written governance structure to guide its threat information sharing activities;
- Did not complete, approve, and implement a governance Charter to establish a common understanding of the role for the FDIC's Intelligence Support Program, or to define an overall strategy and its requirements;
- Did not develop goals, objectives, or measures to guide the performance of its Intelligence Support Program;
- Did not establish adequate policies and procedures that defined roles and responsibilities for key stakeholders involved in the threat information sharing program and activities; and
- Did not fully consider threat information sharing in its Enterprise Risk Inventory and Risk Profile.

Further, we identified additional gaps in the FDIC's processes for acquiring, analyzing, and disseminating threat information, and in how the use of threat information could be improved. For example, the FDIC:

- Did not develop written procedures for determining its threat information requirements;

- Did not engage all relevant stakeholders when it developed its threat information needs;
- Did not establish procedures to guide its analysis of threat information; instead, the FDIC relied solely on the discretionary judgment of certain individuals to determine the extent to which threat information should be analyzed to support business and supervisory needs;
- Did not develop procedures for disseminating threat information;
- Had not established an infrastructure that would allow for the secure handling of classified information to certain senior FDIC officials; and
- Did not establish a procedure to obtain feedback from recipients of threat information to assess its utility and effectiveness.

We also found numerous gaps in the FDIC's management of threat information sharing, including: not having backup personnel for its Senior Intelligence Officer nor plans for an absence or departure; not establishing minimum training requirements for the Senior Intelligence Officer position; not obtaining required security clearance for certain senior FDIC officials; and not properly categorizing unclassified threat information.

We made 25 recommendations to the FDIC to strengthen its governance processes for acquiring, analyzing, disseminating, and using relevant and actionable threat information to guide the supervision of financial institutions.

Special Note on Banks' Cyber Incident Reporting Requirements**:** In April 2020, as part of our ongoing Threat Information Sharing review, the OIG identified an issue--that the banks were not required to report significant cyber incidents to the FDIC in a timely manner. After identifying this issue, we submitted a memorandum recommending that financial institutions be required to notify the FDIC of cyber incidents. As a result, in December 2020, the FDIC, the Federal Reserve Board, and the Office of the Comptroller of the Currency announced a proposed new regulation that would require all financial institutions and their service providers to promptly notify their primary Federal regulator if they experience a destructive cyber incident. This rule was made final in November 2021 and requires that a banking organization notify its financial regulator of a significant computer-security incident no later than 36 hours after a cyber incident has occurred. This final rule reflects the great work and contributions of our OIG team, as well as the value and significance of the OIG's work in identifying critical issues for the FDIC and the broader financial sector.

Termination of Bank Secrecy Act/Anti-Money Laundering Consent Orders

Money laundering is a serious crime that aims to conceal or disguise the illicit proceeds of another unlawful activity. The Bank Secrecy Act (BSA) has established recordkeeping and reporting requirements for financial institutions to implement -- in order to detect and prevent money laundering. The FDIC's examinations of banks for compliance with these requirements are essential elements in identifying potential weaknesses in a bank's BSA/Anti-Money Laundering (AML) program.

When a financial institution is not in compliance with such requirements, the FDIC may issue a Consent Order—which is a formal enforcement action against a bank. A BSA/AML Consent Order often contains several provisions for improvements to the bank's program, and FDIC examiners review a bank's progress in addressing these Consent Order provisions.

Our Office conducted an evaluation to determine whether the FDIC considered factors similar to other Federal bank regulators in terminating BSA/AML Consent Orders; terminated BSA/AML Consent Orders in accordance with FDIC-established guidance; monitored FDIC Regional Office termination decision-making to ensure consistency across the Regions; and documented its actions.

We found that the factors considered by the FDIC to terminate Consent Orders differed from the factors used by the Federal Reserve Board and the Office of the Comptroller of the Currency. When Consent Orders are issued, all provisions requiring correction are published on the FDIC website; however informal actions are not issued publicly.

In some cases, the FDIC may terminate a Consent Order when provisions are in "substantial compliance" or "partially met." Therefore, in terminating an FDIC Consent Order, it will be removed from the website – even if not all of the provisions have been corrected. As a result, these website postings make it appear to the public, bank customers, and bank investors that all Order provisions have been corrected, although some previously-publicized Order provisions may not have been met.

We further found that the FDIC did not provide guidance to its examiners in how to apply the terms, "substantial compliance" and "partially met," as a basis for terminating a Consent Order. The term, "partially met," provides extremely wide latitude to terminate a Consent Order when any portion of it is met. As a result, the FDIC could not be certain that some Consent Orders were terminated using a consistent interpretation of these terms.

In addition, we found that:

- Termination decisions were not centrally monitored, which would serve as an important internal control.
- The FDIC did not consistently prepare and maintain documentation in its systems of record to support the monitoring and termination decisions for BSA/AML Consent Orders.

Incorrect documentation of Consent Order terminations caused the FDIC to provide nine incorrect reports to the FDIC Board of Directors concerning enforcement actions; and caused the FDIC not to report three BSA/AML Consent Order terminations to the Financial Crimes Enforcement Network (FinCEN) in the Department of the Treasury.

We made 10 recommendations to enhance the FDIC's BSA/AML Consent Order termination guidance and procedures.

The FDIC's Implementation of Supply Chain Risk Management

The FDIC awarded more than $2 billion via 483 contracts in 2021, procuring products and services from many types of vendors, contractors, and subcontractors. The supply chain for each vendor, contractor, or subcontractor may present unique risks to the FDIC, including the installation of counterfeit hardware and software in the FDIC environment, or reliance on a malicious or unqualified provider. Supply chain threats could compromise the FDIC's Information Technology and data on its information systems and provide adversaries a means to exfiltrate sensitive information such as confidential bank examination information.

Therefore, the FDIC must implement a robust Supply Chain Risk Management (SCRM) Program to identify and mitigate supply chain risks that threaten its ability to fulfill its mission, goals, and objectives; protect its sensitive and nonpublic information; and maintain the integrity of its operations. We conducted an evaluation to determine whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices.

We found that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter (November 2019) and was not conducting supply chain risk assessments in accordance with best practices. For example, the FDIC had not:

1. Identified and documented known risks to the Agency's supply chain;
2. Defined a risk management framework to evaluate risks to non-Information Technology procurements; or
3. Established metrics and indicators related to continuous monitoring and evaluation of supply chain risks.

We also found that the FDIC did not conduct supply chain risk assessments during its procurement process for Chief Information Officer Organization and other Division and Office contracts. In addition, the FDIC had not ensured that its Enterprise Risk Management processes fully captured supply chain risks. Further, FDIC Contracting Officers did not maintain contract documents in the Contract Electronic File system, as required.

We made nine recommendations to the FDIC to address the findings in our report and strengthen its SCRM Program.

FDIC OIG Assessed the Top Management and Performance Challenges Facing the FDIC

Our assessment of the Top Challenges facing the FDIC is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

We identified nine Top Challenges facing the FDIC, as follows:

The FDIC's Readiness for Crises. The FDIC must be prepared for all crises, because of its unique role in overseeing and administering the DIF, which insures the bank accounts of millions of depositors and consumers. The FDIC faces Challenges in fully developing its plans to respond to an unfolding crisis. Further, the FDIC should consider climate-related risks with respect to the report issued by the Financial Stability Oversight Council, and whether it will take actions in response to the report's recommendations in preparing its supervisory and examination processes. The FDIC should also be ready to respond to evolving risks associated with the current pandemic and other crises, including supervising and examining Government-guaranteed loans at banks and related fraud risks.

Cybersecurity for Banks and Third-Party Service Providers. Cybersecurity has been identified as the most significant threat to the banking sector and the critical infrastructure of the United States. The FDIC faces Challenges to ensure that examiners have the appropriate skillsets and knowledge to conduct information technology examinations that adequately identify and mitigate cybersecurity risks at banks and their third-party service providers. Further, the FDIC should establish a process to receive, analyze, and act on reports of significant cyber incidents at banks in order to adjust supervisory strategies, policies, and training for bank examiners; to warn other banks of such threats; and to prepare for potential bank failures. Mitigating cybersecurity risk is critical as a cyber incident at one bank or third-party service provider has the potential to cause contagion within the financial sector. The FDIC also should assess the risks to banks presented by crypto assets, particularly with respect to the anonymous nature of these assets and the increased risk of money laundering and other wrongdoing.

Supporting Underserved Communities in Banking. The FDIC should ensure that its programs – including those that support Minority Depository Institutions and Community Development Financial Institutions -- are effectively designed to foster financial inclusion and reduce the number of unbanked and underbanked individuals. Further, the FDIC's examinations should continue to ensure that banks are in compliance with regulations that combat discriminatory lending practices against low-income borrowers and minority populations. The FDIC also should ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence in decision-making and minimize any undue bias related to the algorithms or historical data used.

Organizational Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to manage the affairs of the Agency and its risks, formulate regulatory policy, and provide clear guidance to banks and FDIC Regional Offices. Through these processes, the FDIC can allocate resources, prioritize and improve the flow of risk information to decision-makers, and work towards achieving the FDIC's mission. The FDIC faces Challenges in providing clarity concerning the submission of motions presented to the Board of Directors for consideration and approval. Further, the FDIC should ensure that the Board, through its Audit Committee, can oversee and manage the risks identified and monitored through its Enterprise Risk Management Program. The FDIC also should clarify under what circumstances and which portions or provisions of Executive Branch policies or guidance are to be followed. In addition, the FDIC should ensure that weaknesses in FDIC programs are corrected and recommendations are addressed in a timely manner. FDIC rulemaking and guidance should also be aligned with other regulators to ensure that banks are not treated differently depending upon their primary regulator. FDIC internal guidance also should be clearly defined to ensure consistent application of FDIC program requirements. In addition, FDIC rulemaking should be a transparent process that analyzes the need for safety and soundness regulations and the compliance burden placed on banks.

Information Technology (IT) Security at the FDIC. The FDIC relies on its IT systems for day-to-day activities and especially during crises. The FDIC continues to face Challenges to ensure that it has strong information security processes to guard against persistent and increasing cyber threats against Federal agencies. Security control weaknesses of FDIC systems limit the effectiveness of FDIC controls, which places the confidentiality, integrity, and availability of FDIC systems and data at risk. The FDIC should address its outstanding corrective actions related to IT security controls, management of privileged Administrative Accounts, and oversight and monitoring of information systems. Further, the FDIC should ensure that it establishes effective security controls for its mobile devices and for the automated systems that monitor and control critical building services at facilities.

Security and Privacy at the FDIC. The FDIC employs a workforce of approximately 5,800 employees and 1,600 contract personnel at 92 FDIC facilities throughout the country, and it is custodian of 76 IT systems and voluminous hard-copy records. The FDIC should continue to manage risks associated with its personnel security and suitability processes to ensure that employees and contractors undergo appropriate and timely investigations and re-investigations commensurate with their positions. As well, the FDIC should maintain its risk-based physical security program and ensure that its policies promote an FDIC work environment that is free from discrimination, harassment, and retaliation. Further, the FDIC should have effective programs to safeguard all forms of sensitive and Personally Identifiable Information in its possession.

The FDIC's Collection, Analysis, and Use of Data. Data and information can enhance capabilities to mitigate threats against banks and the U.S. financial system. The FDIC faces Challenges in establishing effective processes to govern its sharing of threat information to guide the supervision of financial institutions. Effective sharing of threat information helps the FDIC to protect the DIF and the financial system by building situational awareness; supporting risk-informed decision-making; and influencing supervisory strategies, policies, and training.

The FDIC should establish a written governance structure and implement a Charter to establish a common understanding of its Threat Information Sharing program and define an overall strategy and requirements for it. Further, the FDIC should develop goals, objectives, and measures to guide the performance of its Intelligence Support Program, and it should establish adequate policies and procedures to define roles and responsibilities. The FDIC faces Challenges in the four component functions of Threat Information Sharing – acquisition, analysis, dissemination, and feedback. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior officials can depend upon the data to assess program effectiveness throughout the organization.

Contracting and Supply Chain Management at the FDIC. The FDIC awarded over $2 billion in contracts for goods and services in 2021 in support of its mission. The FDIC faces Challenges to establish an effective contract management program that ensures the FDIC receives goods and services according to contract terms, price, and timeframes. Further, the FDIC should have processes in place to identify and ensure heightened monitoring of contracts for Critical Functions, so that the Agency maintains control of its mission functions and prevents over-reliance on contractors. The FDIC also should have programs in place to manage and mitigate security risks associated with the supply chains for contracted goods and services. Further, the FDIC should ensure notifications to contractors and sub-contractor personnel, so that they are advised about and aware of their whistleblower rights and protections, and that they know how to report allegations of misconduct, violations, and gross mismanagement.

Human Resources at the FDIC. The FDIC relies on the talents and skills of its employees to achieve its mission, and it faces Challenges in managing its human capital lifecycle. At the present time, nearly 25 percent of the FDIC workforce is eligible to retire, and this figure climbs to nearly 40 percent by 2026. These figures include personnel in key divisions supporting the FDIC mission – including the Division of Resolutions and Receiverships (over 59 percent by 2026); Division of Finance (over 55 percent by 2026); Legal Division (over 51 percent by 2026); and Division of Administration (about 49 percent by 2026). Further, the FDIC should continue to improve its program for the retention of employees, as well as the collection and analysis of relevant personnel data. In addition, the FDIC should continue to ensure diversity and inclusion among its workforce. Absent effective human capital management, the

FDIC may lose valuable knowledge and leadership skill sets upon the departure of experienced examiners, managers, and executives. Meeting these Challenges is especially important as the FDIC shifts its operations to a hybrid work environment.

FDIC OIG Investigations Helped Ensure Integrity in the Banking Sector and Addressed Fraud in the Federal Pandemic Response

Our Office is committed to partnerships with other OIGs, the Department of Justice (DOJ), and other state and local law enforcement agencies in pursuing criminal acts affecting banks and in helping to deter fraud, waste, abuse, and misconduct. The OIG also actively participates in many financial fraud and cyber working groups nationwide to keep current with new threats and fraudulent schemes that can undermine the integrity of the FDIC's operations and the financial services industry as a whole.

Our investigative results over the 12 months ending March 31, 2022, included the following: 148 indictments; 135 convictions; 109 arrests; and potential monetary recoveries (fines, restitution, and asset forfeitures) of nearly $1.3 billion.

As illustrated in the case examples that follow, we continue to identify emerging financial fraud schemes that affect FDIC-supervised and insured institutions. We also partner with other agencies, including the Small Business Administration (SBA), to identify fraud in the guaranteed loan portfolios of FDIC-supervised institutions. These investigations are important, as large-scale fraud schemes can significantly affect the financial industry and the financial condition of FDIC-insured institutions. In this regard, and as illustrated below, we continue to investigate Paycheck Protection Program (PPP) cases of individuals defrauding the Government guaranteed-loan program intended to help those most in need during the pandemic crisis. Examples of our investigative work follow.

DC Solar Owner Sentenced to 30 Years in Prison for a Billion Dollar Ponzi Scheme

On November 9, 2021, Jeff Carpoff, owner of DC Solar, was sentenced to 30 years in prison and ordered to pay restitution of $790 million. Between 2011 and 2018, DC Solar manufactured mobile solar generator (MSG) units, which were solar generators that were mounted on trailers and were promoted as being able to provide emergency power to cellphone towers and lighting at sporting events. A significant incentive for investors was generous federal tax credits due to the solar nature of the MSGs.

The conspirators carried out an accounting and lease revenue fraud using Ponzi-like circular payments. Carpoff and others lied to investors about the market demand for DC Solar's MSGs and its revenue from leasing to third parties, then covered up these lies with techniques including false financial statements and fake lease contracts. Their fraud concealed a circular payment structure where Carpoff and others were simply using new investors' money to pay older investors the purported lease revenue that investors were expecting.

As DC Solar lost vast sums of money with this fraudulent model, Carpoff and other conspirators stopped building the MSGs altogether, selling thousands of MSGs that did not even exist to investors. To carry out this part of the fraud, Carpoff and others made it appear that MSGs existed in locations that they did not, swapped vehicle identification number stickers on MSGs that had been built earlier, and attempted to deceive certain investors during equipment inspections. In reality, at least half of the approximately 17,000 mobile solar generators claimed to have been manufactured by DC Solar did not exist. The fraud scheme resulted in investor losses totaling approximately $1 billion.

Source: *USAO, Eastern District of California.*

Responsible Agencies*: FDIC OIG, Federal Bureau of Investigation (FBI), and Internal Revenue Service-Criminal investigation (IRS-CI). Prosecuted by the USAO, Eastern District of California, Sacramento.*

Jury Convicts Five Former Officers and Employees of Banc-Serv Partners in $5 Million Scheme to Defraud the Small Business Administration

On August 5, 2021, a Federal jury convicted five former officers and employees of Banc-Serv Partners LLP in a 13-year conspiracy to defraud the SBA in connection with its programs to guarantee loans made to small businesses.

According to the evidence presented at trial, the defendants — Kerri Agee, of Noblesville, Indiana, former president, chief executive officer and founder of Banc-Serv; Kelly Isley, of Westfield, Indiana, Banc-Serv's former chief operating officer; Nicole Smith, of Indianapolis, Indiana, a former Banc-Serv employee; Chad Griffin, of Carmel, Indiana, Banc-Serv's former chief marketing officer; and Matthew Smith, of Westfield, Indiana, Banc-Serv's co-founder and a former director of a lending institution that originated loans with Banc-Serv — fraudulently obtained SBA-guaranteed loans on behalf of their clients, knowing that the loans did not meet SBA's guidelines and requirements for the guarantees.

The evidence at trial proved that from approximately 2004 until October 2017, the defendants helped originate SBA loans on behalf of various financial institutions and other lenders and, on multiple occasions, fraudulently obtained guarantees for loans that the SBA had deemed ineligible. They did so by, among other things, knowingly misrepresenting what the loans would be used for and unlawfully diverting previously denied loan applications into expedited approval channels at the SBA. When the fraudulently guaranteed loans defaulted, the defendants caused the submission of the reimbursement requests to the SBA to purchase the defaulted loans from investors and lending institutions, thereby shifting some of the losses on the ineligible loans to the SBA. The fraudulent loans presented at trial totaled approximately $5 million in guaranteed disbursements, which were not eligible for SBA guarantees.

Agee was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and four counts of wire fraud affecting a financial institution. Isley was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and two counts of wire fraud affecting a financial institution. Nicole Smith was convicted of one count of conspiracy to commit wire fraud affecting a financial institution and two counts of wire fraud affecting a financial institution. Griffin was convicted of one count of conspiracy to commit wire fraud affecting a financial institution. Matthew Smith was convicted of one count of conspiracy to commit wire fraud.

These individuals were subsequently sentenced, as follows: Kerri Agee, was sentenced to 68 months in prison; Kelly Isley was sentenced to 57 months; Chad Griffin, was sentenced to 28 months; Matthew Smith, was sentenced to 46 months; and Nicole Smith, was sentenced to 30 months.

In addition to their prison sentences, all five defendants were ordered to pay restitution to the SBA. Agee, Isley, and Nicole Smith were each ordered to pay $2,289,681; Griffin was ordered to pay $685,022; and Matthew Smith was ordered to pay 1,651,450.

Source: *SBA OIG.*

Responsible Agencies: *FDIC OIG, SBA OIG, Department of Housing and Urban Development OIG, and FBI. Prosecuted by the DOJ Fraud Section in the Southern District of Indiana.*

First Person Charged for Fraudulently Seeking COVID-Relief Business Loans is Sentenced

On October 7, 2021, David Adler Staveley was sentenced to serve 56 months in Federal prison followed by 3 years of supervised release after pleading guilty to conspiracy to commit bank fraud and failure to appear in court. Staveley was the first person in the country charged with fraudulently seeking forgivable pandemic relief small business loans guaranteed by the SBA under the CARES Act. Staveley fled from prosecution after removing his electronic monitoring device and attempted to stage a suicide 3 weeks after being charged and appearing in U.S. District Court in May 2020. In order to further his ruse, Staveley left suicide notes with associates and left his wallet in his unlocked car that he parked along the ocean in Massachusetts. Further investigation determined that between May 26 and July 23, 2020, Staveley traveled to various states using false identities and stolen license plates. He was apprehended by the United States Marshals Service in Alpharetta, GA, on July 23, 2020.

Staveley and David Butziger conspired to file four fraudulent CARES Act PPP forgivable loan applications with a Rhode Island bank, falsely claiming they owned businesses with large monthly payrolls when, in fact, they did not own the businesses. Staveley admitted that as part of the scheme, he and Butziger filed fraudulent loan applications seeking $185,570 to pay employees at Top of the Bay restaurant in Warwick, RI; $144,050 for Remington House Inn restaurant in Warwick, RI; $108,777 for On The Trax restaurant in Berlin, MA; and $105,381 to pay employees at Dock Wireless, an unincorporated business. Staveley had no ownership interest in Top of the Bay, Remington House Inn, or On The Trax, which were closed at the time the loan applications were submitted and remain closed. Dock Wireless had no employees and no wages were ever paid by the business.

Source: *USAO District of Rhode Island.*

Responsible Agencies: *FDIC OIG, FBI, IRS-CI, and SBA OIG. Prosecuted by USAO, District of Rhode Island.*

***

Learn more about the FDIC OIG at www.fdicoig.gov or follow us on Twitter at FDIC_OIG.

Office of Inspector General
Federal Housing Finance Agency

The Federal Housing Finance Agency (FHFA) Office of Inspector General (OIG) conducts audits, evaluations, investigations, and other activities relating to the programs and operations of FHFA. OIG promotes economy, efficiency, effectiveness, ethics, and equity and helps protect FHFA and the entities it regulates against fraud, waste, and abuse, contributing to the liquidity and stability of the nation's housing finance system.

Background

Established by the Housing and Economic Recovery Act of 2008 (HERA), FHFA supervises and regulates: the Federal National Mortgage Association (Fannie Mae); the Federal Home Loan Mortgage Corporation (Freddie Mac) (together, the Enterprises); Common Securitization Solutions, LLC (CSS, an affiliate of each Enterprise); and the Federal Home Loan Bank System – which includes 11 Federal Home Loan Banks (FHLBanks) and the Office of Finance. FHFA's mission is to ensure that Fannie Mae, Freddie Mac, the FHLBanks (collectively, the regulated entities), and any entity-affiliated party operate in a safe and sound manner so that they serve as a reliable source of liquidity and funding for housing finance and community investment through the economic cycle. For the first quarter of 2022, the Enterprises collectively reported more than $7.3 trillion in assets and the FHLBanks reported more than $762 billion in assets.

Since September 2008, FHFA has also served as conservator of the Enterprises. The Agency's dual roles as supervisor for the Enterprises and the FHLBanks and as conservator of the Enterprises present unique challenges for OIG. Consequently, OIG structures its oversight program to rigorously examine FHFA's exercise of its dual responsibilities, which differ significantly from the typical federal financial regulator.

We outline our fiscal year priorities in an Annual Plan. On an annual basis, we also assess and report to the FHFA Director FHFA's most serious management and performance challenges which, if not addressed, could adversely affect FHFA's accomplishment of its mission. We focus much of our oversight activities on identifying vulnerabilities in these areas and recommending positive, meaningful actions that the Agency could take to mitigate these risks and remediate identified deficiencies. The management and performance challenges are:

Supervision of the Regulated Entities

As HERA recognizes, FHFA's supervision of the Enterprises is of paramount importance to their safe and sound operation. History has shown that a precipitous decline in the Enterprises' safety and soundness contributed to a severe crisis in the national economy and required nearly $200 billion in taxpayer support to keep them afloat. For these reasons, we have deemed FHFA's supervision of the Enterprises – via the Agency's Division of Enterprise Regulation (DER) – to be one of four critical risks on which we have focused our oversight efforts. We have issued multiple reports which, taken collectively, detailed numerous deficiencies in the supervision program itself, as well as in its execution.

Notable Report: FHFA Must Resolve the Conflicts in its Guidance for Examinations of the Enterprises to Meet its Commitment to Develop and Maintain a World Class Supervision Program (OIG-2021-003, September 1, 2021)

In prior reports, we found that FHFA's guidance for examination of the Enterprises was far more flexible and less prescriptive than the guidance of other federal financial regulators. As a result of that substantial flexibility, we reported that examiners in the Agency's Division of Enterprise Regulation (DER) have significant discretion in conducting examinations, which has resulted in inconsistent examination practices. In a 2019 evaluation (EVL-2019-003, Sept. 10, 2019), we found that FHFA had not finalized many of its supplemental examination modules for examinations of the Enterprises and that many of them remained in "field test" status for more than five years. We recommended, and FHFA agreed, that FHFA establish and communicate clear expectations for use of revised and new examination modules by DER examiners. DER's failure to implement this recommendation was the basis for this management advisory.

According to DER, its 2020 Operating Procedures Bulletin (OPB) on targeted examinations implemented our 2019 recommendation and was intended to foster greater consistency in the application of examination standards across the examination teams. In fact, the 2020 OPB vested significant discretion in DER examiners to structure their examination procedures and failed to establish clearer expectations for examiners than the guidance in place in September 2019. DER adopted an Enterprise-specific Examination Manual that contained more prescriptive guidance in its Examination Work Programs than the corresponding language in the OPB, but it considered the less specific language in the OPB to control. FHFA agreed with our recommendations that it (1) revise the 2020 OPB to establish specific guidance with respect to the circumstances under which DER expects examiners to follow examination procedures in the Work Programs, and (2) align the guidance in the governing OPB with the guidance in the Work Programs.

Conservator Operations

As conservator, FHFA is vested with express authority under HERA to operate the Enterprises, including expansive authority over trillions of dollars in assets and billions of dollars in revenue. FHFA also makes business and policy decisions that influence the entire mortgage finance industry. Given the taxpayers' enormous investment in the Enterprises, the conservatorships' unknown duration, the Enterprises' critical role in the secondary mortgage market, and their unknown ability to sustain future profitability, OIG determined that FHFA's administration of the conservatorships has been, and continues to be, a critical risk. For reasons of efficiency, concordant goals with the Enterprises, and operational savings, FHFA has delegated authority for general corporate governance and day-to-day matters to the Enterprises' boards of directors and executive management. FHFA, as conservator, delegated to each Enterprise's board of directors a significant portion of day-to-day management and risk controls responsibilities. FHFA's regulations also authorize the boards to delegate execution of day-to-day operations to Enterprise employees. As conservator, FHFA has retained authority to decide specific issues and can, at any time, revoke previously delegated authority.

Notable Report: Oversight of Multifamily Borrowers' Compliance with CARES Act and Freddie Mac Tenant Protections and Freddie Mac's Response to the Potential Financial Impact of COVID-19 **(OIG-2022-003, March 24, 2022)**

In March 2020, the onset of the COVID-19 pandemic prompted Congress, FHFA, and Freddie Mac to act to protect the interests of tenants in multifamily properties financed by federally backed multifamily mortgage loans. Congress enacted the Coronavirus Aid, Relief, and Economic Security Act (CARES Act), which imposed a 120-day moratorium that prohibited all borrowers with federally backed multifamily loans from filing legal actions to recover possession of a covered dwelling unit from a tenant solely due to the nonpayment of rent or other fees or charges. Freddie Mac's forbearance program also provided tenants with protection against eviction during the forbearance period (a temporary period during which a mortgage borrower may pause mortgage payments); required multifamily borrowers in forbearance to notify eligible tenants in writing and inform them of the available protections; and required those borrowers to allow tenants to pay back missed rent payments over a "reasonable time," rather than in one lump-sum payment at the end of the forbearance period.

We undertook this special project, in part, to determine how Freddie Mac monitored multifamily servicers' and borrowers' compliance with the CARES Act's and Freddie Mac's forbearance program tenant protections. We concluded that Freddie Mac did not actively monitor its borrowers' compliance with the tenant protections of the CARES Act or its forbearance agreements. Freddie Mac stated that it does not have the authority or ability to directly enforce the CARES Act and it relies on servicers to administer its forbearance agreements. FHFA shared this view. Freddie Mac also relies on its servicers to conduct the investigations into allegations of borrower noncompliance with the CARES Act or its forbearance agreements. Freddie Mac emphasized that borrowers are obligated under the loan documents to comply with applicable law. In limited circumstances, borrowers are required to supply certifications of their compliance and servicers collect them on Freddie Mac's behalf. Freddie Mac asserted that it plans to audit the servicers' processes for doing so.

We also undertook this special project to assess how Freddie Mac forecasts evictions and estimates their potential financial impact on the Enterprise and its lender counterparties. Freddie Mac explained that it does not forecast evictions directly because of the limited amount of data. Instead, it prepares forecasts using third-party occupancy and vacancy data, which incorporate evictions, to assess the strengths and weaknesses of the multifamily market, and Freddie Mac monitors its multifamily properties' income and vacancy levels through financial reports. As part of its risk management, Freddie Mac temporarily imposed debt service reserve requirements on borrowers for certain loans to ensure that they had funds available to make principal (if applicable) and interest payments should the property experience economic stress due to the pandemic. Freddie Mac also increased its multifamily loan loss reserves during 2020. FHFA stated that it is confident that Freddie Mac's multifamily portfolio is "not seeing significant credit risk at this time."

Information Security

FHFA's regulated entities are central components of the U.S. financial system and are interconnected with other large financial institutions. As part of their processes to guarantee or purchase mortgage loans, the Enterprises receive, store, and transmit highly sensitive private information about borrowers, including financial data and personally identifiable information. Both the Enterprises and the FHLBanks have been the targets of cyber attacks.

Cybersecurity is also a pressing concern for the federal government. FHFA has computer networks that are part of the nation's critical financial infrastructure, and FHFA is required to design information security programs to protect them. Computer networks maintained by federal government agencies have been proven to be a tempting target for disgruntled employees, hackers, and other intruders. Over the past few years, cyber attacks against federal agencies have increased in frequency and severity. As cyber attacks continue to evolve and become more sophisticated and harder to detect, they pose an ongoing challenge for virtually every federal agency.

Notable Report: FHFA Did Not Record, Track, or Report All Security Incidents to US-CERT; 38% of Sampled FHFA Users Did Not Report a Suspicious Phone Call Made to Test User Awareness of its Rules of Behavior (AUD-2021-009, June 25, 2021)

The Federal Information Security Modernization Act of 2014 defines "incident" as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies." We conducted this audit to assess FHFA's incident detection and response controls during Fiscal Years 2019 and 2020 against standards and guidelines established by FHFA and the federal government. While FHFA established and maintained an Incident Response Plan and used its Security Information and Event Management tool, we found that it did not record, track, or report all security incidents to the United States Computer Emergency Readiness Team (US-CERT) or contemporaneously document the results of a table-top exercise of those controls. In addition, 38% of sampled FHFA users did not report a suspicious phone call we made to test user compliance with a reporting requirement in FHFA's Rules of Behavior. To address the identified shortcomings, we recommended that FHFA: (1) develop and implement written procedures that define: (a) the pertinent information that needs to be recorded, tracked, and reported for all security incidents and (b) the controls to ensure the accuracy and completeness of the security incident records; (2) ensure that minutes documenting future incident response tabletop exercises are prepared timely; and (3) continue to emphasize to employees and contractors the need to report suspicious activities, including phone calls, to the Help Desk in accordance with FHFA's Rules of Behavior. FHFA disagreed with our first recommendation and it was closed as rejected. FHFA agreed with our second and third recommendations.

Counterparties and Third Parties

The Enterprises rely on institutional counterparties such as sellers and servicers, mortgage insurers, clearinghouses, and other counterparties to provide services that are critical to their business. By doing so, they must account for and mitigate potential counterparty credit risk, which is the risk associated with the inability or failure of a counterparty to meet its contractual obligations. The Enterprises and FHFA recognize that such risk is significant. If an institutional counterparty defaults on its obligations, it could negatively impact an Enterprise's ability to operate. Our criminal investigations include alleged fraud by different types of counterparties, including real estate brokers and agents, builders and developers, loan officers and mortgage brokers, and title and escrow companies. The Enterprises and FHFA also recognize that third parties that provide operational support for a wide array of professional services could also negatively impact an Enterprise's ability to operate. FHFA lacks the statutory authority to directly examine the Enterprises' counterparties and third parties, so it has communicated to the Enterprises its expectations of their oversight of those entities.

Notable Report: FHFA's Division of Enterprise Regulation Did Not Follow or Train to its Procedures for Information Sharing of Enterprise Counterparty Performance Issues (AUD-2021-014, September 28, 2021)

In the course of their operations, the Enterprises rely on counterparties to provide services that are critical to their business such as mortgage servicing, mortgage insurance, single-family mortgage-backed security issuance and administration, and technology functions. FHFA's DER, in support of its supervisory activities, issued an OPB in August 2013 titled *Information Sharing of Counterparty Performance Issues*; that same OPB was reissued in February 2020 without content change. This OPB sets forth the expectations and establishes the protocol to follow regarding when critical information about one Enterprise is to be shared, how it is to be shared, and what the responsibilities of the examination team(s) will be upon receipt of the information, including documentation requirements. We conducted this audit to determine whether DER followed its guidance when a counterparty performance issue was identified at an Enterprise. We found that DER did not follow the procedures in the OPB when it shared information on counterparty performance issues; DER officials told us while examiners had shared such information, they were unaware of the OPB and had not been trained to it. Further, adherence to the OPB and its reissuance in February 2020 was not subjected to DER's quality control process. We also found that FHFA's Office of General Counsel was reviewing the OPB for possible recasting as an Agency-wide policy and procedures document for information sharing of counterparty performance issues. FHFA agreed with our recommendations that it expedite the recasting of DER's OPB on information sharing of counterparty performance issues as an Agency-wide policy and procedure document, and ensure that the OPB was implemented with proper training.

OIG Investigative Accomplishments

OIG's investigative mission is to prevent and detect fraud, waste, and abuse in the programs and operations of FHFA and its regulated entities. OIG's Office of Investigations (OI) executes its mission by investigating allegations of significant criminal and civil wrongdoing that affect the Agency and its regulated entities. OI's investigations are conducted in accordance with professional guidelines established by the Attorney General of the United States and CIGIE's *Quality Standards for Investigations*.

OI is comprised of highly-trained law enforcement officers, investigative counsels, analysts, and attorney advisors. We maximize the impact of our criminal and civil law enforcement efforts by working closely with federal, state, and local law enforcement agencies nationwide.

OI is the primary federal law enforcement organization that specializes in deterring and detecting fraud perpetrated against the Enterprises. OI also investigates cases involving the 11 regional FHLBanks and, in some instances, cases involving banks that are members of the FHLBanks.

Notable Criminal Cases

Business Owner Sentenced to Over 12 Years in Prison in Real Estate Fraud Scheme, California

On August 2, 2021, in the Central District of California, Patrick Soria was sentenced to 152 months in prison and three years supervised release for orchestrating a real estate fraud scheme that victimized more than 2,000 homeowners, involved fraudulent filings that affected the title to properties across the country, and caused more than $7 million in losses. Soria had previously pleaded guilty to conspiracy to commit wire fraud and contempt of court.

According to court documents, Soria stole money from homeowners and prospective home buyers and also victimized numerous lenders through a two-pronged fraud scheme. Soria owned and operated a business using various company names. Participants in the scheme identified properties with mortgage liens on the title, the owners of those properties, and potential purchasers. Soria and others would market properties for sale as though one of the Soria-controlled business entities held title to the properties when, in fact, neither Soria nor a Soria-controlled business entity had any ownership interest in the properties or any claim to or right, title, or interest in the mortgage loan securing the property. Rather, Soria and others had filed fraudulent documents on the title to the properties to create the false appearance that Soria-controlled business entities held title. Soria and others in this way would take over title through fictitious filings. Soria never owned the homes, and he instead used the victims' "purchase" money for his own personal expenses, including escort services, stays at luxury hotels, and Bentley and Lamborghini car rentals.

Soria also marketed loan relief and modification services to owner-borrower victims. Soria and others would communicate to victims that an attempt would be made with their lender to renegotiate their mortgage and if renegotiation was not possible, Soria and one of his business entities would take over the loans from the victims' lenders. After the victims would execute paperwork provided by Soria and others, mortgage payments would be made to Soria-controlled business entities. Soria lulled victims into doing nothing to protect themselves when they started receiving foreclosure and eviction notices. Many homeowners targeted in the scheme lost their homes. Soria, his business entities, or conspirators had no lawful interest in any of these mortgage loans or the right to collect mortgage payments.

The Enterprises were investors in several loans associated with this scheme.

Eight Conspirators Sentenced in Large Scale Multimillion-Dollar COVID Relief Fraud Scheme; Three Become Fugitives, California

On June 25, 2021, a federal jury in the Central District of California convicted four conspirators for a scheme, involving eight participants, where more than 150 fraudulent loan applications were submitted seeking nearly $22 million in COVID relief funds through the Paycheck Protection Program (PPP) and Economic Injury Disaster (EIDL) Relief Program under the CARES Act. According to the evidence presented at trial, the defendants used fictitious, stolen, or synthetic identities to submit fraudulent applications for PPP and EIDL loans. Prior to the trial, four other scheme participants pleaded guilty to criminal charges in the case. In support of these applications, the defendants also submitted false and fictitious documents to lenders and the SBA, including fabricated identity documents, tax documents, and payroll records. Several FHLBank member banks were targets of the fraudulent applications.

The conspirators obtained more than $18 million in COVID relief funds. The defendants then used the fraudulently obtained loan proceeds for down payments on luxury homes. They also used the illicit funds to buy gold coins, diamonds, jewelry, luxury watches, fine imported furnishings, designer handbags, clothing, and a Harley-Davidson motorcycle.

From September 2021 through January 2022, the scheme participants were sentenced to the following:

- Richard Ayvazyan, fraud ringleader (Fugitive) - 17 years in prison, five years supervised release, and ordered to pay over $17 million in restitution, jointly and severally.

- Marietta Terabelian (Fugitive) - 72 months in prison, five years supervised release, and ordered to pay over $17 million in restitution, jointly and severally.
- Tamara Dadyan (Fugitive) - 130 months in prison, five years supervised release, and ordered to pay over $17 million in restitution, jointly and severally.
- Artur Ayvazyan - 60 months in prison, five years supervised release, and ordered to pay over $17 million in restitution, jointly and severally.
- Vahe Dadyan - One year and a day in prison, three years supervised release, and ordered to pay over $10 million in restitution.
- Manuk Grigoryan - 72 months in prison, four years supervised release, and ordered to pay over $2.6 million in restitution.
- Edvard Paronyan - 30 months in prison, three years supervised release, and ordered to pay $430,177 in restitution.
- Arman Hayrapetyan - Ten months of probation, including seven and one-half months of home confinement.

After being convicted Richard Ayvazyan and Marietta Terabelian removed their bracelet monitors and absconded. It was revealed that the husband and wife left their three teenage children to be cared for by their grandparents along with a typewritten letter explaining they had to flee. Further, Richard Ayvazyan's sister in-law, Tamara Dadyan, who pleaded guilty for her role in the scheme, failed to appear to serve her sentence and became a fugitive.

In February 2022, Ayvazyan, Terabelian, and Dadyan were arrested in Montenegro. Extradition is being sought.

Former President of First Mortgage Company Sentenced to Serve 104 Months in Federal Prison and Pay More than $51.8 Million in Restitution to Victims, Oklahoma

On November 29, 2021, in the Western District of Oklahoma, Ronald McCord was sentenced to 104 months in prison, three years supervised release, and ordered to pay over $51 million in restitution, including over $8.5 million to Fannie Mae, and over $28 million in forfeiture for his role in defrauding two FHLBank member banks, Fannie Mae, and others. McCord had previously pleaded guilty to bank fraud, making a false statement to a financial institution, and money laundering.

McCord was the former President of First Mortgage Company, LLC, an Oklahoma City-based mortgage lending and loan servicing company. McCord defrauded two FHLBank member banks, Spirit Bank and Citizens State Bank, and their residential mortgage subsidiaries. According to court documentation, McCord defrauded Spirit and Citizens by misusing lines of credit, as well as selling loans funded by the banks, many to Fannie Mae, without paying off the lines of credit, leaving the Spirit and Citizens banks' debts out of trust.

Additionally, McCord defrauded Fannie Mae by diverting escrow monies intended to pay homeowners' taxes, insurance, principal, and interest, to cover First Mortgage's operating expenses. As a result, First Mortgage lacked sufficient funds to pay borrowers' real estate tax payments. McCord also used the diverted escrow monies to write himself checks as well as to pay more than half the purchase price of his son's nearly $1 million home and build himself a custom vacation home in Colorado.

Business Owner Sentenced in Decade-Long $60 Million Fraud Scheme, New Jersey

On March 30, 2022, in the District of New Jersey, Seth Levine was sentenced to 97 months in prison, five years supervised release, and ordered to pay $65 million in forfeiture for orchestrating long-running bank fraud and securities fraud schemes, which exposed the Enterprises to significant risk and led to large-scale losses for financial institutions and investors. Levine previously pleaded guilty to conspiracy to commit bank fraud, and securities fraud.

According to court documentation, Levine, founding partner, owner, and managing member of Norse Holdings, directed a scheme to fraudulently refinance multifamily properties by providing materially false information to financial institutions about the rents collected, the number of apartments leased, the expenses, and the true owners of the properties. Levine and others provided lenders fabricated documents, including falsified leases that created the appearance that vacant spaces were occupied and that overstated the rent paid by tenants; false personal financial statements; and fictitious expense documents and operating agreements that misrepresented ownership interests in the multifamily properties. Levine also forged signatures on some of the fraudulent documents. The fraudulent refinances resulted in cash payouts from the lenders, which Levine and others used for their own enrichment and to continue the fraud scheme.

Levine also defrauded investors by soliciting investments used to purchase the multifamily properties based on false statements. After the properties were acquired, Levine sold off portions of his ownership interests, brought in additional investors, and refinanced the properties without the investors' consent.

Many of the approved mortgages based on the false statements were sold to the Enterprises. Since the refinances were obtained with fraudulent data regarding the properties' income and expenses, the multifamily properties were overvalued and rents and other income from the properties did not cover the mortgage payments and other expenses associated with the properties. To cover the shortfalls, Levine obtained additional cash-out refinances or additional investors, thereby increasing his total debt incurred. In total, Levine controlled at least 70 multifamily properties, comprising approximately 2,500 apartments.

At the time the fraud was discovered, the outstanding balance of the fraudulently obtained mortgages on the multifamily properties was more than $150 million, including 40 mortgages held by Freddie Mac with an outstanding loan balance of approximately $103 million. The bank fraud conspiracy resulted in losses to victim lenders of at least $47 million.

Business Owner Sentenced in Connection with Obtaining More Than $6 Million in COVID Relief Fraud Scheme, Georgia

On January 4, 2022, in the Northern District of Georgia, Hunter VanPelt was sentenced to 41 months in prison, five years supervised release, and ordered to pay over $7 million in restitution and more than $2 million in forfeiture for a fraud scheme. Multiple FHLBank member banks were targets in the scheme that resulted in more than $6 million in PPP loans being disbursed. VanPelt previously pleaded guilty to bank fraud.

According to court documentation, VanPelt, aka Ellen Corkum, submitted six fraudulent PPP loan applications, using both names, for VanPelt owned or controlled business entities seeking over $7.9 million in total. Over $6 million was disbursed to VanPelt; $2.1 million of the fraudulent proceeds was seized from VanPelt.

Office of Inspector General
U.S. Department of Housing and Urban Development

The U.S. Department of Housing and Urban Development (HUD), Office of Inspector General (OIG), safeguards HUD's programs from fraud, waste, and abuse and identifies opportunities for HUD programs to progress and succeed.

Background

HUD's mission is to create strong, sustainable, inclusive communities and quality affordable homes for all. HUD is working to strengthen the housing market to bolster the economy and protect consumers; meet the need for quality affordable rental homes; use housing as a platform for improving quality of life; and build inclusive and sustainable communities free from discrimination. Its programs are funded through roughly $60 billion in annual congressional appropriations. While organizationally located within HUD, HUD OIG provides independent oversight of HUD programs and operations.

HUD has two component entities that have a major impact on the Nation's financial system: the Federal Housing Administration (FHA) and the Government National Mortgage Association (Ginnie Mae). As one of the largest providers of mortgage insurance in the world, FHA provides lenders with protection against losses when homeowners and owners of multifamily properties and healthcare facilities default on their loans. FHA has insured more than 50.8 million single-family and roughly 68,000 multifamily and healthcare facility mortgages since its inception in 1934. FHA reported that in fiscal year 2021 it helped 716,000 single-family home buyers purchase a home using an FHA-insured mortgage, made over 400 new insurance commitments for residential care facilities and hospitals, and insured more than 1,500 multifamily mortgages. As of December 2021, FHA had a combined insurance portfolio valued at $1.4 trillion.[2] FHA receives limited congressional funding and is primarily self-funded through mortgage insurance premiums.

Ginnie Mae is a self-financing, U.S. Government corporation in HUD. It approves lenders (known to Ginnie Mae as issuers) to issue mortgage-backed securities (MBS) secured by pools of government-backed home loans. These loans are insured or guaranteed by FHA, HUD's Office of Public and Indian Housing (PIH), the U.S. Department of Veterans Affairs (VA), and the U.S. Department of Agriculture. Ginnie Mae guarantees investors the timely payment of principal and interest on MBS backed by the full faith and credit of the United States government. If an issuer of an MBS fails to make the required pass-through payment of principal and interest to investors, Ginnie Mae is required to advance the payment as part of its guarantee and, in the instances of issuer default, will assume control of the issuer's MBS pools and the servicing of the loans in those pools. The purchasing, packaging, and reselling of mortgages in a security form frees up funds that lenders use to originate more loans. In fiscal year 2021, Ginnie Mae issued nearly $934 billion MBSs, pushing the total MBS outstanding to over $2.17 trillion.

2 https://www.hud.gov/sites/dfiles/Housing/documents/FHAFY2021ANNUALMGMNTRPT.pdf

HUD OIG Oversight Relating to Financial Matters

HUD OIG strives to influence positive outcomes for HUD programs and operations through timely and relevant oversight, while safeguarding HUD's programs from fraud, waste, and abuse. HUD OIG's oversight efforts focus on identifying and addressing HUD's most significant management challenges, including through our Top Management Challenges for Fiscal Year 2022 report.[3] Some of the top challenges that HUD faces are affected by the pandemic and HUD's relief programs and funds. Ultimately, HUD OIG uses the top challenges we identified to drive our oversight efforts, including in the following areas most related to the financial sector:

Mitigating Counterparty Risks in Mortgage Programs – Through FHA and Ginnie Mae, HUD supports sustainable homeownership and encouraging investment in affordable rental housing. It does so through a two-pronged approach: by insuring mortgage loans lenders provide to traditionally underserved home buyers and to owners of various affordable rental housing and by guaranteeing payments to investors who purchase securities collateralized by government-insured loans, providing liquidity in this market. HUD must continue to take steps to address counterparty risks faced by FHA and Ginnie Mae to protect taxpayer funds.

Fraud Risk Management - Beyond the monetary loss of taxpayer funds, fraud against HUD's programs negatively impacts the most vulnerable populations with critical housing needs. Dollars lost to fraud are dollars that cannot assist those in need, and ineligible participants take spots away from others who need access. HUD is challenged to use all available tools, such as training, outreach, monitoring, and enterprise risk management, to safeguard its program funds from fraud, especially in light of the billions of dollars to provide housing to those impacted by the pandemic. HUD also faces challenges in protecting its programs and limited funds and resources from fraud through risk assessments and improper payment reviews.

Sustaining Progress in Financial Management - HUD sustained progress during FY 2021 in addressing its remaining financial management weaknesses. However, several weaknesses in HUD's internal control framework and its financial management systems remain. HUD needs to be able to continue sustaining the improvements it has made in financial management so that HUD and its components can operate at a level that will consistently produce reliable and timely financial reports and ensure continuity during challenging times, such as those brought on by the COVID-19 pandemic.

Recent HUD OIG Oversight Related to the Financial Sector

During the 1-year period ending March 31, 2022, HUD OIG issued 41 audits, evaluations, and other reviews to strengthen the programs and operations of HUD. Key oversight reports and investigations related the broader financial sector are summarized below.

FHA Borrowers Did Not Always Properly Receive COVID-19 Forbearances From Their Loan Servicers[4]

The Coronavirus Aid, Relief, and Economic Security Act (CARES Act) provided a mortgage payment forbearance option for all borrowers who suffered a financial hardship due to the COVID-19 national emergency. We audited FHA's oversight of this COVID-19 forbearance option. Several media reports and complaints filed with the Consumer Finance Protection Bureau indicated instances when servicers did not properly administer or offer COVID-19 forbearance. In addition, OIG's Office of Evaluation previously identified issues with the forbearance information

3 Top Management Challenges Facing the U.S. Department of Housing and Urban Development for Fiscal Year 2022, issued Nov. 12, 2021 (available at https://www.hudoig.gov/sites/default/files/2021-11/Top%20Management%20Challenges%20Facing%20HUD%20in%20FY%202022_0.pdf)

4 HUD OIG Audit Report 2022-KC-0001, issued Dec. 15, 2021 (available at: https://hudoig.gov/reports-publications/report/fha-borrowers-did-not-always-properly-receive-covid-19-forbearances)

available on servicers' websites.[5] Our audit aimed to determine whether FHA-insured borrowers properly received the COVID-19- related forbearance.

We found that borrowers were not always made aware of their right to a COVID-19 forbearance under the CARES Act. Based on a statistical sample, at least one-third of the nearly 335,000 borrowers who were delinquent on their FHA-insured loans and not on forbearance in November 2020, were either not informed or misinformed about the COVID-19 forbearance. As a result, any of these borrowers experiencing a hardship due to COVID-19 did not benefit from the COVID-19 forbearance. Further, we found that servicers did not always properly administer the COVID-19 forbearance. Based on a statistical sample, servicers improperly administered the forbearance for at least one-sixth of the nearly 815,000 borrowers on forbearance plans in November 2020, with the most common errors being unnecessary document requirements, improper periods for forbearance, and credit reporting. Servicers also performed excessive communication and collection efforts for borrowers who were already in forbearance. As a result, these borrowers experienced additional burdens from improperly administered forbearance.

We recommended that FHA identify borrowers who are delinquent and did not fully benefit from the COVID-19 forbearance and ensure that information about the CARES Act and COVID-19 forbearance is distributed to these borrowers. Notably, FHA issued letters to delinquent borrowers in June 2021 informing them about the COVID-19 forbearance. We also recommended that FHA review the 21 loans in our statistical sample with improperly administered forbearance to ensure that the borrowers were assisted by the servicers, if possible, and ensure that these servicers updated their forbearance procedures to prevent future noncompliance; ensure that the issues found during our audit are incorporated into servicing monitoring reviews to deter future noncompliance and prevent potential loss to the FHA fund; and provide additional guidance to the servicers so that they limit their communication and collection efforts for the borrowers in forbearance.

Delays in FHA Catalyst's Development[6]

In March 2021, HUD OIG became aware of potential project changes and shifting schedules on FHA Catalyst. FHA Catalyst is FHA's IT modernization initiative, and is the foundation on which FHA will plan to use new and innovative ways to fulfill its mission throughout its technology transformation. In response to these concerns, OIG evaluated (1) why HUD paused work on the FHA Catalyst, (2) what caused that pause, (3) whether and to what extent HUD is back working on FHA Catalyst, and (4) the revised dates for completion of FHA Catalyst.

Our evaluation found that in February 2021, the Office of the Chief Information Officer (OCIO) identified funding risks with the development contract under which HUD contracted for FHA Catalyst's development. In response, HUD officials took steps to slow FHA Catalyst spending on the contract while awaiting approval for additional contract funds. Despite efforts to slow project spending, it was not enough to prevent funding shortfalls before the contract's base year end. Poor contract oversight enabled OCIO to exhaust funds before the end of the base year, which stopped work on FHA Catalyst. Additionally, several issues hindered FHA Catalyst development activities. As of August 2021, HUD had resumed FHA Catalyst development work at limited capacity. As of October 2021, HUD estimated that it would complete FHA Catalyst development in March 2025, which is later than originally planned.

Approximately 31,500 FHA-Insured Loans Did Not Maintain the Required Flood Insurance Coverage in 2020[7]

In March 2022, we issued an audit of FHA-insured loans serviced in calendar year 2020 to determine whether borrowers maintained proper flood insurance coverage. FHA's current rules regarding the requirement to maintain

5 Evaluation Memorandum, Some Mortgage Loan Servicers' Websites Offer Information about CARES Act Loan Forbearance That Is Incomplete, Inconsistent, Dated, and Unclear, issued April 27, 2020 (available at: https://www.hudoig.gov/sites/default/files/2020-04/Single%20Family%20Mortgage%20Forbearance%20Brief.pdf); Evaluation Memorandum, Some Mortgage Loan Servicers' Websites Continue To Offer Information about CARES Act Loan Forbearance That Could Mislead or Confuse Borrowers, or Provide Little or no Information at all, issued September 30, 2020 (available at: https://www.hudoig.gov/sites/default/files/2020-10/Single%20Family%20Mortgage%20Forbearance.pdf)

6 HUD OIG Evaluation Report 2021-OE-0003a, issued November 77, 2021 (available at: https://www.hudoig.gov/reports-publications/memorandum/delays-federal-housing-administration-catalysts-development)

7 HUD OIG Audit Report 2022-KC-0002, issued March 22, 2022 (available at: https://www.hudoig.gov/reports-publications/report/approximately-31500-fha-insured-loans-did-not-maintain-required-flood)

flood insurance coverage on property located in an SFHA do not permit private flood insurance as an option to satisfy purchase requirement. We compared location data from FHA-insured loans to Federal Emergency Management Agency flood maps to identify a targeted universe of properties that appeared to be located in special flood hazard areas (SFHA).

We found FHA insurance remained outstanding on an estimated 31,500 loans for properties in SFHA flood zones that did not have the required flood insurance during calendar year 2020. We found loans that had private flood insurance instead of the required NFIP coverage, NFIP coverage that did not meet the minimum required amount, or no coverage during calendar year 2020. This condition occurred because FHA did not have adequate controls to detect loans that did not maintain the required flood insurance and its handbooks did not adequately guide servicers on the flood insurance requirements. As a result, the FHA insurance fund was potentially exposed to greater risk from at least $4.5 billion in loans that did not maintain adequate NFIP coverage.

As a result, we recommended that FHA take steps to address the 21 loans in our statistical sample that appeared to not have appropriate flood insurance coverage, develop a control to detect loans that did not maintain the required flood insurance to avoid potential future costs to the FHA insurance fund from inadequately insured properties, and consult with HUD's Office of General Counsel to review the language in the statutes, regulations, and handbooks and make any necessary adjustments to the forward mortgage and Home Equity Conversation Mortgage handbooks.

COVID-19 Forbearance Data in HUD's Single Family Default Monitoring System Generally Agreed With Information Maintained by Loan Servicers Reviewed[8]

We audited lender reporting of COVID-19 forbearances for FHA- insured loans in the Single Family Default Monitoring System (SFDMS). We compared default reporting data from SFDMS to loan data provided by five sampled servicing lenders that serviced a third of the FHA single-family portfolio. We initiated this audit to determine whether COVID-19 forbearance data available in SFDMS were consistent with the information maintained by loan servicers.

We found that COVID-19 forbearance data available in SFDMS were generally consistent with the information maintained by loan servicers reviewed. Nearly 90 percent of the loans in forbearance, according to the servicer records reviewed, were reported as such by the servicers in SFDMS. The remaining 10 percent of loans in forbearance, according to servicer records but not reported as forbearances in SFDMS, were properly accounted for. In addition, key metrics showed that servicers generally complied with HUD's forbearance reporting requirements.

HUD Did Not Have Adequate Controls in Place to Track, Monitor, and Issue FHA Refunds Owed to Homeowners[9]

We audited HUD oversight of FHA refunds based on a hotline complaint alleging that HUD was trying to make it difficult for claimants to obtain refunds or discourage them from pursuing the refunds, which are due to eligible homeowners from the unearned portion of the upfront mortgage insurance premium paid. Our audit objective was to determine whether HUD appropriately tracked, monitored, and issued FHA refunds due to homeowners of terminated loans.

Our audit revealed that HUD did not have adequate controls in place to ensure that refunds were appropriately tracked, monitored, and issued. Specifically, HUD (1) did not ensure that the homeowner information for at least 23,579 loans with unpaid refunds totaling approximately $15.8 million was included in its public listing of unpaid refunds, (2) did not adequately track the status of refunds, (3) lacked policies and procedures for various stages of the refund process, (4) did not fully implement procedures it developed requiring additional documents from homeowners, and (5) did not follow the requirements of the Paperwork Reduction Act. We found HUD did not emphasize reviewing or monitoring the refund process to identify weaknesses and focused primarily on sending

8 HUD OIG Audit Report 2021-KC-0005, issued Aug. 16, 2021 (available at: https://www.hudoig.gov/reports-publications/report/covid-19-forbearance-data-huds-single-family-default-monitoring-system)

9 HUD OIG Audit Report 2022-LA-0001, issued January 7, 2022 (available at: https://www.hudoig.gov/reports-publications/report/hud-did-not-have-adequate-controls-place-track-monitor-and-issue-fha)

refund applications and issuing refunds to homeowners who returned the applications. As a result, HUD could not ensure that it implemented a consistent refund process, and homeowners and third-party tracers were not able to search for all refunds HUD owed, which may have reduced the chance for homeowners for at least 23,579 loans to obtain approximately $15.8 million in refunds. We made several recommends that HUD develop and improve its policies and processes to improve the FHA refund process.

Investigative Activity and Outcomes

OIG also helps protect HUD from counterparty risk by conducting investigations of alleged fraud negatively affecting the FHA insurance funds and securing recoveries. For the period April 1, 2021, through March 31, 2022, HUD OIG completed 97 single-family investigations of fraud against the FHA insurance fund. Many of the investigations focused on loan origination fraud involving forward mortgages. Recoveries from these cases totaled over $57 million (criminal, civil, and administrative recoveries). For example:

Father and Son Collectively Sentenced to 58 Months Incarceration[10]

A former majority owner of an Alzheimer's assisted living facility, and his son, the facility administrator, were collectively sentenced in U.S. District Court to 58 months incarceration and 4 years supervised release. The assisted living facility was financed with an FHA Section 232-insured loan, which provided a favorable interest rate and did not require the owners of the facility to take personal responsibility for the loan when it went into default. The facility agreed to be bound by a regulatory agreement with HUD that prohibited distributing property funds to an owner when a property is in default or a non-surplus case position. HUD suffered the financial loss when the facility defaulted on the loan and the property went into foreclosure. Instead of paying the loan, and in violation of the regulatory agreement, the two took hundreds of thousands of dollars from the facility. The facility administrator was sentenced in connection with his earlier guilty plea to equity skimming and was ordered to pay $2 million in restitution to HUD. The former majority owner was sentenced in connection with his earlier guilty plea to fraud against HUD and was ordered to pay jointly and severally with the facility administrator more than $3.6 million in restitution to HUD.

Landlord Enters Into $805,000 Settlement Agreement With HUD[11]

The owner of a mixed-use residential and commercial property, entered into a settlement agreement and agreed to pay $805,000 to HUD to resolve allegations that he made improper payments to his family trusts while disregarding his obligation to make payments on the FHA-insured mortgage obtained in 2010 to finance the construction of the property. The owner also submitted a false statement to FHA related to those payments, in violation of the civil equity skimming statute and the Financial Institutions Reform, Recovery, and Enforcement Act of 1989. For more than 2 years, the company stopped paying its mortgage but continued to transfer money to family trusts, causing the mortgage to go into default. To prevent foreclosure, FHA agreed to pay down a substantial portion of the mortgage after the owner falsely stated that, while the mortgage was in default, the company paid to its lender all net cash remaining after project expenses had been paid.

Nine Swindlers Collectively Sentenced to 16 Years Incarceration[12]

Nine individuals – a real estate agent and business owner, two paralegals, several employees of a company, notaries, and a credit repair specialist – were collectively sentenced in Superior Court of California to 16 years incarceration, 10 years probation, 11 years supervised release, and ordered to pay $606,815 restitution to various victims, of which $598,335 was ordered jointly and severally. For over 7 years, the co-conspirators participated in an advance fee mortgage relief scheme that resulted in the foreclosure delays of over 200 properties, impacting 15 FHA-insured mortgages. The co-conspirators submitted false deeds and petitions in support of bankruptcies filed with the courts to delay the foreclosures.

10 https://www.justice.gov/usao-edtx/pr/former-administrator-texarkana-assisted-living-facility-sentenced-federal-violations
11 https://www.justice.gov/usao-ndny/pr/owner-malta-s-ellsworth-commons-agrees-pay-805000-and-permanent-exclusion-federal
12 https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-arrests-and-indictments-alleged-6-million

Real Estate Professionals Sentenced to 48 Months Incarceration

A former real estate broker and owner of a realty company, and a former real estate salesperson and branch manager for a mortgage company, were collectively sentenced in Federal court to 48 months and 1 day incarceration and 6 years supervised release. For more than 2 years, the two individuals orchestrated a short sale scheme by fraudulently misrepresenting borrowers' primary residences as rental properties and inflating the market value of the primary residences on the borrowers' loan applications to obtain FHA-insured or conventional loans for the purchase of new homes. The two individuals then falsely submitted short sale requests for the borrowers' primary residences, based on purported financial hardships, and improperly collected profits, commissions, fees, and kickbacks as part of this scheme. The former real estate salesperson and branch manager was sentenced to bank fraud and was ordered to pay, jointly and severally, with the former real estate broker $253,013 restitution to Freddie Mac and various financial institutions. The former real estate broker was sentenced in connection with his earlier guilty plea to bank fraud and money laundering and was ordered to pay an additional $4,875,691 restitution to Freddie Mac and Fannie Mae.

Former Public Housing Agency Finance Officer Ordered To Pay Nearly $5.3 Million in Restitution[13]

A former finance officer for a public housing authority (PHA) was sentenced in Federal court in connection with her earlier guilty plea to wire fraud. For more than 3 years, the former finance officer used a variety of schemes to embezzle $6.9 million in public money, including by diverting PHA funds in connection with the purchase of land and preparing and submitted false invoices to the PHA by making them appear as if the purchases were from an outside vendor. The former finance officer was sentenced to 51 months incarceration and 3 years supervised release and ordered to pay nearly $5.3 million in restitution, of which more than $4.2 million will be paid to the PHA.

13 https://www.justice.gov/usao-wdwa/pr/former-low-income-housing-executive-sentenced-prison-embezzling-nearly-7-million

Office of Inspector General
National Credit Union Administration

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) promotes the economy, efficiency, and effectiveness of NCUA programs and operations and detects and deters fraud, waste and abuse, thereby supporting the NCUA's mission of providing, through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit.

Agency Overview

The NCUA is responsible for chartering, insuring, and supervising federal credit unions and administering the National Credit Union Share Insurance Fund (Share Insurance Fund). The agency also manages the Operating Fund,[14] the Community Development Revolving Loan Fund,[15] and the Central Liquidity Facility.[16]

Credit unions are member-owned, not-for-profit cooperative financial institutions formed to permit members to save, borrow, and obtain related financial services. NCUA charters and supervises federal credit unions and insures accounts in federal and most state-chartered credit unions across the country through the Share Insurance Fund, a federal fund backed by the full faith and credit of the United States government.

The NCUA's mission is to provide through regulation and supervision, a safe and sound credit union system that promotes confidence in the national system of cooperative credit and its vision is to protect consumer rights and member deposits. The NCUA further states that it is dedicated to upholding the integrity, objectivity, and independence of credit union oversight. The agency implements initiatives designed to meet these goals.

Major NCUA Programs

Supervision

The NCUA supervises credit unions through examinations, regulatory enforcement, providing guidance in regulations and letters, and taking supervisory and administrative actions as necessary.

The agency's Office of National Examinations and Supervision oversees examination and supervision issues related to consumer credit unions with assets greater than $10 billion (a recent proposal would raise this threshold to $15

14 The Operating Fund was created by the Federal Credit Union Act of 1934. It was established as a revolving fund in the United States Treasury under the management of the NCUA Board for the purpose of providing administration and service to the federal credit union system. A significant majority of the Operating Fund's revenue is comprised of operating fees paid by federal credit unions. Each federal credit union is required to pay this fee based on its prior year asset balances and rates set by the NCUA Board.

15 The NCUA's Community Development Revolving Loan Fund, which was established by Congress, makes loans and Technical Assistance Grants to low-income designated credit unions.

16 The Central Liquidity Facility is a mixed-ownership government corporation the purpose of which is to supply emergency loans to member credit unions.

billion) and all corporate credit unions, which provide services to consumer credit unions. Due to the relative size of their insured share base, these very large credit unions are deemed systemically important to the Share Insurance Fund.

In addition to the NCUA's authority, the Consumer Financial Protection Bureau (CFPB) has the authority under the Dodd-Frank Act to examine compliance with certain consumer laws and regulations by credit unions with assets over $10 billion.

Insurance

The NCUA administers the Share Insurance Fund, which is funded by credit unions and provides insurance for deposits held at federally insured credit unions nationwide. The insurance limit is $250,000 per depositor.

Credit Union Resources and Expansion

The NCUA's Office of Credit Union Resources and Expansion (CURE) supports credit union growth and development, including providing support to low-income, minority, and any credit union seeking assistance with chartering, charter conversions, by-law amendments, field of membership expansion requests, and low-income designations. CURE also provides access to online training and resources, grants and loans, and a program for preserving and growing minority institutions.

Consumer Protection

The NCUA's Office of Consumer Financial Protection (OCFP) is responsible for consumer protection in the areas of fair lending examinations, member complaints, and financial literacy. OCFP consults with the CFPB, which has supervisory authority over credit unions with assets of $10 billion or more. CFPB also can request to accompany the NCUA on examinations of other credit unions.

Asset Management

The NCUA's Asset Management and Assistance Center (AMAC) conducts credit union liquidations and management and recovery of assets to minimize costs to the Share Insurance Fund and to credit union members. AMAC assists agency regional offices with the review of large complex loan portfolios and actual or potential bond claims. AMAC also participates extensively in the operational phases of conservatorships and records reconstruction.

Office of Minority and Women Inclusion

The NCUA's Office of Minority and Women Inclusion, in accordance with the Dodd-Frank Act, is responsible for measuring, monitoring, and establishing policies for diversity in the agency's management, employment, and business activities, and with respect to credit unions, excluding the enforcement of statutes, regulations, and executive orders pertaining to civil rights.

Office of Continuity and Security Management

The Office of Continuity and Security Management evaluates and manages security and continuity programs across the NCUA and its regional offices. The office is responsible for continuity of operations, emergency planning and response, critical infrastructure and resource protection, cyber threat and intelligence analysis, insider threats and counterintelligence, facility security, and personnel security.

The NCUA Office of Inspector General

The 1988 amendments to the Inspector General Act of 1978 (IG Act) established IGs in 33 designated federal entities, including the NCUA.[17] The NCUA Inspector General (IG) is appointed by, reports to, and is under the general supervision of a three-member presidentially appointed Board. OIG staff consists of ten employees: the IG, the Deputy IG, the Counsel to the IG/Assistant IG for Investigations, the Director of Investigations, five auditors, and an office manager. The OIG promotes the economy, efficiency, and effectiveness of agency programs and operations, and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of facilitating the availability of credit union services to all eligible consumers through a regulatory environment that fosters a safe and sound credit union system. The OIG supports this mission by conducting independent audits, investigations, and other activities, and by keeping the NCUA Board and the Congress fully and currently informed of its work.

Recent Work

We conducted an audit regarding the NCUA's governance of information technology (IT) initiatives that could be instructive for the broader financial sector. Our audit, which we issued on September 28, 2021, determined that overall, the NCUA had an effective process for identifying, controlling, prioritizing, and implementing IT initiatives. However, we recommended that the NCUA publish policies and procedures that included definitions, roles, responsibilities, and processes for IT governance and selecting, controlling, and evaluating IT investments. We also recommended that the NCUA make clearer the authorities, responsibilities, and functions of its Information Technology Oversight Council (ITOC) and require the ITOC to provide a rated and ranked listing of proposed IT projects to the NCUA Board, highlighting those that are legally required, and provide ITOC meeting minutes to the Board.

We also participated in two CIGFO working groups that worked on the report titled Guidance in Preparing for and Managing Crises, and the audit of FSOC's response to the May 20, 2021, Executive Order on Climate-Related Financial Risk. We also continued to participate in a CIGFO working group designed to coordinate investigative efforts combating fraud associated with CARES Act stimulus programs.

17 5 U.S.C. app. § 8G.

Office of Inspector General U.S. Securities and Exchange Commission

The U.S. Securities and Exchange Commission (SEC or agency) Office of Inspector General (OIG) promotes the integrity, efficiency, and effectiveness of the critical programs and operations of the SEC and operates independently of the agency to help prevent and detect fraud, waste, and abuse in those programs and operations, through audits, evaluations, investigations, and other reviews.

I. Background

The SEC's mission is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation. The SEC strives to promote capital markets that inspire public confidence and provide a diverse array of financial opportunities to retail and institutional investors, entrepreneurs, public companies, and other market participants. Its core values consist of integrity, excellence, accountability, teamwork, fairness, and effectiveness. The SEC's goals are focusing on the long-term interests of Main Street investors; recognizing significant developments and trends in evolving capital markets and adjusting agency efforts to ensure the SEC is effectively allocating its resources; and elevating the SEC's performance by enhancing its analytical capabilities and human capital development.

The SEC is responsible for overseeing the nation's securities markets and certain primary participants, including broker-dealers, investment companies, investment advisers, clearing agencies, transfer agents, credit rating agencies, and securities exchanges, as well as organizations such as the Financial Industry Regulatory Authority, Municipal Securities Rulemaking Board, Public Company Accounting Oversight Board, Securities Investor Protection Corporation, and the Financial Accounting Standard Board. Under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the agency's jurisdiction was expanded to include certain participants in the derivatives markets, private fund advisers, and municipal advisors.

The SEC's headquarters are in Washington, DC, and the agency has 11 regional offices located throughout the country. The agency's functional responsibilities are organized into 6 divisions and 25 offices, and the regional offices are primarily responsible for investigating and litigating potential violations of the securities laws. The regional offices also have examination staff to inspect regulated entities such as investment advisers, investment companies, and broker-dealers. As of March 2022, the SEC employed 4,477 full-time equivalents.

The SEC OIG was established as an independent office within the SEC in 1989 under the Inspector General Act of 1978, as amended (IG Act). The SEC OIG's mission is to promote the integrity, efficiency, and effectiveness of the SEC's critical programs and operations. The SEC OIG prevents and detects fraud, waste, and abuse through audits, evaluations, investigations, and other reviews related to SEC programs and operations.

The SEC OIG Office of Audits conducts, coordinates, and supervises independent audits and evaluations of the SEC's programs and operations at its headquarters and 11 regional offices. These audits and evaluations are based on risk and materiality, known or perceived vulnerabilities and inefficiencies, and information received from the Congress, SEC staff, the U.S. Government Accountability Office, and the public.

The SEC OIG Office of Investigations performs investigations into allegations of criminal, civil, and administrative violations involving SEC programs and operations by SEC employees, contractors, and outside entities. These investigations may result in criminal prosecutions, fines, civil penalties, administrative sanctions, and personnel actions. The Office of Investigations also identifies vulnerabilities, deficiencies, and wrongdoing that could negatively impact the SEC's programs and operations.

In addition to the responsibilities set forth in the IG Act, Section 966 of Dodd-Frank required the SEC OIG to establish a suggestion program for SEC employees. The SEC OIG established its SEC Employee Suggestion Program in September 2010. Under this program, the OIG receives, reviews and considers, and recommends appropriate action with respect to such suggestions or allegations from agency employees for improvements in the SEC's work efficiency, effectiveness, and productivity, and use of its resources, as well as allegations by employees of waste, abuse, misconduct, or mismanagement within the SEC.

II. SEC OIG Work Related to the Broader Financial Sector

In accordance with Section 989E(a)(2)(B)(i) of Dodd-Frank, below is a discussion of the SEC OIG's completed and ongoing work, focusing on issues that may apply to the broader financial sector.

Completed Work

Registered Investment Adviser Examinations: EXAMS Has Made Progress To Assess Risk and Optimize Limited Resources, But Could Further Improve Controls Over Some Processes: Report No. 571; January 25, 2022

Within the SEC's Division of Examinations (EXAMS), the investment adviser/investment company (IA/IC) examination program assesses whether, among other things, registered investment advisers (RIAs) and investment companies comply with federal securities laws. RIAs are among the variety of financial professionals that provide services to help individuals manage their investments. Generally, RIAs include firms or individuals that, for compensation, advise others as to the value of securities, or as to the advisability of investing in, purchasing, or selling securities. RIAs represent the largest portion of the registered firm population overseen by EXAMS, and the majority of EXAMS' examinations are of RIAs.

We conducted this audit to determine whether EXAMS has established effective controls over its RIA examination planning processes to foster compliance with federal securities laws and ensure efficient allocation of its limited RIA examination resources. We also followed up on the implementation of corrective actions in response to recommendations from our 2016 evaluation.

We verified that, in response to two recommendations from the prior OIG evaluation *(Office of Compliance Inspections and Examinations' Management of Investment Adviser Examination Coverage Goals*; OIG Report No. 533; March 10, 2016), EXAMS worked to optimize its limited resources and increase its efficiency and effectiveness, improve its IA/IC examination program's examination candidate selection processes, and implement the U.S. Government Accountability Office's risk-management framework, specifically, within the IA/IC examination program. OIG Report No. 533 noted that, in fiscal year (FY) 2015, the average number of IA/IC examinations completed per examiner was about three. That number nearly doubled in FY 2021. Additionally, in FY 2015, EXAMS met its annual goal of examining 10 percent of RIAs. Notably, the percentage of RIAs examined improved to 15 percent in FY 2020 and 16 percent in FY 2021.

We selected and reviewed a non-statistical, random sample of 501 RIA examinations from the audit universe of 4,993 RIA examinations that were approved and closed between FY 2019 and FY 2021, quarter 2. For each sample item, we tested key examination planning processes and controls and found that, although 23 of 26 operated effectively, controls over the remaining RIA examination planning processes need improvement. For example, for 81 of the 501 RIA examinations we reviewed (or about 16 percent), staff commenced substantive RIA examination procedures before management reviewed and approved key examination planning and scoping processes as part of the examination pre-fieldwork phase. In some cases, staff failed to first request management's approval before commencing substantive examination procedures. In other cases, management failed to provide timely approval when requested. As a result, pre-fieldwork approval—a primary control for ensuring, among other things, that staff execute examinations in accordance with Division policies and procedures—occurred between 1 and 391 days late (or an average of 54 days late) for the 81 RIA examinations in question. Additionally, for 70 of the 501 RIA examinations we reviewed (or about 14 percent), staff either did not (1) ensure the EXAMS system of record included evidence of required communications with examined registrants, or (2) maintain documents in the Communications section of the system, as required. Inconsistent documentation of examination communications may lead to difficulties in reviewing and supervising examinations.

Lastly, we identified a matter that did not warrant a recommendation but was discussed with agency management for their consideration. Specifically, 8 of the 501 examinations we reviewed included non-EXAMS staff participation. However, we were unable to find evidence that an examination supervisor notified registrants of non-EXAMS staff participation for seven of these eight RIA examinations.

We issued our final report on January 25, 2022, and made three recommendations to further strengthen the SEC's IA/IC examination program. Because this report contains nonpublic information about the SEC's examination program, we released a redacted version on our website at https://www.sec.gov/files/Registered-Invst-Adviser-EXAMS-Made-Prog-Assess-Risk-Optimize-Limited-Resources-Could-Further-Imp-Controls-Over-Some-Processes-Rpt-571.pdf.

DERA Staff Research and Publications Support the SEC's Mission, But Related Controls and Agency-wide Communication and Coordination Could Be Improved (Report No. 567); September 17, 2021

Staff from the SEC's Division of Economic and Risk Analysis (DERA) develop and implement novel research on a variety of topics germane to the SEC's mission and publish the results of that research in a wide range of academic and practitioner journals, conference volumes, and scholarly books. Staff may complete research products as part of their official work or during their personal time. According to agency officials, between FY 2018 and FY 2020, DERA staff submitted 116 working papers and items of personal research for review and clearance for public release.

We conducted this evaluation to evaluate the role DERA staff's research and publications—including working papers, academic publications, and other published research—play in furthering the mission of the SEC; and to determine whether effective controls exist to (a) review and approve staff research and publications, and (b) safeguard SEC nonpublic or other sensitive information used for such activities.

DERA provides, among other things, insights from scientific research in support of the SEC's mission, including its rulemaking, enforcement, and examinations functions. As such, management has recognized the importance of staff research and publication activities, and established procedures to address common issues that arise, including issues related to data usage and outside activities. Nonetheless, management can improve its internal control over staff's research and publication activities. Specifically, we found that DERA does not:

- formally track working papers and refereed reports, or how staff research and publications advance a subpart of the SEC's mission;
- review working papers and personal research before staff submit them to the SEC Office of Ethics Counsel for the Office of General Counsel's review and clearance for public release; or

- centrally maintain records related to staff research and publication activities.

Implementing these or similar control activities would provide the organization with greater assurance that it is achieving its objectives in this area and effectively mitigating related risks. Without such control activities, management may not have a complete picture of how organizational resources are used (when applicable), how staff research advances a subpart of the SEC's mission, and whether research is addressing agency needs across mission areas. In addition, management may lack assurance that working papers, personal research, and supporting documents submitted to the SEC's Office of Ethics Counsel and reviewed by the Office of General Counsel are complete, accurate, and ready for review and clearance. Finally, the lack of complete, centralized records could present challenges over time, particularly if key personnel have separated from the agency.

Additionally, to ensure other SEC divisions and offices are aware of research in progress and to obtain information on any relevant rulemaking or pending litigation, DERA e-mails various SEC management and staff a quarterly communication known as *DERA's Research Pipeline*. We surveyed personnel from 13 SEC divisions and offices that received the *Research Pipeline*, and they generally found DERA's research to be useful and an effective recruitment tool for hiring economists. However, a third of respondents felt that DERA could better communicate and coordinate staff research and publication activities. Specifically, we found DERA has not clearly identified and communicated its expectations to other divisions and offices. In addition, DERA has not established controls to ensure (1) all pending staff research and publications are timely listed in *DERA's Research Pipeline* before research is made public; (2) the quarterly e-mails are released timely and consistently; and (3) stakeholders in other divisions or offices have sufficient information to understand the significance of the research that is included. Through improved communication and coordination, SEC divisions and offices could better assess and comment on DERA staff research in progress, thereby better meeting the needs of all divisions and offices, including DERA.

We issued our final report on September 17, 2021, and made four recommendations to further strengthen internal controls over staff research and publications activities, as well as communication and coordination with internal stakeholders. The report is available on our website at https://www.sec.gov/files/DERA-Staff-Research-and-Publications-Support-SECs-Mission-Report-no-567.pdf.

Ongoing Work

Evaluation of the Division of Enforcement's Efforts and Goals To Expedite Investigations

The Division of Enforcement (Enforcement) is critical to the Commission's ability to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. Specifically, Enforcement uncovers misconduct and advances the Commission's mission each year by investigating and bringing hundreds of actions against individuals and entities for fraud and other misconduct, and by securing remedies that protect investors and the markets. As stated in Enforcement's 2020 annual report, "[Enforcement's] actions have the greatest impact when filed as close in time to the conduct as possible."

The SEC OIG has initiated an evaluation to (1) assess Enforcement's efforts to expedite investigations, where possible and appropriate, and (2) review Enforcement's performance goal-setting and monitoring processes related to the pace of investigations. The evaluation scope period will include Enforcement time-to-file data and goal-setting processes covering FYs 2016 through 2021, and associated efforts and actions to meet established goals in accordance with applicable criteria.

We expect to issue a report summarizing our findings during the next reporting period.

Audit of the U.S. Securities and Exchange Commission's Whistleblower Program

FY 2020 marked both the 10-year anniversary of the inception of the SEC's whistleblower program under Dodd-Frank, as well as numerous record-breaking whistleblower program accomplishments in terms of individuals and dollars awarded, claims processed, and tips received. In FY 2020, the SEC processed more claims than in any other year of the program, and the SEC issued the largest number of Final Orders resolving whistleblower award claims in a FY, including both award and denial orders. According to the SEC's public website, this record-breaking trend continued into early FY 2021, when the SEC issued an individual award of $114 million, eclipsing the previous record of $50 million set months prior in FY 2020. Overall, from its inception through the end of FY 2020, the whistleblower program received more than 40,000 tips, and awarded approximately $562 million to 106 individuals.

The SEC OIG has initiated an audit to assess the growth of the SEC's whistleblower program and the functioning of key program controls, such as those for communicating with stakeholders, reviewing information provided by whistleblowers, and determining award amounts.

We expect to issue a report summarizing our findings before the end of FY 2022.

Evaluation of the Office of the Advocate for Small Business Capital Formation

The Office of the Advocate for Small Business Capital Formation (OASB) is a newly established, independent office within the SEC. OASB commenced operations in January 2019 and was established pursuant to the SEC Small Business Advocate Act of 2016 to advance the interests of small businesses and their investors at the SEC and in the capital markets. OASB advocates for small businesses and their investors by conducting outreach to solicit views on relevant capital formation issues, providing assistance to resolve significant problems small businesses may have with the SEC or self-regulatory organizations, analyzing the potential small business impact of proposed regulations and rules, and recommending changes to mitigate capital formation issues and promote the interests of small businesses and their investors.

The SEC OIG has initiated an evaluation to assess the design and implementation of OASB's operations, policies, and controls to include, as applicable, coordination and collaboration with other SEC divisions and offices and external stakeholders, to determine whether OASB has met applicable statutory requirements and strategic goals and objectives.

We expect to issue a report summarizing our findings during the next reporting period.

Special Inspector General for the Troubled Asset Relief Program

The mission of the Office of the Special Inspector General for the Troubled Asset Relief Program (SIGTARP) is to prevent and detect fraud, waste, and abuse in the more than $442 billion appropriated by Congress through the Emergency Economic Stabilization Act (EESA) and $2 billion funded through the Consolidated Appropriations Act of 2016, and to promote economy, efficiency, effectiveness, and accountability in these economic stability programs. SIGTARP conducts investigations of suspected illegal activity in, and independent audits of, these EESA long-term economic stability programs.

Background

EESA has two parts:

(1) Short-term Treasury purchases of "troubled assets," which led to investments in banks, insurance companies and automotive companies - these programs have been largely completed, as has SIGTARP's work in this area; and

(2) Long-term programs intended to bring economic stability to the financial industry and communities by protecting home values and preserving homeownership - programs that spent over $1 billion during fiscal years 2020-2021, and will continue to operate until 2024.

Under these long-term economic stability programs, the Department of Treasury and Fannie Mae (with assistance from Freddie Mac) run a program that funds incentives to more than 150 financial institutions, including some of the largest in our nation, to lower mortgage payments to terms that are affordable and sustainable for homeowners at risk of foreclosure. Treasury also funded grant-like programs administered by housing finance agencies in 19 states. This included assistance for homeowners unemployed, underemployed, or suffering other hardships due to the COVID-19 pandemic.

SIGTARP is primarily a federal law enforcement office. SIGTARP investigations have resulted in criminal charges against 467 defendants with a 96% DOJ conviction rate. Courts have sentenced to prison 315 defendants, including 74 bankers. SIGTARP's investigations have also resulted in DOJ, the SEC, and others bringing enforcement actions against 25 banks or corporations, including some of the largest financial institutions.

More than $11 billion has been recovered from SIGTARP investigations – a cumulative 29 times return on investment. Already in FY 2022, the government has recovered $144,000 with more projected later in the fiscal year.

SIGTARP's Select Audit Results (April 1, 2021 to March 31, 2022)

SIGTARP Announced Three Evaluations, Released Two Evaluation Reports; One Management Advisory. Four Evaluations Pertain to the Home Affordable Modification Program (HAMP)

In October and November 2021, SIGTARP announced three new evaluations examining different aspects of HAMP. For the first two evaluations, SIGTARP will identify key characteristics of homeowners and mortgage servicers in HAMP using Treasury's data and other relevant data sources. For the third evaluation, SIGTARP will review Treasury's oversight of mortgage servicers participating in HAMP. SIGTARP will examine Treasury's oversight of HAMP servicers, as well as oversight conducted on behalf of Treasury by Freddie Mac and Fannie Mae. The results of these evaluations will provide valuable information to Treasury, Congress, and the public on who is currently benefitting from HAMP and the servicers participating in the program, and how federal taxpayer dollars are being used.

In August 2021, SIGTARP released an evaluation report, Treasury's Public Reporting on the Home Affordable Modification Program, which found that although Treasury provides some transparency to the public on HAMP, more transparency is needed on active homeowners in the program and the performance of 118 bank and non-bank mortgage servicers that administer it. This additional transparency would provide greater insight on who is currently benefitting from HAMP and help the public understand the effectiveness of HAMP in achieving its goals to modify mortgages to be affordable and sustainable. The added transparency would also bring more accountability and insight into servicers' poor performance and violations of Treasury's rules.

Earlier, in June 2021, SIGTARP issued an evaluation report, Treasury Has Been Effective at Shifting the HHF to Assist Homeowners Suffering Pandemic-Related Hardships, Efforts That Could Be Further Enhanced. SIGTARP also issued a Management Advisory Letter the same month, which recommended that Treasury take corrective action to require an important fraud and waste prevention control in the HHF Blight Elimination Program.

SIGTARP's Select Investigative Results (April 1, 2021 to March 31, 2022)

Risk of Fraud, Waste, and Abuse by Financial Institutions in the HAMP Program

SIGTARP's top law enforcement priority is to investigate and bring to justice unlawful conduct by any of the banks and other financial institutions that received $21.98 billion in HAMP. [18] HAMP modifies mortgages (interest rates, terms, etc.) for homeowners at risk of foreclosure, to make mortgage payments more affordable and sustainable for homeowners. There are over 586,000 homeowners participating in all 50 states. California, Florida, New York, and Illinois each have more than 30,000 homeowners actively in HAMP. In fiscal years 2021-2022, Treasury distributed $654.3 million under HAMP, including to banks ($47.1 million to Wells Fargo, $31.7 million to JP Morgan Chase, $33.3 million to Bank of America, and $10.3 million to Citigroup), and non-banks (i.e., $183.4 million to Ocwen Financial, $85.95 million to Nationstar). Treasury's payment of EESA funds to these financial institutions is not automatic, but instead requires that the financial institutions comply with the law and rules of the program. SIGTARP has a number of open, confidential investigations.

Justice for Defendants Convicted of Scamming Homeowners Who Were Seeking Foreclosure Assistance Through HAMP

SIGTARP has caught 121 scammers who were convicted for defrauding nearly 31,000 homeowners nationwide seeking foreclosure relief through HAMP. The courts have sentenced 101 scammers to prison.

18 SIGTARP's March 2022 analysis of Treasury and Fannie Mae's most recent MHA data; Aggregate Cap Monitor Report - March 2022.

New York Man Sentenced for Defrauding Hundreds of Victims in Mortgage Modification Scam

On October 8, 2021, Guy Samuel from Long Island, New York was sentenced to time served in prison, two years supervised release, ordered to forfeit $425,000, and to pay restitution of $721,000. Samuel pled guilty to wire fraud, financial institution fraud, conspiracy to commit wire fraud, and filing false statements in connection with a multi-million-dollar mortgage modification scheme. Over the course of two and a half years, Samuel, along with several co-conspirators, collected advance fees totaling over $2.3 million from hundreds of struggling homeowners with the false promise that they would have their mortgages modified under HAMP. This matter was prosecuted by the U.S. Attorney's Office in the Southern District of New York.

Federal Court Sentences Man to Prison for Participating in Multimillion-Dollar Fraud Scheme Against Those Seeking Assistance From HAMP

On August 20, 2021, Mario Alvarenga was sentenced to six months in prison and three years of supervised release, ordered to forfeit $189,000, and ordered to pay restitution of more than $9.4 million after pleading guilty to conspiracy to commit fraud, bank fraud, and conspiracy to commit obstruction of justice, for participating in a scheme to fraudulently induce distressed homeowners to sell their homes to a company associated with defendants, Launch Development, LLC.

Since at least 2013, Alvarenga and his co-conspirators defrauded distressed homeowners throughout the Bronx, Brooklyn, and Queens, New York, by falsely representing to these homeowners – some of whom were elderly or in poor health – that they could assist the homeowners with a loan modification or similar relief from foreclosure that would allow the homeowners to save their homes. However, rather than assisting these homeowners, the defendants deceived them into selling their homes at a settlement to Launch Development, a for-profit real estate company also affiliated with Alvarenga and his co-conspirators. The homeowners did not know that they were selling their homes to Launch Development for well below market value. One of the co-conspirators went to a homeowner's home and demanded that the homeowner vacate the premises or eviction proceedings would commence. This fraud generated millions of dollars because the houses were then re-sold at enormous profits. SIGTARP was joined in the investigation by the FBI and the New York State Department of Financial Services. The U.S. Attorney's Office for the Southern District of New York prosecuted the case.

California Man Sentenced to More than Four Years in Prison in $2.3 Million Fraud Scheme Under False Names that Victimized More than 400 Homeowners Related to HAMP Program

In September 2021, a federal court sentenced Brian Joseph Pacios to 52 months in prison, the fifth defendant sentenced to prison for a nationwide scheme that defrauded more than 400 homeowners. The court also ordered Pacios to pay restitution of more than $2.3 million. During 2014 and 2015, Pacios and four co-conspirators operated under aliases and told homeowners they worked for HOPE Services, later changed to HAMP Services, which sounded similar to the HAMP program. They falsely told victims they were part of a non-profit, government-affiliated agency, and that the homeowners were eligible and approved for loan modifications. The homeowners were instructed to make three trial payments that would be held in a trust account or escrow, but not to inform their lender about the trial payments. Pacios and co-conspirators fraudulently received at least $2.3 million in trial payments from more than 400 victims nationwide spanning from their base of operation in California to points as far as Egg Harbor City, New Jersey, and Mount Airy, Maryland. Instead of using the funds to assist homeowners, the funds were spent on sales commissions and living expenses of Pacios and the others, as well as trips to Las Vegas. The court previously sentenced four co-conspirators to prison. Alan Jessie Chance was sentenced to twelve months in prison and three years supervised release. Chad Caldaronello was sentenced to three years and five months in prison. Michael P. Paquette was sentenced to one year and three months in prison. Dennis Lake was sentenced to three years probation and six months home confinement. The FBI and Federal Trade Commission were instrumental in assisting SIGTARP in this investigation. The United States Attorney's Office for the Central District of California prosecuted the case.

DC Woman Charged in 35-Count Indictment Alleging Theft of Over $400,000 in Government Benefits Intended for Veterans and the Disabled

On November 18, 2021, Rosemary Ogbenna of the District of Columbia was charged with multiple counts of mail fraud, wire fraud, theft of public funds, aggravated identity theft, representative payee fraud, false statements, tampering with documents, and first-degree theft. The indictment alleges Ogbenna operated a rooming house for retired and disabled individuals for over a decade. It also alleges Ogbenna used over $400,000 in government payments from the Social Security Administration and the Veteran's Administration for her own benefit that were intended for the care of elderly, mentally ill, disabled, and veteran beneficiaries. This case is being prosecuted by the U.S. Attorney's Office for the District of Columbia.

SIGTARP Uses an Analytical Approach to Find Crime in Financial Institutions

SIGTARP continued its longstanding record of holding financial institutions and bankers accountable. SIGTARP supports the Justice Department's prosecutions of individuals and entities investigated by SIGTARP. SIGTARP found that financial institution fraud had evolved from the insider self-dealing fraud that marked the savings and loan crisis. Fraud schemes were now designed to escape detection by traditional fraud identification methods of self-reporting and regulator referrals. As a result, SIGTARP created an analytical approach to discover insider crimes at banks that previously went undetected. SIGTARP also caught bankers who personally profited from fraudulent loans and used TARP to hide their fraud. Additionally, SIGTARP uncovered fraudulent sales practices related to residential mortgage backed securities (RMBS). This includes, TARP's Public Private Investment Partnership (PPIP) program, discussed below, which involved the purchase and sale of RMBS.

New Jersey Hotel Owner Sentenced to 63 Months in Prison for Defrauding TARP Bank in $15 Million Loan Fraud Resulting in $3.6 Million Loss

On April 29, 2021, Mehul Khatiwala, a New Jersey resident who owned various hotels, was sentenced to 63 months in prison, followed by four years of supervised release, fined $50,000, and ordered to pay restitution of $3.6 million for his role in defrauding Cecil Bank. In April 2019, Khatiwala was convicted of conspiracy to commit bank fraud and three counts of bank fraud for defrauding Cecil Bank to obtain loans to purchase hotels and a multifamily residential property, resulting in losses of $3.6 million. In December 2008, Cecil Bank received an $11.56 million bailout from TARP. While the bank was in TARP, from 2011 to 2014, Khatiwala defrauded the bank out of $15 million in loans.

The bank suffered $3.6 million in losses on those loans. In June 2017, Cecil Bank filed bankruptcy, resulting in losses to TARP of more than $10.6 million. U.S. Attorney for the District of Maryland, Robert Hur, whose office prosecuted the case stated, "The defendant used deceit to steal millions of dollars from the victims, which ended up including not only the bank but the American taxpayers." SIGTARP was joined in the investigation by the Federal Housing Finance Agency Office of Inspector General, the Federal Deposit Insurance Corporation Office of Inspector General, and the Small Business Administration Office of Inspector General.

Alabama Man and Georgia Man Sentenced in Conspiracy to Defraud a TARP Recipient Bank; Georgia Woman convicted

On September 8, 2021, Michael Craig Brewster of Huntsville, Alabama, former senior loan officer and Executive Vice President at TARP recipient River City Bank in Rome, Georgia, pled guilty to a charge of receipt of gifts or commissions in exchange for procuring loans. He was sentenced on the same day to 12 months home confinement and three years of supervised release, fined $5,000, and ordered to pay restitution of $46,948.

On September 23, 2021, co-conspirator Edmond Cash pled guilty to a count of bank fraud. On January 7, 2022, Cash was sentenced to time served, three months home confinement, three years supervised release, and ordered to pay restitution of $46,948. River City Bank failed to pay nine quarterly dividend payments to Treasury while in TARP, totaling more than $1 million. Treasury also wrote off $826,721 after auctioning off its preferred shares in a loss. According to the indictment originally returned in February 2021, Cash was involved in developing and investing in residential neighborhood construction projects, including in the Longbranch Lakes development in Spencer, Tennessee. Brewster purchased and sold property in the development. Cash was the lead developer for Longbranch Lakes.

On February 2, 2022, LaDonna Barton also pled guilty to a bank fraud charge in connection with the same conspiracy. Barton's sentencing is set for mid-2022. Barton was an employee of Cash's company and an investor in the development. Cash and his business partners were past due on several loans taken out from River City Bank. Cash and Barton falsely applied for a bank loan for Barton to purchase two parcels of property, when the true purpose of the loan was for Cash to make past due payments on loans that he and his business partners owed to the bank. One day after the bank disbursed the loan proceeds, Barton and Cash made past due payments on loans owed to the bank, paid operating costs for Longbranch Lakes, and pocketed the remaining loan proceeds. SIGTARP was joined in the investigation by the Federal Deposit Insurance Corporation Office of Inspector General. The U.S. Attorney for the Northern District of Georgia is prosecuting the case.

Two Defendants Convicted, One Sentenced to Prison in Operation Phantom Bank

In conjunction with SIGTARP's investigation of TARP recipient Saigon National Bank on December 8, 2021, Defendant Du Truong "Andrew" Nguyen was convicted of all money laundering and money laundering conspiracy charges in a two-day federal jury trial. Nguyen will be sentenced in 2022.

On September 1, 2021, Diana Huong Nguyen pled guilty and was later sentenced, on February 28, 2022, to time served in prison and one year of supervised release.

"Operation Phantom Bank" was a long-term money laundering sting operation from 2010 to 2014 investigated by SIGTARP and its law enforcement partners, the FBI and Internal Revenue Service - Criminal Investigations. This case resulted in six indictments that charged a total of 25 defendants. Convictions to date include a former shareholder of Saigon Bank, a high-level Mexican money launderer, an East West Bank Vice President, the former president of the Chinese Consolidated Benevolent Association and several domestic money launderers with ties to Armenian Power and Chinese Triads. Fugitives include a Racketeer Influenced and Corrupt Organizations (RICO) defendant in Hong Kong and a money laundering defendant in Liechtenstein. The case is being prosecuted by the U.S. Attorney's Office in the Central District of California.

CEO of Louisiana Federal Credit Union Pleads Guilty to Filing a False Document in Connection with TARP Program

On December 13, 2021, Helen Godfrey-Smith, former Chief Executive Officer of the Shreveport Federal Credit Union, pled guilty to a charge of making and using a false document in connection with the TARP funds the Shreveport Federal Credit Union received from the U.S. Treasury. She was charged with this crime in November 2021. In December 2016, Godfrey-Smith signed a document stating the credit union was financially healthy, when in fact the credit union was in dire fiscal condition. Due to its dismal financial condition, the credit union was placed into a conservatorship in April 2017 and was liquidated in October 2017. Godfrey-Smith was scheduled to be sentenced in April 2022.[19] The U.S. Attorney's Office for the Western District of Louisiana is responsible for the prosecution of this case.

Former Supervisor of Residential Mortgage-Backed Securities (RMBS) Trading Desk Agrees to Enter Pretrial Diversion Program in Connection with Scheme to Overcharge Customers

On January 11, 2022, Ross Shapiro, former supervisor of the Residential Mortgage-Backed Securities (RMBS) trading desk at Nomura Securities International (Nomura) in New York admitted that he conspired with others to misrepresent the prices which the Nomura trading desk had obtained or sold certain RMBS. Shapiro and his co-

19 On April 6, 2022, Godfrey-Smith was sentenced to one year probation and ordered to pay a fine of $5,000.

conspirators did this with the intention of deceiving Nomura's customers to increase Nomura's profits at the expense of those customers. At the time, the RMBS desk at Nomura was involved in transacting eligible RMBS that were part of the U.S. Treasury's Public Private Investment Partnership (PPIP) program, one of the TARP-funded programs. Shapiro agreed to enter a pretrial diversion program with the U.S. Attorney's Office for the District of Connecticut.

Former Chief Executive Officer of New Jersey Bank Sentenced in Conspiracy to Mislead the Federal Deposit Insurance Corporation (FDIC)

On February 1, 2022, Joseph Natale, the former Chief Executive Officer of First State Bank of New Jersey was sentenced to five years of probation and ordered to forfeit $359,333 and pay restitution of $715,000 as a result of his guilty plea in conspiracy to file false entries to deceive the FDIC. First State Bank applied for, but did not receive, TARP funds in 2008. The FDIC issued the bank a cease-and-desist order in July 2011 and it was closed down by its regulators in October 2011. Natale and his other co-conspirators deceived bank regulators and the FDIC by using First State Bank's own funds to make it appear that outside investors had provided new capital for the bank. They also created nominee entities and recruited three individuals with close ties to the bank to create the false appearance that they were legitimate investors in the bank. Fraudulent financial statements were provided to both the FDIC and the bank's regulators that inflated the value of the bank, eventually leading to its failure. This matter was prosecuted by the U.S. Attorney's Office for the District of New Jersey.

Kansas Father Pleads Guilty; Son is Sentenced Related to a Wire Fraud Conspiracy Involving a TARP Recipient Bank

K. Kevin James and his son, Charlie James, owned and operated several construction companies in Kansas. These companies secured a line of credit with Blue Valley Bank, a TARP recipient bank. Beginning in 2009 through 2011, K. Kevin James and Charlie James participated in a scheme to provide falsified financial statements for the construction companies to Blue Valley Bank misrepresenting the true financial condition of the construction companies. In May 2011, the James' construction companies filed for bankruptcy, resulting in a loss of over $3 million to Blue Valley Bank. On January 14, 2022, K. Kevin James pled guilty to wire fraud and conspiracy charges for his part in this scheme and is awaiting sentencing. On March 9, 2022, Charlie James was sentenced to 12 months of probation and ordered to pay restitution of $214,305, after having pled guilty to a conspiracy charge in April 2018. The U.S. Attorney's Office for the District of Kansas is prosecuting this case.

Office of Inspector General Department of the Treasury

The Department of the Treasury (Treasury) Office of Inspector General (OIG) performs independent, objective reviews of specific Treasury programs and operations with oversight responsibility for one federal banking agency – the Office of the Comptroller of the Currency (OCC). That federal banking agency supervises approximately 1,200 financial institutions.

Introduction

Treasury OIG was established pursuant to the 1988 amendments to the Inspector General Act of 1978. The Treasury Inspector General is appointed by the President, with the advice and consent of the Senate. Treasury OIG performs independent, objective reviews of Treasury programs and operations, except for those of the Internal Revenue Service (IRS), the Troubled Asset Relief Program (TARP), and those programs and activities under the jurisdictional oversight of the Special Inspector General for Pandemic Recovery (SIGPR). Treasury OIG also keeps the Secretary of the Treasury and Congress fully informed of problems, deficiencies, and the need for corrective action. Treasury OIG is comprised of four divisions: (1) Office of Audit, (2) Office of Investigations, (3) Office of Counsel, and (4) Office of Management. Treasury OIG is headquartered in Washington, DC.

Treasury OIG has oversight responsibility for OCC, which supervises approximately 797 national banks, 269 federal savings associations, and 52 federal branches of foreign banks. The total assets under OCC's supervision are $14.9 trillion. Treasury OIG also oversees four offices created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) which are (1) the Office of Financial Research, (2) the Federal Insurance Office, (3) the Office of Minority and Women Inclusion within Treasury's Departmental Offices, and (4) the Office of Minority and Women Inclusion within OCC. Additionally, Treasury OIG oversees Treasury's role related to the financial solvency of the Federal National Mortgage Association and the Federal Home Loan Mortgage Corporation under the Housing and Economic Recovery Act of 2008, to include Treasury's Senior Preferred Stock Purchase Agreements established for the purpose of maintaining the positive net worth of both entities.

Treasury OIG is also responsible for audit and investigative oversight of Treasury programs providing financial assistance to address the economic impacts of Coronavirus Disease 2019 (COVID-19). Since March 2020, more than $645 billion of financial assistance, overseen by Treasury OIG, has been authorized by the *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act)[20] enacted on March 27, 2020; the *Consolidated Appropriations Act, 2021*[21] enacted on December 27, 2020; and the *American Rescue Plan Act*[22] enacted on March 11, 2021. Through these pieces of legislation, Treasury provides financial assistance to the transportation industry for the continuation of salaries and benefits; to all 50 States, units of local government, U.S. territories, and tribal governments to provide economic relief

20 Public Law 116-136 (March 27, 2020).
21 Public Law 116-260 (December 27, 2020)
22 Public Law 117-2 (March 11, 2021)

including rental and mortgage assistance and support for small businesses; and to community development financial institutions to inject emergency capital investment into low-income communities to address the ongoing pandemic. Treasury established the Office of Recovery Programs to administer the pandemic relief funds. The enormity of these programs requires continued coordination between the Office of Audit, the Office of Investigations, and the Office of Counsel to handle complaints concerning hundreds of recipients and sub-recipients that received financial relief.

Treasury Management and Performance Challenges Related to Financial Regulation and Economic Recovery

In accordance with the Reports Consolidation Act of 2000, the Treasury Inspector General annually provides the Secretary of the Treasury with his perspective on the most serious management and performance challenges facing the Department. In a memorandum to the Secretary dated October 14, 2021, the Inspector General reported five management and performance challenges that were directed towards financial regulation and economic recovery. Those challenges are discussed below and include: Coronavirus Disease 2019 (COVID-19) Pandemic Relief; Transition of a New Administration; Cyber Threats; Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement; and Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments.[23]

COVID-19 Pandemic Relief

The COVID-19 pandemic continues to affect the health and economic stability of communities worldwide. In the early stages of the COVID-19 outbreak in March 2020, Congress passed three key pieces of legislation in succession to address the public health crisis and the economic fallout affecting individuals, businesses, and many industry sectors. The *Coronavirus Preparedness and Response Supplemental Appropriation Act of 2020*, signed into law on March 6, 2020, authorized $8.3 billion in emergency funding to address health and medical care.[24] Shortly thereafter, the *Families First Coronavirus Response Act* was enacted on March 18, 2020, which provided approximately $104 billion to address the financial stress of individuals and households.[25] The *Coronavirus Aid, Relief, and Economic Security Act* (CARES Act)[26] passed on March 27, 2020. The CARES Act provided over $2.4 trillion in health and economic relief to hospitals and healthcare providers, individuals and households, businesses and employees, as well as, states, local and tribal governments, and federal agencies, among others. As the public health crisis continued into late 2020 and the new year, Congress legislated additional relief in passing the *Consolidated Appropriations Act, 2021*[27] (CAA, 2021) on December 27, 2020, and the *American Rescue Plan Act of 2021*[28] (ARP) on March 11, 2021. These laws provided another $900 billion and $1.9 trillion of economic stimulus, respectively.

As reported in the October 29, 2020 management and performance challenges memorandum, Treasury has been instrumental to the implementation of economic relief provisions of the CARES Act. Since then, Treasury's responsibilities and workloads have expanded enormously as several CARES Act provisions were extended under CAA, 2021 and ARP in addition to new programs being established within Treasury. As such, pandemic recovery programs and provisions of the CARES Act, CAA, 2021, and ARP within the oversight purview of Treasury OIG are extensive and include programs that support transportation industry workers; renters and homeowners; and state, local, territorial, and tribal government entities through direct financial assistance.

23 The Treasury Inspector General's memorandum included one other challenge not directly related to financial regulation and economic recovery: Information Technology Acquisition and Project Management. The memorandum also discussed concerns about three matters: the coin redemption program at the United States Mint, managerial cost accounting, and internal control matters at the Bureau of Engraving and Printing.

24 Public Law 116-123 (March 6, 2020)

25 Public Law 116-127 (March 18, 2020)

26 Public Law 116-136 (March 27, 2020)

27 Public Law 116-260 (December 27, 2020)

28 Public Law 117-2 (March 11, 2021)

Financial Assistance for Air Carrier Worker Support and Other Transportation Service Providers

Air Carrier Worker Support

To maintain pay and benefits of airline industry workers, Treasury implemented the Air Carrier Worker Support Program provisions of the CARES Act (hereinafter referred to as the Payroll Support Program) that authorized direct financial assistance for passenger air carriers, cargo air carriers, and contractors. Financial assistance is to ensure the continuation of workers' payroll and benefits with the stipulation that employees are not involuntarily furloughed and do not receive reductions in pay and benefits. Using existing resources and contractor support, Treasury quickly stood up the initial CARES Act Payroll Support Program (PSP1). Financial support for air carrier workers was extended twice by CAA, 2021 and ARP. These extensions became known as PSP2 and PSP3, respectively. Using the mechanisms to establish PSP1, Treasury implemented PSP2 and PSP3 to make corresponding payments.

The CARES Act and CAA, 2021 require Treasury OIG to audit the certifications of sworn financial data submitted to Treasury by passenger and cargo carriers that do not report financial information to the Department of Transportation (referred to as non-241 carriers) and contractors. Additionally, CAA, 2021 requires Treasury OIG to audit contractors' certifications of insufficient funds under the PSP1 to recall employees involuntarily between March 27, 2020 and January 4, 2021. Treasury OIG will continue audits of PSP1 recipients' certifications and initiate audits of certifications submitted by PSP2 recipients in fiscal year 2022. Treasury OIG was not mandated to audit the applicants' certifications to receive PSP3 payments authorized under ARP. However, Treasury disbursed financial assistance to passenger air carriers and contractors based on information submitted by recipients on their PSP2 certifications. Treasury OIG plans to assess Treasury's calculation of award amounts under PSP3 and Treasury's post-award monitoring of recipients under PSP1, PSP2, and PSP3. It is incumbent upon the Department to implement and maintain strong internal controls over recipients' compliance with signed terms and conditions for receiving financial assistance. That is, Treasury's compliance monitoring function is essential to ensuring that recipients use funds for the continuation of salaries and benefits as intended.

Coronavirus Economic Relief for Transportation Services

Congress expanded financial support to non-air carrier transportation service providers under the *Coronavirus Economic Relief for Transportation Services* (CERTS) provisions of CAA, 2021. Treasury established the CERTS Program that provides non-competitive grants to eligible companies that certify revenue loss of 25 percent or more due to the COVID-19 pandemic. In consultation with the Department of Transportation, Treasury provided initial guidelines on May 6, 2021, that included among other things, the priority use of funds must be for payroll, although operating expenses and debt accrued to maintain payroll are eligible uses. To be a qualifying transportation provider, an applicant must demonstrate eligibility as a motor coach, school bus, passenger vessel, or pilotage vessel transportation service. While Treasury has acted swiftly to establish CERTS Program requirements, ongoing administration of grants and monitoring recipient compliance with grant agreements will be challenging with an expected recipient pool in the thousands.

Financial Assistance to State, Local, Tribal, and U.S. Territorial Governments

Coronavirus Relief Fund

The $150 billion Coronavirus Relief Fund (CRF), established under Title VI of the *Social Security Act*, as amended by Title V of the CARES Act, continues to be a large endeavor for Treasury. The Department disbursed direct payments to States, units of local government, the District of Columbia, U.S. Territories, and Tribal governments. Disbursement of funds was a complicated undertaking given the number of recipients at varying levels of government and other payment requirements of the CARES Act. That is, payments to States and local units of government were formula-driven and based on the 2019 U.S. Census, while other payments were based on consultations with the Department of the Interior and Tribal governments and other information obtained by the Department. The CARES Act created a unique challenge in distinguishing between the programmatic administrative responsibility for payments made from the CRF and the Treasury OIG's independent oversight. Although Treasury was authorized to make payments, the CARES Act assigned Treasury OIG with responsibility for monitoring and oversight of the receipt, disbursement, and use of funds. Additionally, Treasury OIG was given authority to recoup funds if it is determined that recipients fail to comply with uses of funds for COVID-19 related costs under Section 601 (d), "Uses of Funds," of the *Social Security Act*, as amended.[29]

Given the direct oversight authorities of the Treasury OIG, the Department did not establish an administrative program to ensure recipient compliance. Recipients were not bound to detailed terms and conditions for the receipt of funds, which we reported in our first audit of CRF regarding the lack of terms and conditions and accountability and transparency of funds.[30] While this is unusual for a federal agency that administers financial assistance programs, Treasury officials have committed to supporting our oversight role for ensuring transparency, accountability, and adherence to all statutory requirements and will continue to collaborate with us to ensure compliance by recipients. This continued collaboration has been critical for overseeing such a large and widely dispersed recipient population given the ongoing challenges of defining and interpreting eligible uses of CRF proceeds. That said, it is crucial that the Department maintain its fundamental role to clarify its policy[31] over the uses of funds when interpretation matters arise. As recipients are still in the process of finalizing use and closing out the funds, Treasury OIG anticipates that questions will continue to arise that will require interpretation. Providing as much clarity as possible over allowable uses is essential for ensuring recipients understand the compliance requirements and are accountable and transparent in how they report uses of funds. Treasury OIG has received over 200 complaints regarding recipient, and in some instances sub-recipient, uses of CRF proceeds that require continued collaboration between our offices.

As part of Treasury OIG's monitoring and oversight function, we established a portal using GrantSolutions[32] for recipients to report their uses of funds on a quarterly basis that started in September 2020. The data received is reviewed and approved by Treasury OIG prior to being extracted for display on the Pandemic Response Accountability Committee[33] (PRAC) website (**https://pandemicoversight.gov**).[34] CAA, 2021 extended the covered period for recipients to use CRF payments through December 30, 2021, and now requires funding agencies under Division A of the CARES Act to report recipient obligation and expenditure data required under sections 15010 and 15011 of CARES Act Division B. This transferred the CRF recipient reporting responsibility to Treasury. While the responsibility is Treasury's, we continue to administer the GrantSolutions portal under an Economy Act Agreement.

Coronavirus State and Local Fiscal Recovery Funds

While disbursing CRF payments was an enormous undertaking for the Department, the Coronavirus State and Local Fiscal Recovery Funds provisions of ARP require Treasury to disburse another $362 billion to State, Local, Territorial, and Tribal governments under the Coronavirus State Fiscal Recovery Fund ($219.8 billion) and the Coronavirus Local Fiscal Recovery Fund ($130.2 billion) (together referred to as SLFRF), Coronavirus Capital Projects Fund (CCPF) ($10 billion), and Local Assistance and Tribal Consistency Fund (CTCF) ($2 billion).

To tackle the $350 billion of SLFRF, Treasury established allocation methodologies, and the Final Rule establishing program requirements to include the uses of funds. Unlike the CRF, recipients may now use funds for a variety of needs to include revenue replacement. Administering SLFRF will pose challenges given the

29 Section 601 (d), Use of Funds, to cover only those costs of the State, Tribal government, or unit of local government that (1) are necessary expenditures incurred due to the public health emergency with respect to COVID–19; (2) were not accounted for in the budget most recently approved as of the date of enactment of this section for the State or government; and (3) were incurred during the period that begins on March 1, 2020, and ends on December 31, 2021, as extended by the CAA, 2021.

30 OIG, Interim Audit Update–Coronavirus Relief Fund Recipient Reporting (OIG-20-036; May 27, 2020)

31 Coronavirus Relief Fund Guidance for State, Territorial, Local, and Tribal Governments Federal Register, Vol. 86, No. 10; January 15, 2021)

32 GrantSolutions is a grant program management Federal Shared service provider under the U.S. Department of Health and Human Services

33 The PRAC, created within the Council of Inspectors General on Integrity and Efficiency, is comprised of Inspectors General of agencies involved in the COVID-19 response to include Treasury OIG, Treasury Inspector General for Tax Administration, and the Special Inspector General for Pandemic Recovery (SIGPR)

34 Of the 939 recipients of CRF payments, 861 recipients meet the threshold for receiving large covered funds of $150,000 or more.

volume of recipients that Treasury must oversee that include all 50 States, U.S. Territories, Tribal governments, local government recipients with population sizes of 250,000 or more, and approximately 30,000 non-entitlement units of local government. Treasury must establish a compliance monitoring function to ensure recipient compliance with use of funds requirements, as well as mechanisms to capture recipient obligation and expenditure data.

As of September 2021, Treasury developed allocation methodologies and guidance for distributing up to $10 billion of CCPF as noncompetitive grants to States, U.S. Territories, and Tribal governments, to address infrastructure challenges, such as reliable internet that low to moderate income and rural communities have experienced during the COVID-19 pandemic.[35] Treasury also began accepting applications through its application submission portal from States and U.S. Territories in September 2021 and plans to open the portal to Tribal governments beginning October 2021. Although Treasury has developed CCPF program requirements and a means to apply for funds, recipient compliance and reporting requirements are still forthcoming. Treasury will need to develop these requirements expeditiously so that they are incorporated into the terms and conditions of CCPF grant agreements.

Under the CTCF, Treasury was appropriated an additional $2 billion for fiscal years 2022 and 2023, for COVID-19 assistance payments to eligible revenue sharing counties and Tribes.[36] Eligibility for counties (to include parishes and boroughs) is based on poverty rates, household income, land values, unemployment rates, and other economic indicators, over a 20-year period ending September 30, 2021. Tribal government eligibility is based on economic conditions of each Tribe. Funds under the CTCF may be used for any governmental purpose other than lobbying.

With the overlap of recipients of CRF, SLFRF, CCPF, and CTCF, we expect that there will be confusion between the uses of funds requirements, and reporting mechanisms for recipients that may be a challenge going forward. Given the volume of recipients and varying requirements under these programs, Treasury will need to ensure that there are sufficient resources for the remaining distribution of funds and ongoing monitoring of recipient reporting and compliance with terms and conditions for funds received. Furthermore, with the level of funding under both CRF and SLFRF, Treasury may now have cognizance over many local governments.[37]

Emergency Rental Assistance Program and Homeowner Assistance Fund

To provide assistance to vulnerable households at risk of housing instability, Congress established two Emergency Rental Assistance (ERA) Programs and a Homeowner's Assistance Fund (HAF) availing over $56 billion to households in need. CAA, 2021, created the initial ERA Program (ERA1) and ARP created a supplemental ERA Program (ERA2) and HAF.

According to CAA, 2021, Treasury established ERA1 to provide up to $25 billion in assistance to States (including Washington, DC), US Territories, Tribal governments (with a provision for the Department of Hawaiian Home Lands), and units of local government with populations of 200,000 or greater. ERA1 funds are to be available for eligible renter households negatively impacted by the COVID-19 pandemic to pay for rent, utilities, and other housing-related expenses and arrears. Under ERA1, an eligible household may receive funds for up to a 12-month period unless the grantee determines an extension is necessary to ensure housing

35 https://www.govinfo.gov/content/pkg/FR-2021-05-17/pdf/2021-10283.pdf

36 Under the American Rescue Plan Act, the term 'eligible revenue sharing county' means— (A) a county, parish, or borough—(i) that is independent of any other unit of local government; and (ii) that, as determined by the Secretary, is the principal provider of government services for the area within its jurisdiction; and (iii) for which, as determined by the Secretary, there is a negative revenue impact due to implementation of a Federal program or changes to such program; and (B) the District of Columbia, the Commonwealth of Puerto Rico, Guam, and the United States Virgin Islands.

37 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, §200.513 Responsibilities (a)(1) Cognizant agency for audit responsibilities. A non-federal entity expending more than $50 million a year in federal awards must have a cognizant agency for audit. The designated cognizant agency for audit must be the federal awarding agency that provides the predominant amount of funding directly (direct funding) (as listed on the Schedule of expenditures of federal awards, see §200.510(b)) to a non-federal entity unless OMB designates a specific cognizant agency for audit. When the direct funding represents less than 25 percent of the total expenditures (as direct and subawards) by the non-federal entity, then the federal agency with the predominant amount of total funding is the designated cognizant agency for audit. (https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=e78c6acc3819f56b44027416dc151015&mc=true&n=sp2.1.200.f&r=SUBPART&ty=HTML#se2.1.200_1513)

stability for the household; then funds may be made available for up to 15 total months. Additionally, ARP extended ERA1 funds' availability until September 30, 2022. Treasury has sent payments of ERA1 funds to government recipients, provided guidance on fund usage, and set up a Portal where recipients are to report on their spending. CAA, 2021 requires that Treasury OIG conducts monitoring and oversight of the receipt, disbursement, and use of ERA1 funds. Treasury OIG will use the data reported in Treasury's ERA Portal to inform our monitoring function; thus, it is imperative that Treasury ensures recipients' compliance to Treasury ERA guidance when reporting to Treasury's ERA Portal.

ARP authorized an additional $21.55 billion of ERA funds to remain available until September 30, 2027, referred to as ERA2. Similar to ERA1, ERA2 provides funding for eligible renter households' rent, utilities, and other housing-related expenses and arrears, but does not include Tribal governments as eligible grantees. Instead, ERA2 earmarks $2.5 billion specifically for high-need grantees which are eligible grantees in jurisdictions with a high number of very low-income renter households. ARP designates that an eligible household may receive ERA for up to 18 total months (this includes ERA1 and ERA2 funding). Treasury has provided ERA2 guidance and allocated funds for the state, territory, and local government recipients. Treasury OIG is tasked with oversight of the program and will conduct ERA2 oversight with a similar methodology to ERA1 oversight.

ARP also created HAF, which authorized $9.961 billion to prevent mortgage delinquencies, defaults, foreclosures, loss of utility services, and displacement by covering mortgage-related expenses, utility expenses, and arrears for homeowners experiencing financial hardship after January 21, 2020. HAF provides funds for States (including the District of Columbia and Puerto Rico), Tribal governments (including the Department of Hawaiian Home Lands), Guam, American Samoa, the U.S. Virgin Islands, and the Commonwealth of the Northern Mariana Islands. The funds are available until September 30, 2025. Treasury has provided guidance to HAF participants and allocated funds for each state and territory recipient based on homeowner need. ARP mandates that Treasury OIG provide oversight of HAF.

Both the ERA programs and HAF require that Treasury provide guidance to supplement the statutes that created the programs. While Treasury has issued relevant guidance for each of the programs, it is essential its program offices continue to be responsive to recipients to clarify guidance and to provide insight into the eligible uses of the funds Treasury distributed. Clear and timely guidance and responsiveness to recipient questions are also critical in enabling program recipients to administer their programs and disburse funds to households in need without delay.

State Small Business Credit Initiative

The State Small Business Credit Initiative (SSBCI), which was originally created in the Small Business Jobs Act of 2010 to increase availability of credit for small businesses, ended in 2017. However, Section 3301 of ARP reauthorized SSBCI and provided $10 billion in funding for the program. Under SSBCI, participating States, U.S. Territories, and Tribal governments may obtain funding for programs that partner with private lenders to extend credit to small businesses. Such programs may include those that finance loan loss reserves, and those that provide loan insurance, loan guaranties, venture capital funds, and collateral support. States, U.S. Territories, and Tribal governments who apply for SSBCI must provide Treasury with plans for using their funding allocations for review and approval and report quarterly and annually on results. Treasury will distribute funds in three different tranches over 10 years.

Additionally, ARP modified SSBCI in a number of ways including the following set-asides: (1) $500 million in allocations to Tribal governments in proportions determined appropriate by the Secretary of the Treasury; (2) $1.5 billion in allocation to States, U.S. Territories, and Tribal governments for business enterprises owned and controlled by socially and economically-disadvantaged individuals (SEDI); (3) $1 billion to be allocated as an incentive for States, U.S. Territories, and Tribal governments that demonstrate robust support for SEDI businesses; (4) $500 million to be allocated to very small businesses with fewer than 10 employees; and (5) $500 million to provide technical assistance to certain businesses applying for SSBCI or other state or federal programs that support small businesses.

Primary oversight of the use of SSBCI funds is the responsibility of the participating State, U.S. Territory or Tribal government. The participants are responsible for providing Treasury with quarterly assurances that their programs approved for SSBCI funding are in compliance with program requirements. However, Treasury will face challenges in holding participants accountable for the proper use of funds as it has not clearly defined the oversight obligations of the States, U.S. Territories, and Tribal governments or specified minimum standards for determining whether participants have fulfilled their oversight responsibilities. In the past, Treasury has also not required participating states to collect and review compliance assurances made by lenders and borrowers or defined what constitutes a material adverse change in a state's financial or operational condition that must be reported to Treasury. As a result, Treasury may have difficulty finding recipients to be in default of program requirements and holding recipients accountable.

Community Development Investment Programs[38]

Emergency Capital Investment Program

Authorized under CAA, 2021, Treasury established the Emergency Capital Investment Program (ECIP) to provide up to $9 billion in capital to low-to-moderate income community financial institutions that support small businesses and consumers. Under ECIP, certified community development financial institutions (CDFI) and minority depository institutions may provide loans, grants, and forbearance for small businesses, minority-owned businesses, and consumers in communities disproportionately impacted by the COVID-19 pandemic. Treasury opened the application portal on March 4, 2021. Since that time, Treasury has experienced challenges in fully implementing ECIP. Because of the demands for resources within the Office of Recovery Programs, Treasury may experience further delays and challenges administering the ECIP.

CDFI Rapid Response Program

CAA, 2021 also authorized $3 billion to the CDFI Fund to deliver immediate assistance to low-income communities through competitive grants to CDFIs. The CDFI Rapid Response Program (RRP) was established and awarded $1.25 billion in June 2021. It will be more challenging for the CDFI Fund to establish the Emergency Support and Minority Lending Program in fiscal year 2022 to deliver the remaining $1.75 billion reserved for low- or moderate-income minority communities. The program introduces a new requirement to make $1.2 billion available for awards to minority lending institutions. CDFI Fund officials acknowledged that it would take time to develop a compliant program. At the same time, the CDFI Fund must monitor the CDFI RRP award recipients for use of funds compliance, while administering several other non-pandemic grant programs.

Accountability and Transparency

As reported in the October 29, 2020 management and performance challenges memorandum, Treasury accomplished much in helping to alleviate hardships of families and industry sectors to include delivering more than $400 billion of Economic Impact Payments under ARP to workers and households through the Internal Revenue Service (IRS) and Bureau of the Fiscal Service (Fiscal Service). Through the IRS, Treasury helps to protect workers and jobs through the Employee Retention Tax Credit and Payroll Tax Deferral authorized by the CARES Act. Treasury also assisted the Small Business Administration in carrying out the Paycheck Protection Program and the Economic Injury Disaster Loans authorized by the CARES Act to support payroll, benefits, and other operating costs of small businesses. Under the Emergency Relief and Taxpayer Protections (commonly referred to as Section 4003), Treasury was authorized to make loans, loan guarantees, and other investments to eligible businesses, states, and municipalities. The Emergency Relief and Taxpayer Protections provisions also authorized the establishment of the Special Inspector General for Pandemic Recovery (SIGPR) within Treasury to oversee loans, loan guarantees, and other investments provided by Treasury. Although some of the aforementioned

38 Treasury OIG is required to submit to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate, and the Secretary of the Treasury, not less frequently than 2 times per year, a report relating to the oversight provided including any recommendations for improvements to the Community Development Investment programs

CARES Act provisions do not fall under the oversight jurisdiction of Treasury OIG, the payment work streams and mechanisms administered by the Fiscal Service do.

In the context of this overarching challenge, we recognize the breadth and scope of Treasury's responsibilities as it impacts programs, operations, and activities regardless of jurisdictional oversight boundaries. Along with administering and delivering economic relief, Treasury must manage the unprecedented pandemic relief oversight. In addition to Treasury OIG's ongoing work on pandemic programs, Treasury is subject to a number of additional oversight bodies. As mentioned above, SIGPR was created to oversee loans, loan guarantees, and other investments provided by Treasury[39] and must report to congress quarterly on SIGPR's activities and Treasury's loan programs. A Congressional Oversight Commission was established to report to Congress on Treasury's and the Federal Reserve Board's implementation activities under Title IV, Subtitle A, "Coronavirus Economic Stabilization Act of 2020." Moreover, the commission is required to report every 30 days on the use of contractors and administration of loan programs, the impact of programs on the Nation's financial wellbeing, whether required disclosures of the CARES Act provide market transparency, and the effectiveness of maximizing benefits and minimizing costs to taxpayers, among other things.[40] Furthermore, the Government Accountability Office (GAO) has ongoing work evaluating the federal response to the COVID-19 pandemic and the effects of the pandemic on federal programs and operations.

Treasury is also accountable for providing transparency over the expenditure of pandemic relief funds. Many reporting requirements of sections 15010 and 15011 of the CARES Act were extended under the CAA, 2021, PRAC amendments. Most notably, Treasury is responsible for reporting obligations and expenditures of large covered funds (over $150,000) to the PRAC. While Treasury OIG continues to collect and report CRF data to the PRAC under an agreement with the Department as noted above, Treasury is responsible for reporting expenditures of its other pandemic relief programs. Furthermore, Treasury must provide public reports quarterly on the use of funds under its ERA program. The Department must balance its ongoing response to the financial impacts of the public health emergency with its responsibility to stakeholders for reporting and transparency.

While the COVID-19 pandemic continues, Treasury must persevere in navigating this challenging time. Treasury has leveraged its existing workforce, hired contractors, and obtained detailees from other Federal agencies to address the demands of the new programs created by pandemic legislation. Going forward, Treasury may experience difficulties in balancing its new responsibilities and workloads while managing several ongoing challenges as described above.

Transition of New Administration

As characteristic with incoming Presidential Administrations, the Departmental Offices, and Treasury bureaus and agencies are challenged with filling and transitioning numerous key senior leadership positions, as well as implementing new executive orders and White House initiatives. As of October 2021, 17 senior leadership positions were vacant including, among others, the Undersecretary for International Affairs, the Undersecretary for Terrorism and Financial Intelligence, the Comptroller of the Currency, the General Counsel, and the Inspector General.

Additionally, the White House introduced EO 14008, Tackling the Climate Crisis at Home and Abroad, to ensure climate considerations are an essential element of U.S. foreign policy and national security. The Secretary of State and the Secretary of the Treasury will lead several efforts related to EO 14008 in coordination with the Special Presidential Envoy for Climate. Furthermore, the White House introduced EO 14030, Climate-Related Financial Risk which aims to: (a) advance consistent, clear, intelligible, comparable, and accurate disclosure of climate-related financial risk, including both physical and transition risks; (b) mitigate that risk and its drivers, while accounting for and addressing disparate impacts on disadvantaged communities and communities of

39 SIGPR terminates five years after enactment of the CARES Act (March 27, 2025)

40 The Congressional Oversight Commission issued its fourteenth report on June 30, 2021 (https://coc.senate.gov/sites/default/files/2021-06/June%20Report%20Final.pdf)

color and spurring the creation of well-paying jobs; and (c) achieve the Administration's target of a net-zero emissions economy by no later than 2050. The Secretary of the Treasury, as the Chair of the Financial Stability Oversight Council, will lead several efforts related to EO 14030.

While Treasury continues transitioning key senior leadership positions and implementing these and other new initiatives and programs going into fiscal year 2022, other previously reported uncertainties have yet to be resolved. Treasury continues to operate in the repeated cycle of budget and debt ceiling stopgaps. A long-term solution has yet to be found. Additionally, although not included as a top open recommendation in its June 2021 letter to the Department,[41] GAO raised concerns to Congress in its July 2015 report[42] with the approach to managing the federal debt limit and its impact on Treasury's borrowing costs and the need for alternative approaches. With that said, Fiscal Service has ongoing communication with the Department, particularly the Office of Fiscal Projections (OFP). OFP provides Treasury decision-makers with information on current and predicted cash balances. As the Federal Government's financial manager, Fiscal Service plays a unique role in ensuring that OFP has current and accurate federal financial data.

Dealing with the transition of key senior leadership positions, new initiatives, additional workloads, and other critical matters such as the budget and debt ceiling stopgaps during the COVID-19 pandemic continues to be more challenging than usual. The impact of this challenge and the uncertainties require the Department to continue to focus its resources on programs that are in the highest need to citizens and/or where there is a unique federal role. It is essential that new initiatives, programs, and reforms be managed and communicated effectively for achieving performance and accountability.

Cyber Threats

Cybersecurity is a long-standing and serious challenge facing the Nation. A reliable critical infrastructure, including information systems and networks, is vital to our national security and economic stability. Cyber threats remain a persistent concern as Treasury's information systems are critical to the core functions of government and the Nation's financial infrastructure, along with the financial sector it oversees. The cyber threats continue to evolve and become more sophisticated, subtle, and easier to perform, which poses ongoing challenges for Treasury to fortify and safeguard its internal systems and operations while modernizing and maintaining them. While managing known risks is an ongoing challenge, Treasury must also be ready to reinforce and/or redirect cybersecurity efforts when unforeseen events occur such as the COVID-19 pandemic and the SolarWinds attack.[43]

Attackers frequently exploit vulnerable networks or systems in a string of trusted connections to gain access to government systems. Organized hacking groups leverage published and unpublished vulnerabilities and vary their methods to make attacks hard to detect and even harder to prevent. Criminal groups and nation-states are constantly seeking to steal information; commit fraud; disrupt, degrade, or deny access to information systems; or infiltrate information systems and maintain a presence to enable future actions. Through cyber information sharing, federal agencies are better prepared to thwart potential attacks to the cyber infrastructure of the Federal government and the financial sector that it serves. In its 2021 high-risk list published biennially, again GAO reported the Nations' cybersecurity as a government-wide issue.[44]

Long-standing cyber threats pose increased risks to networks and information systems during the ongoing COVID-19 global health pandemic as more opportunities are available for bad actors to stage cyber-attacks. As the tools used to perpetrate cyber-attacks become easier to use and more widespread, less technological knowledge and fewer resources are needed to launch successful attacks of increasing sophistication. Such attacks include distributed denial of service, phishing or whaling, fraudulent wire payments, malicious spam

41 GAO, Priority Open Recommendations: Department of the Treasury (June 16, 2021)

42 GAO, Debt Limit: Market Response to Recent Impasses Underscores Need to Consider Alternative Approaches (GAO-15-476; July 9, 2015)

43 The SolarWinds attack, reported in December 2020, was a supply chain attack that used the update mechanism for legitimate software to distribute malicious software.

44 GAO, High-Risk Series, Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas (GAO-21-119SP: March 2020)

(malspam), ransomware, and compromise of supply chains (both hardware and software). The COVID -19 pandemic has shifted the federal workforce to a primarily telework status which has provided attackers with more possibilities to disrupt services. Increased network traffic from remote sources provides cover for attackers to blend in with the federal workforce and launch cyber assaults. Attackers may take advantage of the increased demand for information on COVID-19 by crafting highly attractive phishing, whaling, and malspam attacks that are more likely to succeed by luring workers in with promises of information related to COVID-19. These opportunities may allow hackers to launch a denial of service attack upon a network that can prevent remote workers from performing their duties and disrupt operations. Furthermore, information systems and its users are at heightened risk of COVID-19 related exploitation such as stimulus check scams, tax-fraud schemes, and fraudulent coronavirus testing kit scams, among other things.

There is continuing concern over foreign adversaries creating and exploiting vulnerabilities in the Nation's supply chain for information and communication technology and services as evidenced by the SolarWinds attack that affected many federal agencies and private sector companies. Executive Order 13873 was issued on May 15, 2019, to secure the supply technology and services chain by banning the import, use, or sale of technology or services designed, developed, manufactured, or supplied from persons or companies that are owned or controlled by governments defined as hostile to the United States.[45] On May 11, 2021, this Executive Order was extended again for 1 year.[46] There are risks that Treasury's systems and resources already in use, including critical infrastructure, contain components from sources that have yet to be designated as threats. Once a source is designated as such, repairs and/or upgrades of key system components may no longer be available. Therefore, there is risk of disruption of critical operations. The Department will need to monitor developments in this area closely and plan for the possibility that its current supply chain may no longer be available. Furthermore, Executive Order 14028, *Improving the Nation's Cybersecurity*, issued on May 12, 2021, calls for federal agencies to update existing plans to prioritize resources for adoption and use of cloud technology and to adopt a zero-trust architecture,[47] among other things. Treasury management must be mindful that the efforts to secure Treasury's supply chain may hamper cloud adoption and the implementation of zero-trust architecture.

Treasury is looked upon to provide effective leadership to financial institutions in particular, and the financial sector in general, to strengthen awareness and preparedness against cyber threats to the Nation's critical infrastructure. As such, effective public-private coordination is essential to the Nation's financial and national security. In this regard, The Office of Cybersecurity and Critical Infrastructure Protection coordinates Treasury's efforts to enhance the security and resilience of the financial services sector critical infrastructure and reduce operational risk including risks associated with cybersecurity. Given the stress that the global COVID-19 pandemic continues to place on financial institutions and the financial sector as a whole, it is important that the Department monitors cyber risks in these areas. That said, Treasury and other federal agencies have yet to fully implement the National Institute of Standards and Technology (NIST) guidance to assist federal agencies in managing cybersecurity risks.[48] In 2018, GAO had reported that the extent of adoption of the NIST framework by critical infrastructure sectors was unknown since agencies were not measuring framework implementation. With respect to Treasury, GAO had recommended that steps be taken to consult with respective sector partners to develop methods for determining the level and type of adoption by entities across the financial services sector. In its June 16, 2021[49] letter regarding its top open recommendations, GAO noted that Treasury had established ongoing initiatives such as developing common terminology for cyber terms, but had not developed methods to determine the level and type of framework adoption; the recommendation remained open. GAO acknowledged that Treasury had developed a cybersecurity risk management strategy, which included key elements identified in federal guidance and established a process for conducting an organization-wide cybersecurity risk assessment.

45 Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019)

46 Notice on the Continuation of the National Emergency with Respect to Securing the Information and Communications Technology and Services Supply Chain (May 11, 2021)

47 Zero-trust architecture is a method of designing a system in which all actions are presumed dangerous until reasonably proven otherwise, thereby reducing the chance of a successful attack causing further damage.

48 NIST, Framework for Improving Critical Infrastructure Cybersecurity (Version 1.0, February 12, 2014; superseded by Version 1.1; April 16, 2018)

49 GAO, Treasury Priority Recommendations (GAO-21-549PR; June 16, 2021)

The Department continues to report progress in its risk-based approach to cybersecurity by establishing the Enterprise Cyber Risk Management program to manage vulnerabilities and threats that can cause disruption in the delivery of services. In response to our October 2020 memorandum, the Department reported that it created a centralized Risk Reporting Analytical Cybersecurity System, and developed the Supply Chain Risk Management program for cybersecurity in fiscal year 2020. Treasury also reported prior progress in risk management by identifying High Value Assets,[50] and examining the security architectures of systems and performing risk and vulnerability assessments. While addressing increases in cyber threats during the COVID-19 global pandemic, Treasury will need to continue to balance cybersecurity demands while modernizing and maintaining Information Technology (IT) systems.

Anti-Money Laundering and Terrorist Financing/Bank Secrecy Act Enforcement

Treasury's Office of Terrorism and Financial Intelligence (TFI) has remained dedicated to countering the ability of financial networks that support terrorists, organized transnational crime, weapons of mass destruction proliferators, and other threats to international security through intelligence analysis, sanctions, and international private-sector cooperation. Identifying, disrupting, and dismantling the financial networks that support rogue regimes, terrorist organizations, transnational criminal organizations, and other threats to the national security of the United States and our allies continues to be challenging as TFI's role to counter these financial networks and threats has grown because its economic authorities are key tools to carry out U.S. policy. Additionally, criminals and other bad actors evolve and continue to develop more sophisticated money laundering methods in an attempt to avoid detection.

TFI's counter-terrorism designations disrupt the financial networks that support terrorist organizations. Disrupting terrorist financing depends on a whole-of-government approach and requires collaboration and coordination within Treasury and with other federal agencies. Collaboration and coordination are key to successfully identifying and disrupting all of these financial networks and meeting TFI's mission. This effort requires effective and efficient working relationships among components within TFI and the Intelligence Community.

Data security and information sharing are challenges for the Financial Crimes Enforcement Network (FinCEN), which has experienced unauthorized disclosures of Bank Secrecy Act information. FinCEN is required to maintain a highly secure database for financial institutions to report suspicious activity. FinCEN has previously identified that the success of that system depends on the financial sector's confidence that those reports are adequately protected, but data breaches threaten to undermine that confidence. FinCEN is also required to maintain a government-wide data access service to make information available and useful to federal, state, local, and foreign law enforcement agencies and appropriate regulators and to support intelligence and counterintelligence activities and anti-money laundering initiatives. The challenge for FinCEN is to ensure the Bank Secrecy Act data remains secure in order to maintain the confidence of the financial sector while meeting the access needs of law enforcement, regulatory, and intelligence partners.

Given the criticality of Treasury's mission and its role to carry out U.S. policy, Treasury OIG continues to consider anti-money laundering and combating terrorist financing programs and operations as inherently high-risk.

Efforts to Promote Spending Transparency and to Prevent and Detect Improper Payments

Given the broad implications and critical roles assigned to Treasury by the Digital Accountability and Transparency Act of 2014 (DATA Act), Treasury OIG notes the renewed challenges facing the Department given the need to ensure transparency to the taxpayer and other stakeholders on the use of funds distributed under economic relief packages enacted to address individuals and industry sectors impacted by the COVID-19

50 High Value Assets are assets, information systems information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the U S.' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety.

global pandemic. DATA Act reporting is seen as one of the means to ensure transparency into the use of federal funds related to COVID-19 expenditures. As noted earlier, over the past year, Treasury delivered more than $400 billion of Economic Impact Payments under ARP to workers and households through IRS and Fiscal Service. Treasury is also accountable for providing transparency over the expenditure of pandemic relief funds. Additionally, many reporting requirements of sections 15010 and 15011 of the CARES Act were extended under the CAA, 2021, PRAC amendments. Treasury must also provide public reports quarterly on the use of funds under its Emergency Rental Assistance program, among others. With that said, the Department must balance its ongoing response to the financial impacts of the public health emergency with its responsibility to respond to oversight bodies and stakeholders.

Completed and In-Progress Work on Financial Oversight

OCC's Supervision Related to De-risking by Banks (OIG-CA-21-024)

In response to a July 5, 2016, request from the House Financial Services Committee, we initiated an audit to review OCC's supervision of Bank Secrecy Act and anti-money laundering regulations, Office of Foreign Assets Control sanctions, and other applicable laws, particularly relating to the de-risking trend. Our audit objectives were to determine: (1) whether supervisory, examination, or other staff of OCC had indirectly or directly caused banks to exit a line of business or to terminate a customer or correspondent account, and (2) under what authorities OCC planned to limit, through guidance or regulations, the ability of banks to open or close correspondent or customer accounts, including a review of laws that govern account closings.

Based on work we performed during our review, we concluded that OCC did not indirectly or directly instruct banks to exit a line of business or to terminate a customer or correspondent account for the purpose of de-risking. We also found that in order to limit, through guidance, the ability of banks to open or close correspondent or customer accounts, OCC issued OCC Bulletin 2016-32, Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking, on October 5, 2016, and OCC National Risk Committee Supervision Tip 2017-01, on February 14, 2017. Furthermore, in January 2017, OCC's Compliance and Community Affairs Division conducted a non-mandatory correspondent banking training for all OCC staff related to OCC's position on risk re-evaluation and their supervisory expectations. However, due to the passage of time from the initiation of the audit, and our findings, we determined that continuing our audit would not significantly enhance OCC's supervision of national banks' compliance with the BSA and other applicable laws and regulations, particularly as they relate to the trend of de-risking. Accordingly, we terminated this audit.

OCC Human Capital Policies and Planning (OIG-CA-21-026)

In February 2019, we initiated an audit of OCC's human capital policies and resource planning. The objective of our audit was to determine whether OCC's human capital policies and planning align with its mission and strategic goals.

Given that OCC (1) recently had a human capital review performed by the Office of Personnel Management, which found that OCC's human capital programs support its mission effectively and efficiently while complying with legal requirements and that OCC aligns its human capital goals with its strategic plan and desired performance outcomes, and (2) that there isn't a linear relationship between OCC's number of employees and number of supervised institutions, we determined that continuing our audit would not significantly enhance the human capital policies and planning alignment with OCC's mission and strategic goals. Accordingly, we terminated this audit.

OCC's Supervision of Federal Branches of Foreign Banks (In Progress)

We initiated an audit of OCC's supervision of federal branches of foreign banks. The objective of this audit is to assess OCC's supervision of federal branches and agencies of foreign banking organizations operating in the United States.

OCC's Controls over Purchase Cards (In Progress)

We initiated an audit of OCC's controls over purchase cards. The objective for this audit is to assess the controls in place over OCC's purchase card use and identify any potential illegal, improper, or erroneous transactions.

OCC's Crisis Readiness (In Progress)

We initiated an audit of OCC's crisis readiness. The objective for this audit is to assess OCC's readiness to address crises that could impact OCC's operations and the institutions it supervises.

Corrective Action Verification (CAV) Material Loss Review of Washington Federal Bank for Savings (In Progress)

We initiated an audit to assess whether OCC's management has taken corrective actions in response to the six recommendations made in the Department of the Treasury (Treasury) Office of Inspector General audit report, Material Loss Review of Washington Federal Bank for Savings (OIG-19-009, issued November 6, 2018).

Failed Bank Reviews

In 1991, Congress enacted the Federal Deposit Insurance Corporation Improvement Act amending the Federal Deposit Insurance Act (FDIA). The amendments require that banking regulators take specified supervisory actions when they identify unsafe or unsound practices or conditions. Also added was a requirement that the Inspector General for the primary federal regulator of a failed financial institution conduct a material loss review when the estimated loss to the Deposit Insurance Fund is "material." FDIA, as amended by Dodd-Frank, defines the loss threshold amount to the Deposit Insurance Fund triggering a material loss review as a loss that exceeds $50 million for 2014 and thereafter (with a provision to temporarily raise the threshold to $75 million in certain circumstances). The act also requires a review of all bank failures with losses under these threshold amounts for the purposes of (1) ascertaining the grounds for appointing Federal Deposit Insurance Corporation (FDIC) as receiver and (2) determining whether any unusual circumstances exist that might warrant a more in-depth review of the loss. As part of the material loss review, OIG auditors determine the causes of the failure and assess the supervision of the institution, including the implementation of the prompt corrective action provisions of the act.[51] As appropriate, OIG auditors also make recommendations for preventing any such loss in the future.

From 2007 through March 2022, FDIC and other banking regulators closed 536 banks and federal savings associations. One hundred and forty-four (144) of these were Treasury-regulated financial institutions; in total, the estimated loss to FDIC's Deposit Insurance Fund for these failures was $36.5 billion. Of the 144 failures, 58 resulted in a material loss to the Deposit Insurance Fund, and our office performed the required reviews of these failures.

During the period covered by this annual report, we did not perform a material loss review or limited review of any bank failures.

51 Prompt corrective action is a framework of supervisory actions for insured institutions that are not adequately capitalized. It was intended to ensure that action is taken when an institution becomes financially troubled in order to prevent a failure or minimize the resulting losses. These actions become increasingly severe as the institution falls into lower capital categories. The capital categories are well-capitalized, adequately capitalized, undercapitalized, significantly undercapitalized, and critically undercapitalized.

OIG Investigative Accomplishments

The Office of Investigations, under the leadership of the Assistant Inspector General for Investigations, performs investigations and conducts initiatives to detect and prevent fraud, waste, and abuse in programs and operations within Treasury OIG's jurisdictional boundaries, and investigates threats against Treasury personnel and assets in designated circumstances as authorized by the Inspector General Act. The Office of Investigations also manages the Treasury OIG Hotline to facilitate reporting of allegations involving these programs and operations.

CARES Act Investigations

Departmental Offices Employee Forwarded Sensitive CARES Act Tribal Data to Another Agency Without Encryption or Confidential Warnings

Our investigation, which was initiated upon receipt of information from Congress and the Department of the Interior OIG, revealed that unencrypted CARES Act tribal data was emailed, without confidential warnings to another Government agency, which contributed to a leak of tribal data. Criminal prosecution was presented and declined by the U.S. Attorney's Office (USAO) for the District of Columbia. Our office provided a report of investigation to Departmental Offices (DO), Office of the Assistant Secretary for Management, and to the concerned members of Congress.

Business Owner Submitted Fraudulent Documents to Receive Coronavirus Relief Funds

Our investigation revealed that a home healthcare company owner submitted fraudulent documents to the Louisville, Kentucky government to obtain $17,000 in CARES Act Coronavirus Relief Funds. Criminal prosecution of the individual was presented and declined by the United States Attorney's Office (USAO) for the Western District of Kentucky.

Other Significant Investigations

Debit Card Fraud Conspirators Prosecuted

Our joint investigation with the Federal Bureau of Investigation, Homeland Security Investigations, and U.S. Postal Inspection Service (USPIS) revealed that five subjects conspired to defraud several financial institutions in a scheme using fraudulent debit card returns resulting in an initial estimated loss of $1.1 million to those institutions. The USAO for the Eastern District of Virginia sentenced the subjects to 13 months in prison, 13 years of probation, and $1.2 million in criminal restitution.

Subject Sentenced for Theft of Government Funds and Defrauding a Financial Institution

A final subject in our joint investigation with Internal Revenue Service-Criminal Investigation (IRS-CI), and USPIS was sentenced to 26 months in prison, 96 months of probation, restitution of $283,224, a special assessment of $200, and forfeiture of $60,619. The subject conspired with others and deposited a stolen Department of the Treasury (Treasury or the Department) check, in the amount of $993,176, into a bank account opened in the name of a fictitious business with false identification.

New Jersey Subject Sentenced for Obtaining Funds from a Stolen and Altered Treasury Check and Paycheck Protection Program Fraud Scheme

Our investigation, initiated upon receipt of information from the Bureau of the Fiscal Service, revealed that an individual negotiated a stolen and altered Treasury check and submitted fraudulent Paycheck Protection

Program applications to obtain over $600,000 in program proceeds. After successful prosecution by the USAO for the District of New Jersey, the individual was sentenced to 30 months in prison, 36 months of probation, $137,000 in restitution, $484,000 in forfeitures, and a $200 special assessment.

Subjects Sentenced for Theft of Treasury Checks

Our joint investigation with the U.S. Postal Inspection Service, Internal Revenue Service Criminal Investigation, and Treasury Inspector General for Tax Administration revealed that at least 12 subjects deposited 99 stolen Treasury checks at various branches of the same bank in Arizona, Colorado, Kansas, and Missouri. The estimated loss to the bank was over $447,000. The case was prosecuted by the USAO for the Western District of Missouri.

Update: Our joint investigation concluded with eight subjects sentenced to 258 months in prison, 120 months of probation, 216 months of supervised release, $1.5 million in restitution, and $1,700 in special assessments.