March 29, 2023

Consumer Financial Protection Bureau

2023 Major Management Challenges for the CFPB

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

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

MEMORANDUM

DATE: March 29, 2023

TO: Rohit Chopra
Director
Consumer Financial Protection Bureau

FROM: Mark Bialek
Inspector General

SUBJECT: *2023 Major Management Challenges for the CFPB*

We are providing you with the major management challenges facing the Consumer Financial Protection Bureau in 2023. These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the CFPB's accomplishment of its strategic objectives.

We identified the CFPB's major management challenges by assessing key themes from our discussions with management and our understanding of the agency's programs and operations. The CFPB plays a vital role in enforcing federal consumer protection laws and protecting consumers from abuse, especially during challenging economic times. As such, certain aspects of the management challenges reflect the ongoing challenges presented by the COVID-19 pandemic response. The major management challenges, in order of significance, are as follows:

- Ensuring an Effective Information Security Program
- Managing Human Capital to Maintain a Talented, Diverse, Inclusive, and Engaged Workforce
- Continuing to Refine the Supervision and Enforcement Strategy
- Managing Consumer Complaints

We routinely monitor the CFPB's efforts to address the management challenges we identify. Our monitoring work includes following up on open recommendations and conducting related audit and evaluation work. We are also attentive to the ongoing legal challenges to the constitutionality of the CFPB's funding mechanism. We understand there is uncertainty regarding the timing and outcome of this litigation, and we note that any effect to the agency or its activities resulting from this litigation may prompt our office to reassess our major management challenges. For information on our ongoing and planned audit and evaluation work, please see our *Work Plan*.

We appreciate the cooperation that we received from the CFPB during our update to the management challenges. If you would like to discuss any of the challenges, please feel free to contact me.

cc: Zixta Martinez
Jan Singelmann
Adam Martinez
Seth Frotman
Karen Andre
David Uejio
Ashwin Vasan
Chris Chilbert
Ren Essene
Joshua Galicki
Dana James
Martin Michalosky
Marianne Roth
Tyshawn Thomas

Contents

Ensuring an Effective Information Security Program

Information security continues to be a key risk area for federal agencies, including the Consumer Financial Protection Bureau, as evidenced by cyberattacks that have targeted software supply chains, key federal systems, and critical infrastructure. The CFPB collects and stores sensitive information, including confidential supervisory information and personally identifiable information, to support many of its mission-critical activities. As such, the implementation and maintenance of an effective information security program is key to ensuring the agency can meet its mission and protect its processes, technology, and data. While the CFPB continues to maintain an effective information security program and is taking multiple steps to strengthen and mature its program, the agency faces challenges in three key areas: (1) full implementation of a zero trust architecture (ZTA),[1] (2) optimal integration of enterprise risk management (ERM) and cybersecurity risk management, and (3) enhanced information technology (IT) supply chain risk management practices.

The CFPB has incorporated specific ZTA concepts into its information security program and has developed a strategy to enable the organization to fully transition to a ZTA by fiscal year 2024, in accordance with federal requirements. However, although the CFPB has established a ZTA working group, successful implementation of a ZTA will require close partnerships and coordination between CFPB business lines and divisions to ensure consistent data classification and appropriate network segmentation. This collaboration will require refinement of governance structures and reporting relationships between various disciplines such as information security, identity, architecture, infrastructure, development, endpoint computing, and data management. In addition, the CFPB will need to implement enterprisewide processes for software asset management and data loss protection to increase cybersecurity monitoring and visibility across its enterprise. Further, while the CFPB has made progress in implementing personal identity verification–based multifactor authentication, it will need to deploy solutions to enable phishing-resistant multifactor authentication on its publicly accessible systems.

The CFPB has also developed an ERM strategy and is in the process of developing risk tolerance levels in accordance with federal guidance. As the CFPB's ERM program continues to mature, the agency will need to ensure that its cybersecurity risk processes align with its ERM processes to maintain an acceptable level of cybersecurity risk for the agency. This includes the implementation of a risk register process to consistently capture, categorize, and prioritize cybersecurity risks across the agency.

Finally, the CFPB will need to ensure that it has effective IT supply chain risk management processes in place, as the agency relies on a variety of third-party-operated and third-party-maintained systems, including cloud computing–based systems, to meet its mission. Specifically, the CFPB will need to strengthen processes to ensure that it has effective insight into and knowledge of the cybersecurity environment of third-party and cloud computing providers. While the CFPB has updated its policies,

[1] A ZTA is a set of system design principles and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. A key principle of a ZTA is the assumption that traditional network perimeters have been compromised and federal agencies must build the appropriate security protections.

procedures, and processes to account for several new IT supply chain risk management requirements, it is still working on implementation and will need to ensure that the agency and its vendors consistently follow secure software development standards. Effective IT supply chain risk management will require close coordination and integration across CFPB divisions and disciplines, such as procurement, ERM, and data management.

Managing Human Capital to Maintain a Talented, Diverse, Inclusive, and Engaged Workforce

An agency's efforts to manage its human capital environment can directly affect its ability to effectively execute its mission and maintain a talented, diverse, inclusive, and engaged workforce. To maintain such a workforce, the CFPB's human capital program should continue focusing on supporting changes to the agency's workplace model, addressing workforce planning, advancing diversity and inclusion initiatives, and addressing pay equity concerns.

Like many other organizations, the CFPB altered its workplace model and pivoted to maximum telework in response to the COVID-19 pandemic. In August 2022, the CFPB reached a final agreement with the National Treasury Employees Union (NTEU) on new workplace flexibility options that include more flexible work locations and schedules. As the agency works to implement these various options, it needs to focus its efforts on how to best support its workforce in adapting to these changes, remaining engaged, and working together in a new hybrid work environment.

The CFPB, through the Office of Human Capital (OHC), has also continued its workforce planning efforts. For example, OHC has conducted workforce reviews and expanded its use of data analytics to identify potential patterns in separations, vacancies, retirement eligibility risks, and promotions. OHC has also designed an executive succession and developmental planning program and plans to build an aspiring leaders program to address findings from its workforce reviews.

In addition, the agency has approved a diversity, equity, inclusion, and accessibility strategic plan. This plan aligns with the agency's need to diversify its employees at higher pay-band levels and to address employees' desire for more equitable advancement and development opportunities. To help address these challenges, the CFPB piloted a program designed to provide lower-pay-band employees with individualized development plans and coaching as well as to identify specific opportunities to support career growth and development. The CFPB is also undertaking several other efforts, including assessing workforce gaps, creating various career development programs, and identifying on-the-job developmental opportunities to further its diversity and inclusion initiatives.

Finally, the CFPB has continued working with the NTEU to reform its compensation structure and pay setting program to address pay equity concerns and foster comparability with federal banking regulators. An agreement between the CFPB and the NTEU included establishing a joint labor-management committee to identify employees' creditable work experience as part of an agencywide salary review and reset. In December 2022, the CFPB and the NTEU ratified an agreement on the reset of employee salaries—using credited experience as the sole basis for resetting pay—and new pay-setting practices that reinforce equity, consistency, and transparency. As the CFPB works to implement its new compensation system, the agency will need to ensure that the workforce perceives the implementation as equitable and transparent.

Continuing to Refine the Supervision and Enforcement Strategy

The CFPB is responsible for ensuring compliance with federal consumer financial laws by supervising market participants and bringing enforcement actions when appropriate. The Dodd-Frank Wall Street Reform and Consumer Protection Act provides the CFPB with the authority to supervise depository institutions with more than $10 billion in total assets; their affiliates; and certain nondepository institutions, such as mortgage companies, payday lenders, private education lenders, and larger participants in other markets as defined by rules issued by the CFPB.

An important objective of the Dodd-Frank Act is to ensure that federal consumer financial laws are enforced consistently for both depository and nondepository institutions, and the CFPB continues to refine its supervision and enforcement strategy in light of this objective. For example, one important aspect of the CFPB's supervision and enforcement strategy is the process used to determine whether to apply supervision or enforcement tools to institutions within the agency's jurisdiction. The CFPB may apply these tools in a variety of circumstances, and the selection and application of such tools are crucial to effective oversight. The CFPB must continue to define and mature its tool selection process to promote efficiency in its oversight and to ensure compliance with federal consumer financial laws. In addition, because there are potentially thousands of nondepository institutions of varying sizes and risk profiles under the CFPB's supervisory jurisdiction and the number of depository institutions within the CFPB's jurisdiction continues to increase, the agency should continue assessing the strategy and resources needed to supervise both depository and nondepository institutions efficiently and effectively. Finally, as the CFPB continues to refine its supervision and enforcement strategy, the agency must also evaluate its human capital needs to ensure that it maintains a workforce with the requisite skills and expertise to execute its strategy, and the CFPB must evaluate its technology needs to support its supervisory and enforcement activities.

Managing Consumer Complaints

Under authority granted by the Dodd-Frank Act, the CFPB collects, monitors, and responds to complaints from consumers on financial services and products. The CFPB has identified in its *Continuity of Operations Plan* the handling of consumer complaints as a mission-essential function that is critical to its strategic contingency planning efforts. The CFPB's Office of Consumer Response receives complaints directly from consumers about the challenges they face in the financial services and products marketplace and uses the complaint data to create reports for its internal CFPB customers.

Since its creation, the CFPB has received more than 4.5 million complaints, and more than 6,000 financial companies have responded to their customers through the CFPB's complaint process. The monthly average complaint volume increased from about 29,000 complaints in 2019 to an average of approximately 83,000 complaints in 2021. Moreover, whereas Consumer Response handled 993,800 complaints in 2021, it handled nearly that same complaint volume in the first 9 months of 2022. As the effects of the pandemic persist, consumers could continue to experience problems such as incorrect credit report information, difficulty paying their mortgages, or medical bill collection. Consumers are also facing new challenges associated with new financial technologies; for example, complaints about crypto-assets continued to increase in 2022.

With an increase in consumer complaints, Consumer Response faces an operational risk with respect to the timeliness with which it can respond to these complaints. To mitigate those challenges, Consumer Response continues to rely on its current processes, including the use of a web form for routing complaints to financial services companies and a remote work environment for its call centers to maintain continuity of services for consumers calling the CFPB. Consumer Response also continues to monitor company response timeliness and to publish data about the timeliness of these responses.

Abbreviations

ERM	enterprise risk management
IT	Information technology
NTEU	National Treasury Employees Union
OHC	Office of Human Capital
ZTA	zero trust architecture

Report Contributors

Josh Dieckert, OIG Manager, Information Technology Audits
Bettye Latimer, OIG Manager, Financial Management and Internal Controls
Lindsay Mough, OIG Manager, Management and Operations
Paul Vaclavik, OIG Manager, Information Technology Audits
Michael Zeitler, OIG Manager, Supervision and Regulation
Andrew Gibson III, Senior OIG Manager for Management and Operations
Jackie Ogle, Senior OIG Manager for Financial Management and Internal Controls
Timothy Rogers, Senior OIG Manager for Operations, Planning, and Policy
Laura Shakarji, Senior OIG Manager for Supervision and Regulation
Khalid Hasan, Assistant Inspector General for Information Technology
Cynthia Gray, Deputy Associate Inspector General for Audits and Evaluations
Michael VanHuysen, Associate Inspector General for Audits and Evaluations

Contact Information

General

Office of Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 202-973-5000
Fax: 202-973-5044

Media and Congressional

OIG.Media@frb.gov

OIG

Hotline

Report fraud, waste, and abuse.

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, web form, phone, or fax.

OIG Hotline
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW
Mail Center I-2322
Washington, DC 20551

Phone: 800-827-3340
Fax: 202-973-5044