FISCAL YEAR 2021 REPORT ON THE FEDERAL TRADE COMMISSION'S TOP MANAGEMENT AND PERFORMANCE CHALLENGES

Federal Trade Commission
Office of Inspector General

OIG Report No. OIG-21-05
September 30, 2021

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Office of Inspector General

September 30, 2021

MEMORANDUM

FROM: Andrew Katsaros
Inspector General

TO: Lina M. Khan, Chair

SUBJECT: FY 2021 Report on the FTC's Top Management and Performance Challenges

The *Reports Consolidation Act of 2000* requires that each agency's inspector general provide an annual summary perspective on the most serious management and performance challenges facing the agency, as well as a brief assessment of the agency's progress in addressing those challenges. The challenges summarized in this document are based on work conducted by the Office of Inspector General (OIG), along with observations and discussions with senior leaders at the Federal Trade Commission (FTC).

In section I, the OIG has identified the following issues as the top management and performance challenges currently facing the FTC:

1. **Securing Information Systems and Networks from Destruction, Data Loss, or Compromise**
2. **Seeking Monetary Relief for Consumers**
3. **Controlling Expert Witness Costs**
4. **Ensuring Mission Success Following the Expiration of Current Evacuation Orders**
5. **Understanding Fraudulent Identity Theft Complaints**

In section II, the OIG has identified **Managing Records and Sensitive Agency Information** as a "watch list" item—an issue that does not rise to the level of a serious management and performance challenge but, nonetheless, requires management's continued attention.

We provided a draft of this report to FTC management, whose comments on the FTC's progress in each challenge area have been summarized and incorporated into this final version.

We appreciate the FTC's ongoing support for the OIG.

I. The FTC's Top Management and Performance Challenges

1. Securing Information Systems and Networks from Destruction, Data Loss, or Compromise

Guarding information technology (IT) systems remains a continuing challenge for the FTC. Our FY 2020 Federal Information Security Modernization Act of 2014 (FISMA) evaluation[1] concluded that the FTC's information security program and practices were effective[2]—however, data breaches, ransomware attacks, and other forms of cyber intrusion remain an ever-present concern.

The Office of Management and Budget's (OMB's) *FY 2020 FISMA Annual Report to Congress*[3] noted that the federal government experienced an 8% increase in reported cybersecurity incidents between FYs 2019 and 2020. The report refers specifically to the December 2020 discovery of a sophisticated supply chain attack[4] used to gain access to a large number of information systems across several federal government agencies and U.S.-based companies.[5]

The FTC has communicated to the OIG how neither tests of controls conducted in accordance with NIST 800-53[6] nor compliance with the Federal Risk and Authorization Management Program (FedRAMP)[7] can effectively mitigate outside supply chain attacks that take advantage of unknown vulnerabilities. The FTC further communicated, in part, how FISMA—largely focused on the exfiltration of high-value assets—did not contemplate threat actors that launch ransomware attacks targeting operational vulnerabilities to extract payment, usually in the form of cryptocurrency. For these reasons, the FTC has chosen to direct its IT resources toward what it considers to be these greater threats to its systems, sometimes in lieu of those identified in NIST 800-53.

---

[1] *Fiscal Year 2020 Audit of The Federal Trade Commission's Information Security Program and Practices*, at 1, FTC OIG (Feb. 12, 2021).

[2] The U.S Department of Commerce National Institute of Standards and Technology (NIST) lists five cybersecurity functional areas: Identify, Protect, Detect, Respond, and Recover. The Council of the Inspectors General on Integrity and Efficiency's FISMA guidance uses NIST's five functional areas to create a five-level maturity model for IGs to rate their respective agencies. *See FY 2020 IG FISMA Reporting Metrics*, at 6, *Cybersecurity & Infrastructure Security Agency*. After assessing all five functional areas, we scored the FTC's overall information security program at level 4 (Managed and Measurable). The Department of Homeland Security has established level 4 (Managed and Measurable) as the effective level for federal program maturity. *See FY 2020 IG FISMA Reporting Metrics*, at 6, Cybersecurity & Infrastructure Security Agency (CISA), (Apr. 17, 2020).

[3] *FISMA FY 2020 Annual Report to Congress*, at 4, OMB (May 2021).

[4] In a *supply chain attack*, hackers infiltrate and exploit a vulnerable feature of an organization's network of systems, including those of outside entities supplying software or IT services to the organization.

[5] This supply chain attack was most commonly associated with a compromise of SolarWinds Orion Code. CISA issued Emergency Directive 21-01 to mitigate similar future incidents.

[6] *NIST Special Publication 800-53*, Revision 5 (September 2020), *Security and Privacy Controls for Information Systems and Organizations*, contains federal information security standards and guidelines, including minimum requirements for federal information systems.

[7] FedRAMP, a product of the U.S. General Services Administration Technology Transformation Services, provides a standardized approach to security authorizations for cloud services.

In FY 2021, the OIG adjusted its approach to FISMA. In response to the changing nature of modern threats to information systems, we held multiple early high-level joint discussions with the FTC to understand better those FISMA compliance risks that the FTC will accept. We also adjusted our document requests to align better with the maturity model approach endorsed by the Council of the Inspectors General on Integrity and Efficiency. In addition, we coordinated with the FTC prior to commencing our penetration testing[8] to better measure the agency's security configurations and security control effectiveness.

Although the OIG made no recommendations in the FY 2020 FISMA report, we identified areas for improvement in risk management, configuration management, and data protection and privacy. Addressing these areas for improvement and positioning itself to detect advanced persistent threats to its systems will help the FTC better ensure that its data and information are properly protected.

FTC Progress in Addressing the Challenge

The Commission reports that it continues to manage essential supporting IT activities by taking a risk-based, cost-effective approach. It describes improvements that include the following:

- pursuing the purchase of Security Operation Center as a Service, as well as augmentation of security services;
- addressing staffing challenges, as required by Executive Order 14028, "Improving The Nation's Cybersecurity";
- mitigating the risk of ransomware and supply chain attacks by updating network controls and increasing monitoring and elevated account usage reporting;
- continuing to implement Trusted Internet Connections (TIC) 3.0-compliant services by partnering with the U.S. Department of Homeland Security (DHS) on the Consolidated Log Aggregation Warehouse service, converting legacy IT systems to modern FedRAMP cloud service offerings using the Cloud First approach, and working with DHS Cybersecurity and Infrastructure Security Agency (CISA) and OMB on a zero-trust architecture; and
- reviewing options to implement continuous diagnostic monitoring and conduct a phishing campaign assessment.

2. Seeking Monetary Relief for Consumers

This year's unanimous Supreme Court ruling in *AMG Capital Management, LLC v. Federal Trade Commission*, 593 U. S. __, 141 S. Ct. 1341 (2021), stripped the FTC of its authority—exercised for more than 4 decades—to seek monetary relief for consumers per Section 13(b). Since 2017, the FTC has secured more than $10 billion through Section 13(b)

[8] This refers to planned, largely web application attack tests to uncover vulnerabilities.

actions in federal court.[9] As a result of the Supreme Court ruling, the FTC will now have to rely on its ability to obtain monetary relief under Sections 5 and 19 of the FTC Act for unfair or deceptive acts or practices.[10]

After this decision, unless there is a violation of an established rule enforceable under Section 19(a)(1), the agency will need to secure cease and desist orders through the administrative process before seeking consumer refunds or other forms of monetary relief in federal court. In other words, the agency will need to litigate the case twice—once through the administrative process and once in federal court—which will significantly increase costs for the agency.

Alternatively, the agency can use the rulemaking process to establish additional rules that cover a wider swath of unfair or deceptive conduct. Establishing additional rules would allow the agency to go straight to federal court pursuant to Section 19; however, rulemaking can be a particularly lengthy and arduous process at the FTC relative to other federal agencies.[11]

While the FTC has traditionally used Section 13(b) to seek equitable monetary relief in consumer protection cases (e.g., in cases like AMG), the FTC more recently has used Section 13(b) to seek monetary relief in antitrust cases as well. Section 19, however, only authorizes the Commission to seek monetary relief for unfair or deceptive practices. Accordingly, because of AMG, the Commission can no longer seek monetary relief for unfair methods of competition.

What remains an open question is whether the Court's decision in AMG signals the ultimate demise of the FTC's ability to seek equitable monetary relief in federal district court in all competition cases—as well as in consumer protection cases that do not involve a rule

[9] *See* https://www.ftc.gov/enforcement/cases-proceedings/refunds/data-refunds-consumers.

[10] Under Section 5(b), the FTC may challenge "unfair or deceptive act[s] or practice[s]" or "unfair methods of competition." Under Section 19(a)(1), the FTC can seek monetary relief directly in federal court for violations of FTC rules governing specific unfair or deceptive acts or practices. Under Section 19(a)(2), the agency also can seek monetary relief, in federal court, for unfair or deceptive acts or practices—but only after the Commission has issued a final cease and desist order in an administrative action, and only if the conduct at issue is also objectively "dishonest or fraudulent" conduct. This process under Section 19(a)(2) requires the FTC to issue a complaint to a respondent that sets forth its charges, which the respondent may settle via a consent agreement. If the respondent elects to contest the charges, the complaint is adjudicated before an administrative law judge for an initial decision, which either complaint counsel or respondent, or both, may appeal to the full Commission. If the Commission rules in favor of complaint counsel, the respondent may appeal to a federal court of appeals and ultimately the Supreme Court. *See* https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority. If the Commission ultimately prevails, the Commission can then initiate a new proceeding under Section 19(a)(2) in federal district court to seek monetary relief. Because this two-step, multi-forum process to obtain monetary relief under Section 19(a)(2) takes years to complete, the Commission historically has not used this pathway often because it is highly inefficient and resource intensive.

[11] *Compare* the FTC's rule making authorities pursuant to FTC Act § 18, 15 U.S.C. § 57a (Section 18), with the Administrative Procedure Act (APA), 5 U.S.C. §§ 551-59, 701-06, 1305, 3105, 3344, 4301, 5335, 5372, 7521 (as amended), which applies to most other federal agencies' rulemaking. In particular, Section 18 is more burdensome than the APA because it requires the FTC to 1) issue an Advance Notice of Proposed Rulemaking for public comment; 2) submit a Notice of Proposed Rulemaking to the FTC's congressional oversight committees; 3) publish a preliminary regulatory analysis under Section 22(b)(1) of the FTC Act; 4) hold hearings that allow interested individuals to present their positions orally, cross-examine witnesses, and rebut submissions to resolve any disputed issue of material fact; 5) publish the presiding officer's proposed resolution of any disputed issue of material fact; and 6) publish a final regulatory analysis under Section 22(b)(2).

violation—without first securing a cease and desist order at the administrative level. For the past few years, the FTC has lobbied Congress to pass legislation affirming the FTC's ability to seek equitable monetary relief directly in federal court. In July 2021, the U.S. House of Representatives passed a bill that would restore the Commission's ability to obtain such relief under 13(b).[12] As of the date of publication of this report, the Senate has not yet considered the bill. Without the passage of legislation, the FTC will continue to have challenges in obtaining monetary relief in a significant portion of its cases.

FTC Progress in Addressing the Challenge

Since the Supreme Court issued its decision in AMG, the Commission has described for the OIG how it has taken steps to mitigate the loss of its equitable monetary relief authority under Section 13(b). First and foremost, the Commission reports that it continues to provide support and technical assistance to Congress on proposed legislation that would restore the Commission's authority to obtain monetary relief under 13(b). The Commission also indicates that it has taken the following steps to retain maximum ability to return money back to harmed consumers:

- re-emphasizing consumer protection cases involving rule violations that allow for obtaining monetary relief pursuant to Section 19(a)(1);
- identifying subject matter areas for potential rulemakings to expand the scope of consumer protection cases enforceable under Section 19(a)(1);
- increasing its use of administrative litigation**;**
- filing federal court cases jointly with state attorneys general who, pursuant to state law, have authority to obtain equitable monetary relief and distribute that relief to harmed consumers nationwide; and
- increasing use of its existing civil penalty authority to hold violators financially liable for their unlawful conduct.

In addition, in several cases filed prior to AMG and pending at the time of the ruling, the Commission reports that it negotiated settlements that included some amount of monetary relief notwithstanding the Commission's loss of its equitable monetary relief authority under Section 13(b).

3. Controlling Expert Witness Costs

The escalating costs of expert witness services represents a significant and continuing risk to the FTC. Between FYs 2014 and 2020, the FTC's costs for expert witness services rose from $7.7 million to $21.3 million, far outpacing FTC appropriation increases over the same period.[13] Once totaled, the FTC expects FY 2021 costs to approach FY 2020

[12] *See* https://www.congress.gov/bill/117th-congress/house-bill/2668.

[13] This 179% increase in expert witness costs is compared to the 11% growth in FTC appropriations from 2014 to 2020 ($298 million vs. $331 million). An FTC appropriation history summary can be found at https://www.ftc.gov/about-ftc/bureaus-offices/office-executive-director/financial-management-office/ftc-appropriation.

levels. Aware of this rapid increase in costs, the FTC has designated its expert witness services as a "top risk" on the agency's risk register since 2017.

We noted, in our November 2019 audit of FTC expert witness services, that the agency's primary hurdle in controlling expert witness costs was its ability to anticipate these costs for individual cases and the program overall.[14] In particular, evolving technologies, automation, and intellectual property issues continue to increase the complexity of antitrust investigations and litigation. This complexity—coupled with a significant increase in the number of complaints about harmful business practices and fluctuations in merger activity—continues to make it difficult for the FTC to anticipate the costs of expert witness services.

In our November 2019 audit, we recommended that the FTC update its approach to acquiring expert witness services. The FTC's Bureau of Economics had previously considered relying more heavily on in-house FTC experts, but noted the difficulty in hiring them, given the higher salaries and increased benefits that academic institutions or other federal agencies are able to offer.[15] Following our 2019 audit, FTC management began revisiting a greater use of in-house economists as experts, understanding that (a) FTC cases often require experts with vast knowledge of a very narrow subject matter and (b) a needed area of expertise could change in each case.

In the FTC's FY 2022 budget request,[16] the agency identified a need to allocate an additional $10,200,000 in FY 2021 for competition-related expert witness needs due to the increased numbers of complex investigations and litigation. This large request for resources—along with the accompanying rationale—highlights the difficulties that unpredictable case demands present as the FTC decides whether or not to commit initially to the use of FTC resources for expert services.

FTC Progress in Addressing the Challenge

FTC management reports that, during the past year, the Bureau of Competition (BC) has performed monthly expert witness cost projections—consistently updating them with data from current cases, abandoned cases, and new cases that may require future expert witness costs. While these projections do not necessarily control costs, FTC management asserts that they do provide better data for prioritizing limited resources.

The FTC also describes how management is leveraging in-house economist resources, when possible, to help reduce the reliance and costs associated with contracting for expert witnesses.

Finally, as noted in the FTC's FY 2022 budget request, an additional $10,200,000 was allocated in FY 2021 for competition-related expert witness needs due to increased numbers of complex investigations and litigation.

[14] *Audit of Federal Trade Commission Expert Witness Services*, OIG Report No. A-20-03, FTC OIG (Nov. 14, 2019).

[15] Carlson J and Koohi S, *Economist Recruiting 2019–2020,* FTC (Apr. 16, 2020).

[16] See Federal Trade Commission Fiscal Year 2022 Congressional Budget Justification.

4. Ensuring Mission Success Following the Expiration of Current Evacuation Orders

In March 2020, the COVID-19 pandemic caused the FTC, along with many federal agencies, to transform its work environment abruptly from primarily in-person to almost entirely remote. Despite the challenges brought on by this sudden shift in the work environment, the FTC was able to continue functioning successfully by

- updating the agency's videoconferencing capabilities and use of videoconferencing;
- maintaining an IT infrastructure suitable for telework;
- regularly posting and updating employee resources related to COVID-19 on the FTC intranet site;
- communicating often and directly with staff about the agency's plans and updated policies and procedures related to COVID-19; and
- providing increased flexibility to employees to deal with the outside demands placed on them due to COVID-19.

As it prepares to implement OMB and U.S. Office of Personnel Management (OPM) guidance[17] related to the work environment following the expiration of emergency evacuation orders, the FTC looks to build on its successes with both in-person and virtual work environments. In creating this new work environment, the FTC, like other federal agencies, will face the following challenges:

- *Continually evolving public health conditions*. As COVID-19 and public health conditions continue to fluctuate and federal guidance is updated in response, the FTC will need a work environment plan that is flexible enough to adapt quickly to the changing conditions, guidance, and reasonable staff concerns. This plan will likely require the FTC to be able to switch quickly between telework and in-person work environments and implement timely mitigation measures, such as masking and social distancing.
- *IT-related challenges*. FTC OCIO has provided regular communication on its services to the current teleworking workforce. Access to files via Microsoft SharePoint and Windows environments remains strong. The Cisco Jabber and separate Zoom communication tools have helped the FTC's bureaus stay connected. IT-related challenges that await include managing those same activities for a hybrid workforce, a laptop refresh that largely will occur remotely, as well as the normal issues that would persist regardless of a remote or in-office posture (e.g., software updates, PIV cards).

Any successes the FTC has achieved in its staff-centered approach to communications and remote technology solutions will likely need to be sustained for an additional indefinite period.

[17] *Additional Guidance on Post-Reentry Personnel Policies and Work Environment*, OPM (July 23, 2021); *Integrating Planning for A Safe Increased Return of Federal Employees and Contractors to Physical Workplaces with Post-Reentry Personnel Policies and Work Environment*, OMB M-21-25 (June 10, 2021).

FTC Progress in Addressing the Challenge

FTC management has described how its Pandemic Response Team (PRT), assembled before the current Evacuation Orders required most Commission staff to work remotely, has ensured the continuity of all operations, helping all operating units adapt to changing conditions.

Recognizing the indefinite nature of current working conditions, the PRT convened several working groups to support the FTC's implementation of OMB, U.S. General Services Administration, and OPM guidance and to communicate the insights of FTC senior management on operating in a hybrid environment.

In addition, OCIO informs the OIG that it intends to update the agency's Information Resource Management Plan and IT Strategy to ensure that the agency's investments in IT infrastructure can support management's considerations for indefinite operations in a hybrid environment.

5. Understanding Fraudulent Identity Theft Complaints

As we first mentioned in our FY 2020 top management and performance challenges report, the FTC faces challenges in addressing an increasing number of potentially fraudulent complaints submitted to IdentityTheft.gov. Administered by the FTC, IdentityTheft.gov provides a web tool for consumers to file identity theft complaints with the federal government.[18] These complaints are housed in the FTC's Consumer Sentinel, which provides members with access to more than 50 million consumer complaints about identity theft and a variety of other issues.

In calendar year 2020, Consumer Sentinel received nearly 1.4 million identity theft complaints from consumers—a more than two-fold increase of the more than 650,000 identity theft complaints received in 2019. This trend persists into 2021: through August 31, 2021, the FTC has received more than 983,000 identity theft complaints, a significant increase in the volume of identity theft complaints compared to the same period in 2020.

As the number of all complaints in Sentinel rise, so does the number of fraudulent ones; the FTC's challenge is in determining the legitimacy of these identity theft complaints. Deliberately false identity theft complaints are submitted for various reasons—including to elude payments on purchases, sell bogus credit repair services to unwitting consumers, or otherwise leverage the effects that a report can have on their credit scores. This exploits features of the Fair Credit Reporting Act and the Fair and Accurate Credit Transactions Act, which together require credit reporting agencies to remove negative information from the credit reports of consumers victimized by identity theft. Users of consumer credit information (e.g., for credit, insurance, or employment purposes) must notify the consumer when an adverse action is taken on the basis of such reports.

An FTC analysis of the complaints received during the first 6 months of calendar year 2021 revealed significant patterns that suggest a possible fraudulent use of IdentityTheft.gov. These patterns foretell a risk to the credibility of a high number of

[18] Consumers can also call a hotline and submit an identity theft complaint via a consumer counselor.

complaints within the system. In addition to raising concerns about violations of federal criminal law,[19] a high volume of fraudulent complaints could require considerable FTC resources in identifying and implementing countermeasures—and, more broadly, could affect the FTC's data and reputational integrity.

FTC Progress in Addressing the Challenge

The FTC reports that it is continuously analyzing IdentityTheft.gov for patterns in complaints to identify those that are potentially fraudulent. It also indicates that it is taking steps to mitigate the harm, such as disallowing system users from downloading and printing suspect complaints. The FTC describes how it is actively collaborating with the OIG and external law enforcement on investigations of IdentityTheft.gov abuse.

II. Agency Watch List

The OIG also maintains a "watch list," currently with one issue that does not meet the threshold of a serious management or performance challenge—but nevertheless warrants the vigilant attention of agency officials.

1. Managing Records and Sensitive Agency Information

The success of the FTC's consumer protection and competition missions increasingly depends on ingesting and integrating, large volumes of complex data into Commission activities—and protecting the data from misuse.

The FTC needs a more consistent application of standard procedures over the collection, organization, and standardization of data. Recent OIG oversight work has identified FTC programs that lack data standards, organized systems,[20] and guidance informing the collection and maintenance of data. This absence of consistent data standards led to breakdowns in data uniformity and program coordination.[21] OIG audits have also found that inconsistent data practices inhibit the systematic and reliable analysis of data.[22] We also identified an absence of effective operating procedures over the management of data, as well as guidance that clearly communicates the roles and responsibilities of key players.[23] The FTC has already begun addressing recommendations associated with our recent findings, including by developing enhanced policy guidance and operating procedures on the management of program data.

In FY 2021, we also noted how (a) FTC employees have multiple methods available to them for accessing nonpublic information, increasing the agency's vulnerability to

[19] Potential criminal violations for submitting fraudulent complaints to IdentityTheft.gov include False Statements (18 U.S.C. § 1001) and Wire Fraud (18 U.S.C. § 1343).

[20] The OIG audits have identified opportunities to better store, manage, query, and retrieve data stored with expanded use of relational database systems.

[21] *Audit of Federal Trade Commission Personnel Security and Suitability Program Processes*, OIG Report No. A-20-09, FTC OIG (Sept. 29, 2020).

[22] *Audit of Federal Trade Commission Redress Process Controls*, OIG Report No. A-20-06, FTC OIG (Mar. 4, 2020).

[23] Ibid.

unauthorized disclosures, and (b) the FTC lacks a comprehensive communication, training, and review strategy covering the prohibition of nonpublic information disclosures. As a result, we identified a need for both better practices for controlling sensitive information and better systems for managing casework.[24]

As the FTC addresses recommendations associated with our recent products, it is also in the process of developing records schedules[25] for its bureaus and offices. Currently, the agency is in the process of placing its records into an array of categories (e.g., case files, support files, technical assistance files, and presentations) while it separates all by time and attempts to identify their owners.

For the foreseeable future, the FTC will continue to refine its records management in numerous ways, including improving on its operations, controlling information releases, and complying with NARA guidelines.

Agency Status

The FTC reports exploring ways to eliminate organizational silos and implement a unified agency-wide method for managing matters, information, and records. For example, the FTC has informed us that it is considering establishing and implementing an agency-wide matter management work flow and recordkeeping system used to conduct and preserve all information and records in NARA-approved formats throughout the lifecycle of each matter.

[24] See *Management Advisory on Controlling and Protecting Sensitive FTC Information*, OIG Report No. M-21-04, FTC OIG (Sept. 29, 2021).

[25] As required by the National Archives and Records Administrations (NARA), records schedules provide agencies with mandatory instructions regarding how to maintain operational records and what to do with them when they are no longer needed for current business. These instructions are required to state whether individual series of records are "permanent" or "temporary," as well as how long to retain the records. Records with historical value, identified as "permanent," are transferred to the National Archives of the United States at the end of their retention period. All other records are identified as "temporary" and are eventually destroyed in accordance with the NARA Records Schedule or the General Records Schedule.