

EXHIBIT 4

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Lina M. Khan, Chair
Rebecca Kelly Slaughter
Alvaro M. Bedoya
Melissa Holyoak

In the Matter of)
)
)

CIVIL INVESTIGATIVE DEMAND TO)
MGM RESORTS INTERNATIONAL,)
DATED JANUARY 25, 2024.)
_____)

File No. 242 3028

ORDER DENYING PETITION TO QUASH OR LIMIT
CIVIL INVESTIGATIVE DEMAND

By SLAUGHTER:

MGM Resorts International (“MGM”) petitions the Commission to quash or limit a Civil Investigative Demand (“CID”) issued on January 25, 2024 (and served on MGM’s registered agent on January 29, 2024, Pet. at 1 n.2). The CID was issued in connection with a Commission investigation into whether MGM’s data security practices comply with: Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45; the Standards for Safeguarding Customer Information Rule (the “Safeguards Rule”), 16 C.F.R. pt. 314; and the Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft (the “Red Flags Rule”), 16 C.F.R. § 681.1. The Commission is also seeking to ascertain whether Commission action to obtain monetary relief would be in the public interest.¹

MGM asks that the CID be either quashed or modified to “strike all references to the Safeguards Rule and the Red Flag Rule, strike Specifications 8–53, which are implicitly premised on those rules, and otherwise tailor the CID to lead to information plausibly relevant . . . without imposing undue burden.” Pet. at 3. For the reasons set forth below, we deny MGM’s petition.

¹ The MGM investigation was initiated pursuant to three Commission resolutions: (1) *Resolution Directing Use of Compulsory Process in Nonpublic Investigation of Acts and Practices Related to Consumer Privacy and/or Data Security*, FTC Matter No. 1823036 (Mar. 14, 2019); (2) *Resolution Directing Use of Compulsory Process in a Non-Public Investigation of Unnamed Persons, Partnerships, Corporations, or Others Engaged in Acts or Practices in Violation of Title V of the Gramm-Leach-Bliley Act, Its Implementing Rules, and/or Section 5 of the FTC Act*, FTC Matter No. 0023284 (July 16, 2019); and (3) *Resolution Directing Use of Compulsory Process in Nonpublic Investigation into the Acts and Practices of Unnamed Persons, Partnerships and Corporations Engaged in Acts or Practices in Violation of 15 U.S.C. § 1681 et seq. and/or 15 U.S.C. § 45*, FTC Matter No. 9923120 (Apr. 15, 1999).

I. BACKGROUND

MGM is a publicly traded, international operator of hotels, casinos, and entertainment venues; it also offers online gaming and sports betting through a subsidiary, LV Lion Holding Limited, and a joint venture, BetMGM, LLC.²

In September 2023, MGM's online network was the subject of a data security breach that apparently exposed the personal identifying information of its customers. *See* Pet. at 1. This was the third publicly known data security incident affecting MGM customers since 2019. Soon after this latest data breach, the Commission initiated a non-public investigation into whether MGM had engaged, or was engaging, in violations of the FTC Act or Commission rules.

On January 25, 2024, in connection with that investigation, the Commission issued the subject CID to MGM, seeking the production of documents and responses to interrogatories. *See* Pet. Exh. 1 (Letter of Jan. 25, 2024, from April J. Tabor to MGM Resorts International c/o Corporation Service Company). The CID had a return date of February 26, 2024. *See* CID Issued to MGM Resorts Int'l, FTC Matter No. 2423028 (Jan. 25, 2024) (hereinafter, the "CID"), at 1.

Following discussions between MGM's counsel and the Commission's investigative staff, Commission staff agreed to modify Specifications 16(e), 18, 19(a), 19(b), 22(b), 22(p), 36, 46, and 53. *See* Pet. Exh. 5 (Letter of Feb. 15, 2024, from Maricela Segura to Brian J. Boyle) at 1–4. In addition, Commission staff agreed to limit the scope of information sought in Specifications 5(a), 22(c), 22(d), 22(u), 25, and 28 to customers located within the United States. *See id.* at 4.

On February 20, 2024, MGM filed its petition to quash the CID. MGM requested that its "Petition and Exhibit 3 be afforded confidential treatment pursuant to 16 C.F.R. § 4.2(d) because they contain competitively sensitive information related to MGM's business operations." Request for Confidential Treatment 1. Along with its request for confidential treatment, MGM filed a redacted public version of its petition, as required by Rule 4.2(d)(4) of our Rules of Practice, 16 C.F.R. § 4.2(d)(4).

II. ANALYSIS

MGM's principal argument against compliance with the CID is that MGM is not subject to the Commission's Safeguards Rule or the Red Flags Rule and therefore the Commission has no authority to demand the information and documents in Specifications 8–53. MGM further challenges the CID on the grounds that the CID would interfere with an ongoing criminal investigation into the 2023 data breach and that it is overbroad, unduly burdensome, and calls for speculation. We address these arguments in turn.

A. Application of the Commission Rules to MGM

MGM claims that it is neither a "financial institution" under the Safeguards Rule nor a "creditor" under the Red Flags Rule. MGM argues that the CID should be therefore quashed because "MGM is not subject to the rules that purportedly authorize the CID and the associated

² *See* MGM Resorts Int'l, Annual Report (Form 10-K) (Feb. 23, 2024), <https://www.sec.gov/Archives/edgar/data/789570/000078957023000008/mgm-20221231.htm>.

investigation.” Pet. at 3. MGM’s jurisdictional claim is not a valid basis for quashing the CID because, at a minimum, the Commission “possesses the authority to investigate whether its jurisdiction extends to [the CID recipient].” Order Denying Petition to Limit and/or Quash Civil Investigative Demand Issued to Firefighters Charitable Foundation, Inc., FTC Matter No. 1023023 (Sept. 23, 2010) (“FCF Order”) at 4. Furthermore, the CID seeks information relevant not only to whether Commission rules were violated but also to whether MGM’s data security practices constitute unfair or deceptive acts or practices that violate Section 5 of the FTC Act, 15 U.S.C. § 45. The latter question alone would validate fifty of the CID’s fifty-three Specifications.³

Administrative agencies have “wide latitude in asserting their power to investigate by subpoena,” and “an individual may not normally resist an administrative subpoena on the ground that an agency lacks regulatory jurisdiction if the subpoena is issued at the investigative stage.” *FTC v. Ken Roberts Co.*, 276 F.3d 583, 586 (D.C. Cir. 2001) (internal quotation marks and citation omitted). Thus, we have rejected arguments such as MGM’s on the grounds that “the FTC has the power to determine whether it possesses jurisdiction over a given matter or entity.” Order Denying Petition to Quash Civil Investigative Demand Issued to Police Protective Fund, Inc., FTC Matter No. 1323239 (May 22, 2014), at 4; *see, e.g., Weinberger v. Hynson, Westcott & Dunning, Inc.*, 412 U.S. 609, 627 (1973) (Agency’s “jurisdiction to determine whether it has jurisdiction is as essential to its effective operation as is a court’s like power.”). Moreover, the CID is issued under Section 20 of the FTC Act, 15 U.S.C. § 57b-1, and our “investigatory authority under Section 20 is broader than [our] enforcement authority under Section 5.” Order Denying Petition To Quash Civil Investigative Demand Filed By Childhood Leukemia Foundation, FTC Matter No. 2223073 (Nov. 15, 2023) (“CLF Order”), at 4. We have held, for example, that, “[t]o the extent that [the CID target] may be claiming that it is not subject to Commission jurisdiction because it is a nonprofit entity, such a claim provides no basis for quashing or limiting the CID.” FCF Order at 4; *accord* CLF Order at 3–4.

Indeed, “each independent regulatory administrative agency has the power to obtain the facts requisite to determining whether it has jurisdiction over the matter sought to be investigated.” *Fed. Mar. Comm’n v. Port of Seattle*, 521 F.2d 431, 434 (9th Cir. 1975). *See also* CLF Order at 5 (“The Commission cannot determine whether CLF is truly operated as a nonprofit without obtaining the information requested through the CID.”); *XYZ Law Firm v. FTC*, 525 F. Supp. 1235, 1237–38 (N.D. Ga. 1981) (rejecting argument that FTC could not investigate a target for potential violations of the Fair Debt Collection Practices Act because the target contended it fell under the statute’s exemption for attorneys).

³ MGM incorrectly claims that Specifications 8–53 are “premised” on the Safeguards and Red Flags Rules. Pet. at 3. In fact, only Specifications 30–32 are premised exclusively on those rules, seeking information related to whether MGM complies with the Red Flags Rule. The remaining Specifications—which seek information concerning whether MGM generally has provided adequate data security to its customers—are also germane to whether MGM engaged in “unfair or deceptive acts or practices” under Section 5 of the FTC Act. Its failure to do so could constitute a law violation. *See, e.g., In the Matter of Drizly, LLC*, FTC Matter No. 2023185; *In the Matter of Blackbaud, Inc.*, FTC Matter No. 2023181; *In the Matter of Chegg, Inc.*, FTC Matter No. 2023151.

The Commission thus has the authority to investigate whether MGM is a “financial institution” or a “creditor” under the Safeguards and Red Flags Rules, respectively, because it “has the power to investigate the facts to determine whether an organization is subject to its regulatory jurisdiction.” CLF Order at 5. The CID here seeks such information. Specification 30, for instance, demands that MGM “[s]tate whether [MGM] regularly and in the ordinary course of business . . . [a]dvances funds,” CID at 9—a jurisdictional requirement under the Commission rules. MGM’s argument that it is not a “financial institution” or a “creditor” is, in other words, premature. Thus, we need not decide now whether the Safeguards and Red Flags Rules apply to MGM.

We do note, however, that MGM’s arguments that it is not covered by the Safeguards and Red Flags Rules appear unpersuasive. The Safeguards Rule applies to “financial institutions”—defined as any “institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities.” 16 C.F.R. § 314.2(h)(1).⁴ The term “financial activities” includes “[l]ending [or] exchanging” money, *id.*; 12 U.S.C. § 1843(k)(4)(A), as well as “check cash[ing] and wire transfer[ing].” 16 C.F.R. § 314.1(b); 12 C.F.R. § 225.86(a)(2)(v). The Red Flags Rule imposes obligations on any “creditor,” which is “any person who regularly extends, renews, or continues credit,”⁵ that “regularly and in the ordinary course of business” (i) “obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction;” (ii) “furnishes information to consumer reporting agencies;” or (iii) “advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person.” 16 C.F.R. § 681.1(b)(5) (citing 15 U.S.C. § 1681m(e)(4)); 15 U.S.C. § 1691a(e). Excepted from that coverage is any creditor that “advances funds on behalf of a person for expenses incidental to a service provided by the creditor to that person.” 15 U.S.C. § 1681m(e)(4).

The coverage of the two Rules overlap: While the Safeguards Rule covers firms that are “significantly engaged” in “[l]ending . . . money,” 16 C.F.R. § 314.2(h)(1); 12 U.S.C. § 1843(k), the Red Flags Rule covers firms that “regularly extend[] . . . credit” and “regularly and in the ordinary course of business . . . advance[] funds,” 16 C.F.R. § 681.1(b)(5) (citing 15 U.S.C. § 1681m(e)(4)); 15 U.S.C. § 1691a(e). The Rules thus share two elements: (1) lending money, extending credit, or advancing funds—which we refer to here as the “Loan Element”; and (2) doing so “significantly” and “regularly and in the ordinary course of business”—which we refer to here as the “Thresholds Element.” MGM appears to satisfy both elements, and thus appears to be subject to both rules.

⁴ The Red Flag Rule also applies to “financial institutions,” but its definition of “financial institutions” differs from that of the Safeguards Rule and does not apply here. *See* 16 C.F.R. § 681.1(b)(7) (citing 15 U.S.C. § 1681a(t)).

⁵ As applicable here, the term “credit” refers to “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.” 15 U.S.C. §§ 1681a(r)(5), 1691a(d).

1. The Loan Element

MGM employs financial instruments called “markers” that “allow a small and highly select group of high-value customers to access funds” for their use in casino gaming. Pet. at 5. MGM describes “markers” to its customers as “essentially a line of credit provided by a casino to a player. It allows you to borrow money from the casino to use for gambling purposes, kind of like a short-term loan for gaming.” BetMGM, *What Can Casino Markers Be Useful For?* (Sept. 26, 2023), <https://casino.betmgm.com/en/blog/what-can-casino-markers-be-useful-for/> (last accessed Mar. 28, 2024). Customers who wish to acquire a marker must first complete a credit application, provide their financial information, and authorize a credit check. MGM then assesses the customer-applicant’s creditworthiness and, if approved, issues the marker. *See id.* When the marker is executed by the customer, MGM issues “casino chips or funds equivalent to the amount” requested by the customer. *Id.* Thus, judging from MGM’s own description of “markers,” they satisfy the “Loan Element” because they allow customers to “borrow money,” either in fungible casino chips or actual money, and allow customers to “incur debts and defer [their] payment.” *See* 15 U.S.C. § 1691a.

MGM argues that its markers are not loans but more akin to post-dated personal checks made out to MGM because, MGM claims, once a marker is executed, it becomes a form of payment “just like personal checks . . . payable to MGM immediately upon presentment to any financial institution.” Pet. at 5. MGM also notes that customers with markers “ ‘settle up’ the same day before they leave the casino, pay within 30 days, or MGM does the equivalent of depositing the post-dated check. Customers do not make regular installment payments, and there are no interest charges.” *Id.* But, regardless of how the marker is enforced, whether cashed at a bank or enforced in court, the marker, as with any financial note, evidences the borrower’s debt to MGM. The marker thus constitutes “credit” because it permits customers to “incur debts and defer its payment or to purchase . . . services and defer payment therefor.” 15 U.S.C. § 1691a(d).

MGM also notes that the Nevada Gaming and Control Board Regulation (“NGCBR”) treats markers as “identical” to personal checks. Pet. at 5. But those regulations also describe markers as “credit instruments.” *See* NGCBR § 6.118.⁶ In addition, MGM itself refers to markers as credit instruments in public filings with federal regulators. MGM’s 2023 annual SEC filing, for example, stated: “We conduct a portion of our gaming activities on a credit basis through the issuance of markers which are unsecured instruments.” MGM’s Form 10-K, *supra* note 2, at 18.

2. The Thresholds Element

MGM also appears to satisfy the Thresholds Element. As we discussed above, a firm is a “financial institution” under the Safeguards Rule if it is “significantly engaged” in lending money, and it is a “creditor” under the Red Flags Rule if it “regularly extends . . . credit” or “regularly and in the ordinary course of business . . . advances funds.” 16 C.F.R. §§ 314.2(h), 681.1(b)(5). MGM argues that its use of markers is de minimis and thus MGM cannot satisfy the

⁶ The NGCBR defines “credit instruments” as “a record which evidences a gaming debt owed to a person who holds a nonrestricted license at the time the debt is created, and includes any record taken in consolidation, redemption or payment of a previous credit instrument.” NGCBR § 6.110 (citing N.R.S. § 463.01467).

Thresholds Element. Pet. at 4–6. Review of publicly available information reveals, however, that MGM’s use of markers likely satisfies the Thresholds Element.

For construction of the term “significantly engaged,” we draw on our published guidance for application of our Privacy of Consumer Financial Information Rule, 16 C.F.R. pt. 313 (“Privacy Rule”).⁷ The Privacy Guide is instructive here because the Privacy Rule employs an identical definition of “financial institution” to that in the Safeguards Rule. *Compare* 16 C.F.R. § 313.3(k), *with* 16 C.F.R. § 314.2(h). The Privacy Guide provides, in relevant parts:

Two factors are particularly important in determining whether you are “significantly engaged” in a financial activity. *First, is there a formal arrangement?* A storeowner or bartender who “runs a tab” for customers is not considered to be significantly engaged in financial activities, but a retailer that offers credit directly to consumers by issuing its own credit card would be covered. *Second, how often does the business engage in a financial activity?* A retailer that lets some consumers make payments through an occasional lay-away plan is not “significantly engaged” in a financial activity. In contrast, a business that regularly wires money to and from consumers is significantly engaged in a financial activity.

Privacy Guide, supra note 7, at 2–3 (emphasis added). MGM’s statements and public filings show that both factors are met in MGM’s use of markers. First, whenever MGM issues a customer a marker, MGM requires the customer to sign a financial note promising to pay back the loaned funds. *See* Pet. Exh. 3 (Decl. of Amy Wong) at 1. That evinces a “formal arrangement” between MGM and those customers to whom it issues markers. Second, MGM issues markers to its customers “regularly.” MGM’s website instructs consumers on how to establish “casino credit,” by “obtain[ing] a Marker Limit Application on our website,” which “contain[s] specific directions for processing the application,” or by contacting “our Casino Credit Department.”⁸ Thus, MGM has an established process and infrastructure for “regularly” issuing markers, including an online application,⁹ and a dedicated Casino Credit Department to assess those applications.

Moreover, MGM’s public filings show that its use of markers is not de minimis but in fact a crucial component of its business. In its 2023 annual report to the Securities and Exchange Commission, MGM emphasized the central role of markers in its business:

⁷ *See* Fed. Trade Comm’n, *How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act: A Guide for Small Business from the Federal Trade Commission* (July 2002), <https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf> (“Privacy Guide”).

⁸ *See* MGM Resorts, *General Questions*, <https://www.mgmresorts.com/en/faq.html#/how-do-i-establish-casino-credit> (last accessed Mar. 28, 2024).

⁹ *See* MGM Resorts, *Casino*, <https://www.mgmresorts.com/en/casino.html#/Marker%20Limit%20Forms> (last accessed Mar. 28, 2024).

[W]e extend credit to a large portion of our customers and we may not be able to collect gaming receivables. . . . [H]igh-end players typically are issued more markers than patrons who tend to wager lower amounts. High-end gaming . . . may have a significant positive or negative impact on cash flow and earnings in a particular quarter. . . . Uncollectible receivables from high-end customers could have a significant impact on our results of operations.

MGM’s Form 10-K, *supra* note 2, at 18. In view of these representations, MGM’s current argument that it does not meet the Thresholds Element because it issues markers to only “select high-volume customers,” Pet. Exh. 3 ¶ 7 (MGM issued markers in 2023 to 5,130 of about 3.3 million Las Vegas customers), is unpersuasive. Even if the number of customers who receive markers constitutes a low percentage of MGM’s total gambling base, these customers, according to MGM’s SEC filings, still have a “significant positive or negative impact on cash flow and earnings.” MGM’s Form 10-K, *supra* note 2, at 18. Furthermore, MGM’s petition contains no information about the number of customers who receive markers at its non-Las Vegas casinos, or about how much value was transferred in markers in 2023. These are examples, however, of the information that can be determined through the investigation.

MGM’s other arguments that it is not covered by the Safeguards and Red Flags Rules are likewise unpersuasive. MGM argues that it is exempt from the Red Flags Rule because the markers are “wholly incidental to the entertainment services MGM provides.” Pet. at 4. MGM misconstrues the Rule’s language. The Red Flags Rule creates an exception for creditors that advance funds for “expenses incidental to a service provided by the creditor to that person.” 15 U.S.C. § 1681m(e)(4)(B). The question therefore is not whether the advancing of funds is itself incidental but whether the funds are advanced to cover an *expense that is incidental* to a service provided by the creditor. Here, MGM’s markers are not used to cover an “incidental expense”; they are used to allow MGM’s customers to gamble—the central activity in MGM’s gaming business. Indeed, the legislative history of the Red Flags Rule shows that the “incidental expenses” language was intended to cover circumstances such as ensuring that lawyers may advance funds to pay for services such as expert witnesses or that lawyers and doctors may bill in arrears for past services provided, without becoming “creditors” under the rule. *See* 156 Cong. Rec. S8288-9 (daily ed. Nov. 30, 2010) (statements of Senators Thune and Dodd). Thus, the “incidental expense” exclusion plainly does not apply to MGM’s issuance of markers.

Equally unpersuasive is any suggestion that MGM falls under the Safeguard Rule’s exclusions for “common and informal retail practices that are designed for the convenience of the customers, such as ‘lay away’ and deferred payment plans, and the practice of allowing customers to ‘run a tab.’ ” Pet. at 4 (citing 16 C.F.R. § 314.2 (h)(3)). *See* 16 C.F.R. § 314.2(h)(4). These examples do not even resemble MGM’s practice of issuing markers after its customers complete credit applications, provide their financial information, and authorize credit checks.

MGM also argues, citing *American Bar Association v. FTC*, 671 F. Supp. 2d 64 (D.D.C. 2009), *vacated*, 636 F.3d 641 (D.C. Cir. 2011) (“*ABA*”), that applying the Safeguards and Red Flags Rules to MGM would exceed the FTC’s authority. *See* Pet. at 6–7. MGM is mistaken. The district court in the *ABA* case was addressing a prior version of the Red Flags Rule, which had defined a creditor simply as someone who permitted a debtor to “defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.” *ABA*, 671 F. Supp. 2d at 75. As the D.C. Circuit explained in vacating the district court

ruling as moot, however, Congress later passed the Red Flag Program Clarification Act, which revised the then-existing Red Flags Rule. *ABA*, 636 F.3d at 643. The revision, among other things, “makes it plain that the granting of a right to ‘purchase property or services and defer payment therefore’ is no longer enough to make a person or firm subject to the FTC’s Red Flags Rule—there must now be an explicit advancement of *funds*.” *Id.* at 646–47. That is what the current version of the Rule requires, *see* 16 C.F.R. § 681.1(b)(5), and that appears to be the case here: MGM advances funds to its customers via the issuance of markers, so it qualifies as a “creditor” under the Red Flags Rule. The *ABA* case thus supports our analysis here and supports the Commission’s use of its investigative power to collect this information.

Lastly, we note that MGM’s issuance of markers is not the only basis for applying the Safeguards and Red Flags Rules to MGM. The Safeguards Rule also applies to firms that are “significantly engaged” in “exchanging money” or “check cashing” services. 16 C.F.R. § 314.2(h) (citing 12 U.S.C. § 1843(k)(4)(A)). And the Red Flags Rule also applies to a firm that “regularly extends . . . credit” and “regularly and in the ordinary course of business . . . uses consumer reports . . . in connection with a credit transaction.” 15 U.S.C. § 1691a(e); 16 C.F.R. § 681.1(b)(5) (citing 15 U.S.C. § 1681m(e)(4)). MGM appears to engage in all these activities. MGM’s website tells consumers that MGM will “cash in foreign currency at the casino cage, at no charge” and “cash traveler’s check [sic] at the casino cage and there in [sic] no charge for this service.”¹⁰ MGM also uses “credit reports to evaluate marker applications.” *Pet.* at 6 n.4. In 2023, MGM obtained 4,559 credit reports in relation to its Las Vegas markers alone. *See id.* Whether this MGM conduct meets the thresholds for “significant” and “regular” under the Rules is one of the questions that the CID seeks to answer. Specification 30 asks, for instance, whether MGM “regularly and in the ordinary course of business . . . uses Consumer Reports.” CID at 9. As noted above, the Commission is entitled to information relevant to determining whether it has regulatory jurisdiction over a particular matter or person. The CID here is a proper exercise of that investigative power as well.

In sum, the CID is validly issued, not only to investigate potential violations of Section 5 of the FTC Act, 15 U.S.C. § 45, but also to investigate whether MGM is in fact subject to the requirements of the Safeguards and Red Flags Rules. Judging from MGM’s own statements and public filings, there are strong grounds to believe that it could be.

B. Interference with Other Law Enforcement Investigations

MGM advances three arguments, all without merit, in support of its claim that compliance with the CID may interfere with other ongoing federal law enforcement investigations and prosecutions relating to the 2023 data breach. *Pet.* at 7–8. First, MGM contends that requiring the victim of a possible crime to produce information that it provided to other law enforcement agencies could have a chilling effect on victims’ willingness to cooperate with law enforcement agencies. *Pet.* at 8. While recognizing MGM’s own harm from the data breach, the FTC’s investigation seeks to vindicate the rights of consumers, including those MGM customers whose data was exposed. MGM has not explained how or why the FTC’s efforts to protect the rights of those consumer-victims will diminish MGM’s willingness to cooperate in an

¹⁰ *See* MGM Resorts, *General Questions*, <https://www.mgmresorts.com/en/faq.html> (last accessed Mar. 28, 2024).

investigation to find out who was behind the data breach. Without any such explanation, we cannot accept this argument as grounds for quashing the duly issued CID.

Second, MGM argues that “the fact that any particular information was provided to law enforcement—particularly by a crime victim—in no way entitles [Commission] Staff to that information.” Pet. at 8. MGM misapprehends the scope of the CID. Particular information does not become responsive to the CID because it was shared with other law enforcement agencies. Rather, the information is responsive if it falls within the scope of the enumerated Specifications. At the same time, the fact that some responsive information had been shared with other law enforcement agencies is no basis to withhold it in this investigation.

Third, MGM argues that complying with the CID could interfere with ongoing criminal investigation conducted by the Federal Bureau of Investigation. *See* Pet. at 7–8. This is mere speculation. MGM did not identify a single responsive document or piece of information—real or hypothetical—the production of which could interfere with the FBI’s investigation. MGM cites to the Supreme Court’s decision in *United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950), for the proposition that “[f]orcing a crime victim to be an intermediary between FTC staff and federal law enforcement during ongoing criminal investigations and prosecutions is beyond the scope of FTC’s legitimate investigatory power.” Pet. at 8. To start, the CID does not require MGM to act as an intermediary between the FTC and the FBI; instead, it seeks information that MGM has in its possession, custody, or control. Further, *Morton Salt* in fact militates in favor of—not against—MGM’s compliance with the CID. In that case, the Supreme Court reaffirmed that the FTC, as a law enforcement agency, has a “legitimate right to satisfy [itself] that corporate behavior is consistent with the law.” 338 U.S. at 652.

C. Overbreadth, Undue Burden, and Vagueness

MGM argues that the CID’s applicable time frame is too broad, that the CID’s “catch-all” demands are impermissible, and that some of the interrogatories seek irrelevant information or are unduly burdensome or vague. We address these arguments in turn, but we note first the high thresholds that MGM must pass to establish the overbreadth and undue burden of an agency’s investigative demand.

“Needless to say, any subpoena places a burden on the person to whom it is directed.” *FTC v. Shaffner*, 626 F.2d 32, 38 (7th Cir. 1980). At a minimum, the gathering of information necessary to comply will consume time and resources that could otherwise be directed to other activities. But that is the cost we all pay for living under the rule of law. *See FTC v. Standard Oil Co. of Cal.*, 449 U.S. 232, 244 (1980) (“[T]he expense and annoyance of litigation is part of the social burden of living under government.”) (internal quotation marks and citation omitted). “Some burden on subpoenaed parties is to be expected” and is indeed “necessary in furtherance of the agency’s legitimate inquiry and the public interest.” *FTC v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977).

Accordingly, “the presumption is that compliance should be enforced to further the agency’s legitimate inquiry into matters of public interest.” *Shaffner*, 626 F.2d at 38. Overcoming that presumption demands a strong showing: “courts have refused to modify investigative subpoenas unless compliance threatens to unduly disrupt or seriously hinder normal operations of a business.” *Texaco*, 555 F.2d at 882. The burden of that showing is on the subpoenaed party and is not easily met where the agency demand is pursuant to a lawful purpose

and the demanded information is relevant to that purpose. *See id.* Moreover, to make that showing, MGM must come forward with more than conclusory or unsupported statements. *See FTC v. Standard Am., Inc.*, 306 F.2d 231, 235 (3d Cir. 1962). MGM “may not merely utter the claim; it must persuade us.” *FTC v. Jim Walter Corp.*, 651 F.2d 251, 258 (5th Cir. 1981).

1. The CID’s Applicable Time Period

MGM argues that the CID’s applicable time period—from January 1, 2021, to the date of MGM’s full compliance—is unreasonable because it “long precede[s] the incident giving rise to the investigation,” in late 2023, and MGM’s practices in the prior years have “no bearing on the reasonableness of [MGM’s] security practices in 2023.” Pet. at 10. We disagree. The applicable time period is reasonably tailored to cover the significant events and policy decisions by MGM leading up to the 2023 data breach. Since 2019, MGM apparently has experienced at least three data security breaches, including the one that is the subject of this investigation. In mid-2019, for instance, MGM reportedly suffered a data breach that was not publicly disclosed until February 2020, in which the personal information of 142 million MGM customers was offered for sale on the dark web.¹¹ And, in December 2022, BetMGM, an MGM subsidiary, disclosed a data breach that had occurred in May 2022.¹²

MGM has represented to consumers after each of these incidents that it had enhanced its data security.¹³ An assessment of whether MGM in fact has implemented a reasonable and effective data security program will require consideration of several factors, including MGM’s own assessment of its cybersecurity risk relative to the size and complexity of its business, the nature and scope of its activities, and the sensitivity of the information at issue. *See Fed. Trade Comm’n, FTC Safeguards Rule: What Your Business Needs to Know* (May 2022), <https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know>. Given MGM’s history of breaches, the number of consumers previously affected and currently at risk, the sensitivity of the data at issue, and MGM’s repeated representations that it

¹¹ *See* Catalin Cimpanu, *A Hacker Is Selling Details Of 142 Million MGM Hotel Guests On The Dark Web*, ZDNET (July 13, 2020), <https://www.zdnet.com/article/a-hacker-is-selling-details-of-142-million-mgm-hotel-guests-on-the-dark-web/>.

¹² *See* Office of the Maine Attorney General, *Data Breach Notification by BetMGM, LLC*, <https://apps.web.maine.gov/online/aeviewer/ME/40/ef5d2df4-691f-4471-b476-5459bf590bae.shtml>.

¹³ *See* MGM Resorts, *Notice of Data Breach* (Oct. 5, 2023), at 1 (“We take the security of our systems and data very seriously and have put in place additional safeguards to further protect our systems”), <https://apps.web.maine.gov/online/aeviewer/ME/40/37d6cb69-b76c-48b5-8d46-d68bb59a5df5/97db0fa5-7ac6-4c90-951b-501a146f3e73/document.html>; Letter from Adam Greenblatt, CEO, to BetMGM Customers dated December 21, 2022, at 1 (“We are coordinating with law enforcement and taking steps to further enhance our security.”), <https://apps.web.maine.gov/online/aeviewer/ME/40/ef5d2df4-691f-4471-b476-5459bf590bae/1dd2a54e-2e3b-4486-856b-b78a3f42fc49/document.html>; MGM Resorts, *Notice of Data Incident* (Aug. 30, 2019), *attached to* Letter from Matthew E. Yarbrough to Gordon MacDonald, Attorney General of New Hampshire, at 1 (“We have implemented additional safeguards to improve further data security related to external software incidents.”), <https://www.doj.nh.gov/consumer/security-breaches/documents/mgm-resorts-20190904.pdf>.

has improved its data security systems since 2019, the applicable time period, looking back to January 2021, is both narrowly tailored and necessary to obtain information relevant to the investigation.

2. The CID's "Catch All" Provisions

MGM contends that Specifications 17 and 46 are overbroad and unduly burdensome.¹⁴ Citing our decision on a petition to quash in the Amazon ROSCA matter,¹⁵ MGM argues that these two specifications should be struck as "catch all" questions. Pet. at 11. MGM's arguments are unpersuasive.

The Commission may demand, via compulsory process, any sufficiently described document or information that is "relevant to the investigation—the boundary of which may be defined quite generally" by the Commission. *FTC v. Invention Submission Corp.*, 965 F.2d 1086, 1090 (D.C. Cir. 1992) (emphasis omitted). Indeed, administrative agencies are to be accorded "extreme breadth" when conducting a duly authorized investigation. *Linde Thomsen Langworthy Kohn & Van Dyke, P.C. v. Resol. Tr. Corp.*, 5 F.3d 1508, 1517 (D.C. Cir. 1993).

MGM does not contend that Specifications 17 and 46 fail to clearly define the information sought. Rather, MGM takes issue with their style of language, such as Specification 17's call for information "to the extent not discussed in response to another Specification," which MGM characterizes as "catch-all." MGM thus compares these two Specifications to the CID demand we denied in the Amazon ROSCA matter, but that comparison is inapt. At issue in the Amazon ROSCA matter was a demand for witness testimony regarding "[a]ny additional topic or topics covered by the [CID]." Amazon ROSCA Order at 5. Significantly, the so-called "catch-all" provisions there allowed Commission staff "to identify additional topics for testimony within the scope of the . . . CID with two weeks' notice." *Id.* at 13 (emphasis added). In those circumstances, we found the demand for testimony unreasonable because "the Commission must still provide sufficient information for a CID recipient to evaluate the request, prepare

¹⁴ Specification 17 states: "Describe in detail the steps the Company has taken to prevent unauthorized access to its Administrative Tools, to the extent not discussed in response to another Specification, and state the date upon which each described step was implemented and, if applicable, terminated. In particular, describe in detail the Company's use for its Administrative Tools of intrusion detection, multi-factor authentication, data loss prevention, least privilege access controls, or similar technologies, and, if applicable, the reasons why the Company chose not to use such technologies for its Administrative Tools." CID at 5. Specification 46, as amended, states: "Produce all Documents created, received, or disseminated by the Company regarding the discovery, response, investigation, management, remediation, and reporting of the security incident(s) affecting the Administrative Tools that the Company identified in September 2023." Pet. Exh. 5 at 4.

¹⁵ See Order Granting in Part and Denying in Part Omnibus Petition to Limit or Quash Civil Investigative Demands, *In the Matter of Civil Investigative Demands Dated June 30, 2022, to Amazon.com, Inc. and Certain Current and Former Amazon Employees*, FTC Matter No. 2123050 (Sept. 21, 2022), https://www.ftc.gov/system/files/ftc_gov/pdf/2123050AmazonPTQOpinion.pdf ("Amazon ROSCA Order").

sufficiently, or otherwise seek an administrative remedy.” *Id.* The CID demand for testimony there “as written” failed to “allow for those outcomes.” *Id.*

That is not the case here. Specifications 17 and 46 are “ ‘sufficiently definite to provide guidance as to what is to be produced.’ ” *Resol. Tr. Corp. v. Greif*, 906 F. Supp. 1446, 1452 & n.2 (D. Kan. 1995) (quoting *In re Grand Jury Proceedings*, 601 F.2d 162, 168 (5th Cir. 1979)). We note that, in response to MGM’s concerns, Commission staff has modified Specification 46 to further particularize the requested documents.

In the end, MGM’s petition does not provide much beyond the conclusory statement that the Specifications are not “sufficiently definite.” Pet. at 11. That is not enough to carry MGM’s burden. *See Standard Am.*, 306 F.2d at 235; *Jim Walter Corp.*, 651 F.2d at 258. We thus reject MGM’s challenge to Specifications 17 and 46.

3. Relevance and Undue Burden

MGM next argues that the information sought in the CID is unduly burdensome because it would require “significant investigation and analysis.” Pet. at 9. The CID requests information concerning: (1) MGM’s basic corporate structure and operational control; (2) MGM’s data security practices, (3) the September 2023 data breach, and (4) MGM’s identity theft detection, prevention, and mitigation practices. This information is not unique to the FTC’s investigation. By virtue of its gaming license under Nevada state law, MGM is subject to regulatory demands for similar information.¹⁶ MGM has already provided information about the 2023 data breach to federal law enforcement. *See* Pet. at 7. And MGM is defending civil lawsuits stemming from the most recent and prior data breaches,¹⁷ in which it will likely have to produce similar information.

MGM’s only support for its claim of undue burden is the one-page affidavit of MGM’s Chief Information Security Officer, John Branden Newman, which states that compliance with the CID would require “substantial work on [Newman’s] part, as well as from other employees,” and would “distract [Newman] and others from [their] ordinary duties at MGM.” Pet. Exh. 4 ¶ 4. The affidavit also states—without specificity or substantiation—that compliance with the CID “is likely to significantly adversely affect MGM and interfere with the responsibilities of the individual employees involved.” *Id.* ¶ 6. As we noted above, however, mere distraction from ordinary corporate duties, and even the need to expend substantial effort on responding to the CID, does not constitute undue disruption or serious hindrance of normal business operations for

¹⁶ The Nevada Gaming Control Board, for example, requires covered entities such as MGM to investigate cyber attacks and, upon request, provide reports of the results of their investigation, including “the root cause of the cyber attack, the extent of the cyber attack, and any actions taken or planned to be taken to prevent similar events that allowed the cyber attack to occur.” NGCBR § 5.260(4)–(7).

¹⁷ *See, e.g.*, Mot. to Compel Discovery, *In re MGM Resorts Int’l Data Breach Litig.*, No. 2:20-cv-00376-GMN-NJK, ECF No. 200 (D. Nev. filed Feb. 20, 2024). *See also* David Jones, *MGM Resorts Warns Customers of Fraud as It Faces Class Action Lawsuits*, Cybersecurity Dive (Sept. 25, 2023), <https://www.cybersecuritydive.com/news/mgm-resorts-negligence-lawsuits-cyber/694618/>.

a firm. *See Texaco, Inc.*, 555 F.2d at 882. The burden imposed on MGM is the kind routinely expected from any form of compulsory process.

MGM contends that Specifications 33–37 in particular, which seek the identities of the individuals responsible for MGM’s corporate functions—including data security compliance—are overbroad and unduly burdensome because they are “not relevant to this investigation into the Company’s cyber security practices.” Pet. at 12. We disagree. Identifying the MGM employees and corporate officers responsible for the design and implementation of MGM’s data security programs and for making representations to the public about MGM’s data security is plainly necessary to evaluating both the reasonableness of MGM’s data security practices and whether those practices or representations amount to unfair or deceptive acts or practices under Section 5 of the FTC Act.

MGM also complains that Specifications 5–6 are overbroad and unduly burdensome because they seek information about all of MGM’s consumer products and services, and the type of personal consumer information MGM collects in association with each. Pet. at 12. These requests are necessary to understand the nature and volume of consumer data collected by MGM—which, in turn, bear heavily on the reasonableness of MGM’s data security practices. As we have held before, a CID demand is not unreasonably broad “where the breadth of the inquiry is in large part attributable to the magnitude of the subject’s business operations.” Amazon ROSCA Order at 10 (citing *Texaco*, 555 F.2d at 882).

4. Vagueness

MGM contends that particular terms in several of the CID specifications are vague and ambiguous and therefore should be quashed or modified. *See* Pet. at 13. “A request is impermissibly vague where it lacks reasonable specificity or is too indefinite to allow a responding party to comply.” Order Denying Petition to Quash, *In the Matter of Innovative Capital Strategies, Inc.*, FTC Matter No. 2023164 (May 24, 2021), at 5. We address MGM’s contentions in turn.

First, MGM contends that the following underlined terms in Specifications 13 and 14 are impermissibly vague:

- Specification 13: “Describe in detail the Company’s incident response practices, policies, and procedures for its Administrative Tools, and state the date upon which each described practice, policy, and procedure was implemented and, if applicable, terminated.” CID at 5.
- Specification 14: “Describe in detail the Company’s software update practices, policies and procedures for its Administrative Tools, and state the date upon which each described practice, policy, or procedure was implemented and, if applicable, terminated.” *Id.*

More specifically, MGM’s counsel elaborated during a February 14, 2024, meet and confer that MGM sought to understand the difference between a “practice,” a “policy,” and a “procedure.” In response, Commission staff explained that “policies” refer to official, high-level instructions; that “procedures” refer to the standard protocols for what specific steps to take in

particular circumstances, such as a data breach; and that “practices” refer to the steps actually taken in such circumstances, to the extent they differ from the procedure.

Thus, in light of those clarifications, Specification 13’s reference to “incident response practices” would include a description of what MGM’s employees actually did in response to previous data security incidents. Likewise, Specification 14’s reference to “software update practices” would include how MGM’s employees carried out the software updates. We find neither impermissibly vague.

Second, MGM contends that the following underlined language in Specification 22 is vague and ambiguous: “Describe in detail the security incident(s) occurring during September 2023 in which an unauthorized person(s), among other things, obtained access to Your Administrative Tools and exfiltrated Your customer accounts and Personal Information” Pet. at 13. During the above-referenced February 14, 2024, meet and confer, Commission staff explained to MGM’s counsel that the phrase “among other things” was intended to capture conduct that the unauthorized persons may have taken *in addition* to obtaining access to MGM’s administrative tools and exfiltrating customer data. In light of this clarification, we find the Specification is not impermissibly vague.

Lastly, MGM contends that the following underlined language in Specification 33 is vague and ambiguous: “Identify all officers, directors, principals, owners of the Company or other individuals who have had the authority to control the Company’s data security and information privacy practices, policies, and procedures, either collectively or individually, during the Applicable Time Period. The response should include all individuals who have or had the ability to control or participate in the Company’s practices, policies, and procedures related to compliance with the Red Flags Rule, 16 C.F.R. § 681.1.” Pet. at 13. MGM’s petition does not explain how or why the underlined language is vague, and thus MGM fails to carry its burden in challenging this Specification. *See Standard Am.*, 306 F.2d at 235; *Jim Walter Corp.*, 651 F.2d at 258. In any event, Specification 33 plainly seeks the identities of all individuals responsible for MGM’s efforts to comply with the Red Flags Rule.

5. Call for Speculation

Finally, MGM claims that Specifications 9 and 22 seek information that is still being investigated by law enforcement, rendering any MGM responses speculative. Pet. at 13. Again, MGM “may not merely utter the claim; it must persuade us.” *Jim Walter Corp.*, 651 F.2d at 258; *accord Standard Am.*, 306 F.2d at 235. MGM fails to do so. It provides no support for its claim, and it does not explain how or why any responses would be speculative. We thus reject MGM’s challenge for failing to carry its burden.

Moreover, even a casual scrutiny of the challenged provisions shows MGM’s claim to be meritless. Specification 9 states: “Describe in detail the Company’s employee training related to phishing or spearphishing attempts by email, phone, or otherwise, and state the date upon which each type of training occurred during the Applicable Time Period.” CID at 3. This plainly calls for information within MGM’s own knowledge, possession, or control. We fail to see how the ongoing law enforcement investigation would make such information speculative.

Likewise, Specification 22 seeks information about how the cybercriminals breached MGM’s data security and obtained its customers’ personal information. The Specification does

not seek information from any source other than MGM itself, and indeed most sub-parts explicitly seek information from MGM's perspective. MGM does not explain why that would be speculative. Nor can we. And, during the February 14, 2024, meet and confer, MGM's counsel did not raise any other specific objections to these specifications.

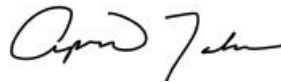
III. CONCLUSION

For the foregoing reasons, MGM's petition to quash is denied.

IT IS HEREBY ORDERED THAT MGM Resorts International's Petition to Quash or Limit the January 25, 2024, Civil Investigative Demand be, and hereby is, **DENIED**.

IT IS FURTHER ORDERED THAT MGM shall comply in full with the Civil Investigative Demand no later than **April 15, 2024 at 9:00 a.m. (Pacific Time)**, or at such other date, time, and location as the Commission staff may determine.

By the Commission, Commissioner Holyoak not participating.¹⁸



April Tabor
Secretary

¹⁸ On March 18, 2024, MGM also filed a petition to recuse or disqualify Chair Khan. *See* MGM Resorts Int'l, Pet. to Recuse or Disqualify Chair Lina Khan, In re Civil Investigative Demand, FTC Matter No. 2423028 (Mar. 18, 2024). Although the Office of the Secretary rejected MGM's filing as not compliant with 16 C.F.R. § 4.17, we would deny MGM's petition even if it were properly filed. MGM first argues that, because Chair Khan was visiting an MGM property when the breach occurred, she has pre-existing personal knowledge of the facts that requires her recusal from the case. But, as MGM's motion makes clear, this so-called pre-existing knowledge consists simply of knowing that a breach occurred and that MGM's operations were disrupted, facts that have been widely reported in the news. That Chair Khan learned of the breach while an MGM hotel guest is not legally significant and stands in stark contrast to cases MGM cites as supporting recusal. *See Williams v. Pennsylvania*, 579 U.S. 1, 11–14 (2016) (judge having “significant, personal involvement in a critical trial decision” while still a prosecutor); *Caperton v. A.T. Massey Coal Co.*, 556 U.S. 868, 886 (2009) (state justice's campaign receiving “extraordinary contributions” from litigant in a pending case); *In re Murchison*, 349 U.S. 133, 134–35 (1955) (judge apparently relying on personal knowledge and impressions that could not be tested by adequate cross-examination); *Am. Cyanamid Co. v. FTC*, 363 F.2d 757, 767 (6th Cir. 1966) (Chairman serving as trier of fact even though he had “investigated and developed many of these same facts” while serving as counsel to a Senate subcommittee). MGM has not pointed to a single case supporting recusal on facts close to these. MGM next suggests that Chair Khan could be a plaintiff against MGM or otherwise participate in one of the fifteen class actions that have been filed. Even if this were a basis for recusal, Chair Khan voluntarily elects to waive any interest that she may have in any relief resulting from the filed class actions or any substantially related matter—thus extinguishing any potential financial conflict arising from these actions.

SEAL:

ISSUED: April 1, 2024

