UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

| | | |
|---|---|---|
| *In re* Civil Investigative Demand to MGM Resorts International | ) | FTC File No. 2423028 |

# MGM Resorts International's Petition to Quash or Limit Civil Investigative Demand

February 20, 2024

Brian J. Boyle
DLA Piper LLP
500 8th St NW
Washington, DC 20004
(215) 656-2450
brian.boyle@us.dlapiper.com

Andrew Sacks
DLA Piper LLP
701 Fifth Avenue, Suite 6900
Seattle, Washington 9810
(206) 839-4890
andrew.sacks@us.dlapiper.com

*Counsel for Petitioner*
(additional counsel listed below)

# MGM RESORTS INTERNATIONAL'S PETITION TO QUASH OR LIMIT CIVIL INVESTIGATIVE DEMAND

## I. Introduction

In early September 2023, Petitioner MGM Resorts International ("MGM" or the "Company") was the victim of a debilitating cyberattack. As was widely reported at the time, the attacked forced MGM to temporarily run its business—which sprawls across numerous properties in the United States and serves millions of customers—without the use of the IT systems that help make its casinos and resorts best-in-class. The attack cost MGM dearly. Although MGM was eventually able to restore its IT systems, the aftershock of the cyberattack continues to reverberate months later, and MGM is cooperating with law enforcement agencies seeking to bring those responsible to justice.

MGM's misfortune that day was compounded by the presence of a powerful public figure at its Las Vegas hotel during the attack. According to press reports, Federal Trade Commission ("FTC") Chair Lina Khan and an unnamed senior aide were guests at the hotel and were inconvenienced by the attack.[1] That senior aide then provided comments to the press about the event.

Notwithstanding MGM's victimization and the substantial cost (financial and otherwise) the Company has already incurred, on January 25, 2024, FTC Staff issued a Civil Investigative Demand ("CID") to MGM seeking reems of documents and information.[2] (Ex. 1.) As set out in

[1] For an example of this press coverage, see Katrina Manson, *Lina Khan Got Stuck in the Fallout of the MGM Hack at Las Vegas*, Bloomberg (Sept. 15, 2023), https://www.bloomberg.com/news/articles/2023-09-15/mgm-was-hacked-and-lina-khan-had-to-write-her-credit-card-number-down-on-paper?utm_source=website&utm_medium=share&utm_campaign=copy

[2] The CID was served on MGM's registered agent on January 29, 2024. This Petition is timely under 16 C.F.R. 2.10(a)(1) ("Any petition to limit or quash any compulsory process shall be filed with the Secretary within 20 days after service of the Commission compulsory process . . . .") and FTC Rule 4.3(a) ("[w]hen the last day of the period so computed is a Saturday, Sunday, or national holiday, or other day on which the office of the Commission is closed, the period shall run until the end of the next following business day.").

detail below, the CID calls for the production of more than one hundred different categories of information, spans multiple years with no relevance to the attack, and, perhaps most problematic of all, represents an unprecedented attempt by Staff to invoke the Safe Guards Rule and the Red Flags Rule, which do not apply to MGM's operations. For these reasons, and despite MGM's attempts to informally resolve these issues with Staff, MGM was left with no choice but to file this Petition to Quash or Limit.

## II. History of Conferrals

MGM held its initial meet and confer with the FTC on February 6, 2024, within the 14-day period required by FTC rules. 16 C.F.R. § 2.7. During that initial conference, MGM and Staff discussed MGM's willingness to cooperate and that MGM would need a few additional days to review the CID and confer internally before its counsel would be ready to discuss the specifics of the CID. Following the call, MGM commenced an extensive effort to determine what responsive information might exist and the burden associated with obtaining it.

During that first call, MGM also requested an initial extension of the deadline to file a petition to modify or quash by just six days, to February 26, 2024, the same day as the deadline for compliance. MGM sought this extension so that it might have a reasonable opportunity to begin negotiating with Staff over the numerous complex legal and practical issues posed by the CID. On February 8, 2024, however, Staff rejected this reasonable request.

On February 13, 2024, MGM sent Staff a detailed letter containing its objections and concerns regarding the CID. (Ex. 2, MGM Letter.) The letter noted at the outset that because Staff "declined to grant any extension of the initial deadline to file a petition to quash, [Staff] left [MGM] very little time to discuss these complex issues." (*Id.*) Even so, it noted, MGM's "hope is that the detail included in this letter will allow us to expeditiously resolve the many serious issues posed by the CID." (*Id.*)

On February 14, 2024, MGM met with Staff for approximately two hours and went through MGM's letter in detail. On February 15, 2024, Staff emailed MGM with some modifications to the CID, purporting to address some of the concerns MGM had raised with respect to vague and ambiguous wording of the requests of the CID. (Ex. 5.) Staff made clear, however, that there would be no modifications to the most problematic aspects of the CID, including the reliance on the Safeguards and Red Flags Rules, the expansive definition of the "Applicable Time Period," and the threat the CID poses to on-going criminal investigations, with no room to negotiate further on these central issues.

## III. The CID should be quashed, or at least significantly modified.

MGM respectfully requests that the CID be quashed. As set forth in greater detail below, MGM is not subject to the rules that purportedly authorize the CID and the associated investigation. In the alternative, MGM requests that the Commission substantially modify the CID to strike all references to the Safeguards Rule and the Red Flags Rule, strike Specifications 8-53, which are implicitly premised on those rules, and otherwise reasonably tailor the CID to lead to information plausibly relevant to legal requirements that apply to MGM without imposing undue burden.

### A. MGM does not provide "financial services" subject to the Rules cited in the CID.

The CID indicates that it is premised upon two FTC Rules governing companies who provide financial services, the "Safeguards" Rule, 16 C.F.R. Part 314, and the "Red Flags" Rule, 16 C.F.R Part 681. The Red Flags Rule implements the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), 15 U.S.C. § 681, and the Safeguards Rule implements Subtitle A of the Gramm-Leach-Bliley Act ("GLB Act") pursuant to 15 U.S.C. § 6804.

Both rules have narrow and specifically delineated reach. They apply to companies providing financial services, not to gaming and hospitality companies like MGM. During MGM's meeting with Staff on February 14, 2024, MGM asked staff if they were aware of any case law holding that these financial services rules apply to companies like MGM. Staff could not identify any. When asked to articulate the basis for their belief that these rules apply to MGM, they identified only their interest in MGM's issuance of so-called "markers" to some customers.[3] Setting aside how far afield that issue is from the cyberattack Staff are purportedly investigating, the practice of issuing markers comes nowhere near bringing MGM within the ambit of the financial services rules. As discussed below, markers are not loans, they are an insignificant part of MGM's business, and they are wholly incidental to the entertainment services MGM provides. Each of these factors is alone sufficient to render the rules inapplicable.

The Safeguards Rule applies only to "financial institutions," including traditional financial institutions such as banks, and other companies who are "*significantly* engaged in financial activities, or significantly engaged in activities incidental to such financial activities." 16 C.F.R. § 314.2(h)(1). The Rule expressly excludes from the definition of "financial services" common and informal retail practices that are designed for the convenience of customers, such as "lay away" and deferred payment plans, and the practice of allowing customers to "run a tab." *Id.* § 314.2(h)(3).

The Red Flags rule applies to traditional financial institutions and to "creditors" as defined by the authorizing statute. 15 U.S.C. § 1681m(e)(4). A "creditor" includes a company that "regularly" and "in the ordinary course of business" advances funds to consumers or uses

[3] MGM licenses its name to a bank in Delaware for use in connection with a credit card offered by the bank, but MGM has no involvement in the provision or servicing of that credit – the bank is the lender and creditor, and as such this is not a financial activity of MGM for purposes of the Rules.

consumer credit reports to make such credit decisions. Importantly, there is an express exemption in the authorizing statute for a business that "advances funds on behalf of a person for expenses incidental to a service provided by that creditor to that person." *Id.* § 1681m(e)(4)(B).

As the Declaration of Amy Wong, attached hereto as Exhibit 3, indicates, MGM is not in the business of providing financial services to its customers and is not a creditor. It does allow a small and highly select group of high-value customers to access funds in the form of "markers" for use in casino gaming, but these markers are the equivalent of a post-dated check as opposed to advancing funds through a line of credit. (Ex. 3.) Indeed, Nevada Gaming regulations provide that markers and similar instruments must be treated as "identical" to personal checks, Nevada Gaming and Control Board, Regulation 6.118, which MGM prominently discloses to customers who apply for markers. (Ex. 3 at ¶ 4.)

[redacted] (Ex. 3 at ¶ 6.) Contrary to Staff's assertions, the markers do not constitute an "advance of funds" subject to the financial services rules, any more than would a grocer's accepting a customer's personal check as a convenient method of payment.

Moreover, these markers are used very rarely, and, customers who obtain markers represent a trivial portion of MGM's overall customer base. [redacted]

[redacted]. Such negligible occurrences do not constitute a "significant" financial activity, nor do they satisfy the "regularly and in the ordinary course of business" standard, necessary for application of the Rules.[4]

In addition, these "markers" are in every sense "incidental to a service provided by" MGM, just like allowing customers to run a tab. 15 U.S.C. § 1681m(e)(4)(B); 16 C.F.R. 314.2(h)(3). The markers have no value except to facilitate gambling *at MGM casinos* by a tiny subset of MGM customers. (Ex. 3 at ¶ 2.) They are intended to enhance the casino experience for these few customers, and are not in any way equivalent to a bank providing credit.

Plainly, Staff's attempt to invoke the Safeguards Rule and the Red Flags Rule as a basis for the CID, and Staff's position that MGM is subject to these rules, represents a massive overreach and lacks any reasonable basis in the language of the Rules. This is an independent and sufficient basis for quashing the CID. Alternatively, it is an ample basis for modifying the CID by striking all references to the Safeguards Rule and the Red Flags Rule, and striking Specifications 8-53, which are implicitly premised on those rules.

### B. Extending the Rules to MGM would Exceed the FTC's Authority

In an instructive case illustrating the limits of the FTC's statutory authority under financial services regulations, a federal court squarely rejected the FTC's attempt to enforce certain aspects of the Red Flag Rule against lawyers who bill their clients after services are rendered. *American Bar Ass'n v. FTC*, 671 F. Supp. 2d 64 (D. D.C. 2009) ("*ABA*"), *vacated on other grounds American*

[4] MGM will on occasion use credit reports to evaluate marker applications, but their use is even more *de minimus.* Throughout all of 2023, from its many millions of customers, MGM obtained only 4,559 credit reports. (*See* Ex. 3)

*Bar Ass'n v. FTC*, 636 F.3d 641 (D.C. Cir. 2011). The court held that the FTC's attempt to apply its Red Flags Rule to attorneys exceeded the FTC's authority granted to it under FACTA. In language that is equally applicable to hotels and casinos, the Court in *ABA* concluded that the legal profession is not subject to the Red Flags Rule:

> The Court is confident in concluding that . . . if Congress . . . intended to regulate attorneys and their invoiced billing practices it would have used the appropriate terminology to denote that intent and not hidden it in a statute expressly targeted at the credit industry. *See Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 468, 121 S.Ct. 903, 149 L.Ed.2d 1 (2001) ("[Congress] does not ... hide elephants in mouseholes.").

*Id.* at 75.

If Congress intended to include casino operations within the definition of financial services for purposes of FACTA and the GLB Act, it would have said so explicitly – as it did when it amended the Bank Secrecy Act to include casinos, *see* 31 U.S.C. § 1532 (X). In fact, the rules have never been applied to hotels, casinos, or any other industries so far removed from traditional banking and financial services. Any attempt to stretch the coverage of these financial services rules to MGM would be unprecedented, unwarranted, and beyond the FTC's statutory authority.

### C. The CID should be quashed or modified to prevent interference with ongoing federal law enforcement investigations and prosecutions.

MGM is a crime victim with an intense and legitimate interest in seeing its attackers arrested and prosecuted. To that end, MGM has cooperated extensively with federal law enforcement since the cyberattack (including not paying ransom) and continues to actively support ongoing investigations. The CID risks jeopardizing those efforts and unfairly places MGM in a risky and highly prejudicial position because it encompasses information related to these criminal investigations. (*See, e.g.*, Spec. Nos. 22, 46.) This was, apparently, the result of Staff's intentional design. Indeed, during the parties' meet and confer on February 6, 2024, Staff requested that MGM prioritize the production of information provided to law enforcement agencies, and

expressly requested that MGM produce any information MGM previously provided to the Federal Bureau of Investigation ("FBI") as quickly as possible. Staff's attempt to obtain this material should be quashed, at least until the conclusion of the relevant prosecutions.

*First*, requiring a victim of crime to produce such information has the effect of punishing crime victims for assisting law enforcement and sets a dangerous precedent. Plainly, the request disincentivizes cooperation with law enforcement by companies subject to cyberattacks or other crimes.

*Second*, the fact that any particular information was provided to law enforcement—particularly by a crime victim—in no way entitles Staff to that information. Staff cannot overcome the inapplicability of the FTC rules they rely on by saying that information was shared with law enforcement. In this case, it certainly does not supersede the numerous problems with the CID outlined elsewhere in this Petition.

*Third*, this request creates a dangerous practical problem. Although MGM has cooperated with federal law enforcement, MGM has neither control over nor visibility into the details of any of the investigations by the FBI or other agencies, or into any criminal prosecutions. Therefore, MGM has no way of knowing what information may adversely affect criminal investigations or prosecutions if disclosed, or if disclosed at the wrong time. Forcing 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. *See United States v. Morton Salt Co.*, 338 U.S. 632, 652 (1950). It is unreasonable, unfairly punitive, and potentially dangerous.

### D. The CID should also be quashed because enforcement would be unduly burdensome.

The CID should not be enforced as written because its enforcement would be unduly burdensome on MGM. To be enforceable, a CID must be reasonable in the "nature, purposes, and scope of the inquiry." *Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 209 (1946). An "investigation into corporate matters may be of such a sweeping nature and so unrelated to the matter properly under inquiry as to exceed the investigatory power." *Morton Salt Co.*, 338 U.S. at 652.

Accordingly, a CID is not enforceable if it is not "reasonably relevant" to a legitimate purpose. *Id.* at 652-53. Nor is it enforceable if it is "unduly burdensome or unreasonably broad," which occurs where "compliance threatens to unduly disrupt or seriously hinder normal operations of a business." *Fed. Trade Comm'n v. Texaco, Inc.*, 555 F.2d 862, 882 (D.C. Cir. 1977). In evaluating the burden, the Commission considers the extent to which a CID is "self-limiting." *In re: Altmeyer Home Stores, Inc. Petition to Quash or Limit Civ. Investigative Demands*, 123 F.T.C. 1730, 1738 (1997). In *Altmeyer*, for example, the Commission described a CID as "self-limiting" because it "provided various options for minimizing its scope," and allowed the production of sample files if more than 500 files were responsive to a particular Specification. *Id.* The Commission also considers whether the "specifications [are] narrowly tailored to obtain information germane to the Commission's investigative purpose as set forth in the Resolution." *Id.*

As explained in greater detail below, and in the Declaration of John Branden Newman attached hereto as Exhibit 4, responding to the CID would be unduly burdensome. Counting subparts, the request contains *ninety-two* interrogatories, almost all of which will require significant investigation and analysis in order to properly respond, and *fifteen* exceptionally broad

document requests, including a massive "catch all" request for "all Documents related to the incident(s)," Spec. No. 46, and a request that would require MGM to search every advertisement, web page, press release, and every other public communication for any representations regarding cybersecurity (which are highly unlikely to exist except for in MGM's Privacy Policy.) The sheer volume of these requests – especially given the three-year time frame – is excessively burdensome on its face, especially coming at a time when there are already particularly high demands on MGM employees as a result of the 2023 cyberattack of which MGM was a victim. (Ex. 4.)

1. *The "Applicable Time Period" as defined in the CID is overbroad and unduly burdensome.*

The CID is fundamentally overbroad and unduly burdensome because it would require MGM to search for, collect, and produce data for periods of time that long precede the incident giving rise to the investigation. The CID defines the "Applicable Time Period" as the period "from January 1, 2021, to the date of full compliance with the CID." This definition is problematic in two primary respects. As an initial matter, productions for the full timeframe would sweep up *years*' worth of information preceding the cyber security incident giving rise to the investigation. The incident occurred in late 2023, and Staff have expressed an intertest in MGM's security practices in effect at the time of the incident, and whether MGM acted reasonably in its immediate aftermath *in 2023*. MGM's practices in 2021 and 2022, however, have no bearing on the reasonableness of its security practices in 2023, nor on the efficacy of MGM's response to the incident.

This unreasonable "Applicable Time Period" infects nearly every Specification in the CID. The CID expressly incorporates its definition of the "Applicable Time Period" into no fewer than *thirteen* of the Specifications, *see* Spec. Nos. 8-9, 11(a)(iv), 26, 32-34, 37, 39, 43-44, and 49-50, and provides an implicit outer time boundary for nearly all of the remaining Specifications, *see*

*e.g.* Spec. Nos. 1-7, 10, 12-21, 29-31, 35-36, 40-42, 45-48. As described in the Newman Declaration, producing so much historical data of questionable relevance will present a significant burden to MGM, diverting the time and attention of key employees from running MGM's business to responding to the CID while providing little value to the stated purpose of Staff's investigation. (Ex. 4 ¶¶ 4-6.)

Because providing information spanning the entire "Applicable Time Period" will simultaneously sweep up a significant volume of data of no relevance *and* impede MGM's ability to operate its business, the CID is unduly burdensome and should be quashed or modified.

2. *The CID is unduly burdensome and should be quashed or modified because it contains several "catch-all" type questions.*

The CID is also overbroad and unduly burdensome insofar as it incorporates a number of impermissible "catch all questions." In a recent Order granting in part a Motion to Quash a CID, the Commission indicated that "catch all questions," such as "provide all other information [on a subject] not otherwise provided in Your responses," are disfavored, and struck a number of such questions from the CID at issue. *Amazon ROSCA*, File No. 212 3050, September 21, 2022. Two requests in the instant CID suffer from this same defect, namely:

- Specification 17: Describe in detail the steps the Company has taken to prevent unauthorized access… *to the extent not discussed in response to another Specification*, Specification Nos. 17; and
- Specification 46: Produce all Documents created, received, or disseminated by the Company regarding the . . . security incident(s) . . . .

Like the improper requests in *Amazon ROSCA*, these catch all questions are not "sufficiently definite." Amazon Rosca, Order at 13, quoting *Resolution Trust Corp. v. Greif*, 906 F. Supp. 1446, 1452 & n.2 (D. Kan. 1995). Accordingly, the CID should be quashed or modified to eliminate them.

3. *The CID is also unduly burdensome in various other ways and requires quashing or modification.*

Other aspects of the CID are also overbroad and unduly burdensome, and it should, therefore, be quashed or modified.

For example, the CID asks in no less than four separate ways for MGM to provide information about its organizational structure, *see* Specification Nos. 33-37, including "how authority and responsibility have been distributed to employees, officer[s], directors, principals, and owners with the Company" without any limitation, *see* Specification No. 37. These requests are overbroad on their faces. Plainly, the manner in which authority is delegated across all of MGM—a global hospitality and entertainment company—is not relevant to this investigation into the Company's cyber security practices. Put another way, it is not clear—and Staff have not articulated—how or why the scope of the authority of a housekeeping manager at MGM's property in Springfield, Massachusetts, for example, is in any way relevant to the Company's cybersecurity practices, which are determined by personnel located elsewhere (particularly where, as here, the precise nature of the intrusion into MGM's IT systems is still under active investigation).

Other Specifications suffer from a similar problem. Specification Nos. 5 and 6, for instance, call for information regarding sales and net revenue for *every* product or service offered by MGM as well as the types of customer information collected in connection with those offerings. Neither Specification Nos. 5 nor 6 contain any substantive limitation of *any kind*, and would therefore purport to require production of financial and other information about literally every aspect of MGM's customer facing business over a multi-year period. Not only would gathering and producing this information be incredibly burdensome, but it would sweep vast swathes of highly commercially sensitive information that has *nothing* to do with the facts under investigation.

### E. The CID should be quashed or modified because responding would require MGM to speculate.

The CID should also be modified or quashed because it would require MGM to speculate—both as to the meaning of certain of the Specifications themselves and the answers to many questions posed.

A number of the requests are rendered impermissibly vague and ambiguous through their use of undefined, unexplained, and unclear terms and phrases. These include: "incident response practices," Spec. 13; "software update practices," Spec. No. 14; "unauthorized person(s) among other things," Spec. No. 22; and "individuals who have or had the ability to control or participate in the Company's practices, policies and procedures," Spec. No. 33. Without further clarification, which Staff have been thus far unwilling to provide, MGM would be left to do little more than make educated guesses about the nature of responsive information. This would be highly prejudicial, and merits quashing or modifying the CID.

Similarly, the CID calls for MGM to provide information that is, at this point, still under investigation by MGM and law enforcement. Specification No. 22, and its subparts (a) through (u), poses no fewer than *twenty-three* separate questions seeking extensive and precise detail as to whether, when, and how the threat actor behind the cyber security incident giving rise to the investigation obtained access to customer personal information. Similarly, Specification No. 9 assumes that the incident was the result of particular types of cyberattack and would require MGM to produce information related to those threat types. As Staff has been at all times aware, however, the FBI is currently engaged in a criminal investigation of precisely these issues. Until that investigation and any others conclude, any response by MGM to these kinds of questions would be speculative.

### F. Proposal for Modification

MGM respectfully requests that the CID be quashed in its entirety. No amount of modification can fully remedy the CID's many defects. MGM is not subject to the Safeguards or Red Flags Rules, and so enforcement of any part of the CID is outside the bounds of the FTC's authority. Alternatively, MGM requests that the Commission substantially modify the CID to strike all references to the Safeguards Rule and the Red Flags Rule, strike Specifications 8-53, which are implicitly premised on those rules, and otherwise reasonably tailor the CID to lead to information plausibly relevant to legal requirements that apply to MGM without imposing undue burden.

Respectfully submitted,

February 20, 2024

*/s/ Brian J. Boyle*

Brian J. Boyle
DLA Piper LLP
500 8th St NW
Washington, DC 20004
(215) 656-2450
brian.boyle@us.dlapiper.com

Andrew Sacks
DLA Piper LLP
701 Fifth Avenue, Suite 6900
Seattle, Washington 9810
(206) 839-4890
andrew.sacks@us.dlapiper.com

Brett M. Feldman
DLA Piper LLP (US)
1650 Market Street, Suite 5000
Philadelphia, PA
(215) 656-3300
brett.feldman@us.dlapiper.com

*Counsel for Petitioner*

## CERTIFICATE OF SERVICE

I certify that, on February 20, 2024, an electronic copy of the foregoing and exhibits thereto were served via electronic mail upon the following:

Office of the Secretary
Federal Trade Commission
600 Pennsylvania Avenue, NW
Suite CC-5610
Washington, D.C. 20580
electronicfilings@ftc.gov
atabor@ftc.gov

Carla Cheung
David Hankin
Federal Trade Commission
Western Region Los Angeles
10990 Wilshire Boulevard, Suite 400
Los Angeles, CA 90024
ccheung1@ftc.gov
dhankin@ftc.com

February 20, 2024

*/s/ Brian J. Boyle*
Brian J. Boyle
DLA Piper LLP
500 8th St NW
Washington, DC 20004
(215) 656-2450
brian.boyle@us.dlapiper.com

*Counsel for Petitioner*

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

| | | |
|---|---|---|
| *In re* Civil Investigative Demand to MGM Resorts International. | ) | FTC File No. 2423028 |

**REQUEST FOR CONFIDENTIAL TREATMENT**

MGM Resorts International ("MGM") requests that this 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, the disclosure of which would result in serious competitive injury to MGM. *General Foods Corp.*, 95 F.T.C. 352, 355 (1980). If this information were made public, competitors and other industry participants may be able to unfairly compete against MGM or undermine MGM's business.

February 20, 2024

*/s/ Brian J. Boyle*

Brian J. Boyle
DLA Piper LLP
500 8th St NW
Washington, DC 20004
(215) 656-2450
brian.boyle@us.dlapiper.com

*Counsel for Petitioner*

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

| | | |
|---|---|---|
| *In re* Civil Investigative Demand to MGM Resorts International. | ) | FTC File No. 2423028 |

**STATEMENT OF COUNSEL PURSUANT TO 16 C.F.R. 2.10**

I, Brian J. Boyle, state as follows:

1. I am a partner at DLA Piper LLP and one of the attorneys representing Petitioner, MGM Resorts International.

2. I make this this statement upon personal knowledge and belief.

3. Prior to filing the accompany Petition to Quash or Modify, I and my colleagues, Andrew Sacks and Brett M. Feldman, conferred with Commission staff pursuant to 16 C.F.R. 2.7(k) in an effort in good faith to resolve by agreement the issues raised by the Petition, but we have been unable to reach agreement as to those issues.

4. As required by Rule 2.7(k), the following are the dates, times, and means of each conference between counsel and the names of all parties participating in each such conference. These conferences are described further in Part II of the Petition.

a. At 3:00 p.m. EST on February 6, 2024, counsel for MGM, Brian J. Boyle, Andrew Sacks, and Brett M. Feldman, participated in a Microsoft Teams conference with FTC staff, Charla Cheung, David Hankin, and Simon Fondrie-Teitler.

b. On February 7, 2024, counsel for MGM, Brian J. Boyle, with Andrew Sacks and Brett Feldman in copy, sent correspondence regarding a potential

petition to FTC staff, Carla Cheung, David Hankin, and Simon Fondrie. Ms. Chueng responded several hours later.

c. On February 13, 2024, counsel for MGM, Brian J. Boyle, with Andrew Sacks and Brett Feldman in copy, sent correspondence outlining the issues identified above to FTC staff, Charla Cheung, David Hankin, and Simon Fondrie-Teitler.

d. At 3:00 p.m. EST on February 14, 2024, counsel for MGM, Brian J. Boyle, Andrew Sacks, and Brett M. Feldman, participated in a Microsoft Teams conference with FTC staff, Charla Cheung, David Hankin, and Simon Fondrie-Teitler.

February 20, 2024

*/s/ Brian J. Boyle*

Brian J. Boyle
DLA Piper LLP
500 8th St NW
Washington, DC 20004
(215) 656-2450
brian.boyle@us.dlapiper.com

*Counsel for Petitioner*

# EXHIBIT 1

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

Office of the Secretary

January 25, 2024

**CONFIDENTIAL**

Via FedEx
MGM Resorts International
c/o Corporation Service Company
251 Little Falls Drive
Wilmington, DE 19808

FTC Matter No. 2423028

Dear MGM Resorts International:

The Federal Trade Commission ("FTC") has issued the attached Civil Investigative Demand ("CID") asking for information as part of a non-public investigation. Our purpose is to determine whether the data security practices of MGM Resorts International comply with Section 5 of the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45 *et seq.*), the Standards for Safeguarding Customer Information Rule ("Safeguards Rule") (16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 *et seq.*), and/or the Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft ("Red Flags Rule") (16 C.F.R. § 681.1(d), issued pursuant to Section 621 of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681s), and whether Commission action to obtain monetary relief would be in the public interest. Please read the attached documents carefully. Here are a few important points we would like to highlight:

1. **Contact FTC counsel, Carla Cheung (202-644-6785; ccheung1@ftc.gov) or David Hankin (202-227-1521; dhankin@ftc.gov), as soon as possible to schedule a telephone call to be held within 14 days.** During that telephone call, FTC counsel can address any questions or concerns you have regarding this CID, including whether there are changes to how you comply with the CID that would reduce your cost or burden while still giving the FTC the information it needs. Please read the attached documents for more information about that meeting.

2. **You must preserve, and immediately stop any deletion or destruction of, electronic or paper documents** in your possession, custody, or control that are in any way relevant to this investigation, even if those documents are being retained by a third party or you believe the documents are protected from discovery by privilege or some other reason. You must also disable auto-delete for, or suspend, restrict, or limit use of, any applications or platforms that automatically delete messages or information that may be relevant to this investigation.

3. **The FTC will use information you provide in response to the CID for the purpose of investigating violations of the laws the FTC enforces.** We will not

disclose the information under the Freedom of Information Act, 5 U.S.C. § 552. We may disclose the information in response to a valid request from Congress, or to other civil or criminal law enforcement agencies for their official law enforcement purposes. The FTC or other agencies may use and disclose your response in any civil or criminal proceeding, or if required to do so by law. However, we will not publicly disclose your information without giving you prior notice.

4. **Please read the attached documents closely.** They contain important information about how you should provide your response.

Please contact FTC counsel as soon as possible to set up an initial meeting. We appreciate your cooperation.

Very truly yours,

April J. Tabor
Secretary

# Civil Investigative Demand

| 1. TO | 1a. MATTER NUMBER |
|---|---|
| MGM Resorts International<br>c/o Corporation Service Company<br>251 Little Falls Drive<br>Wilmington, DE 19808 | 2423028 |

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

☐ You are required to appear and testify.

| LOCATION OF HEARING | YOUR APPEARANCE WILL BE BEFORE |
|---|---|
| | DATE AND TIME OF HEARING OR DEPOSITION |

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

☐ You are required to produce the tangible things described on the attached schedule. Produce such things to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS, ANSWERS TO INTERROGATORIES, REPORTS, AND/OR TANGIBLE THINGS MUST BE AVAILABLE

February 26, 2024 by 5:00 pm ET

3. SUBJECT OF INVESTIGATION

See attached Schedule and attached resolutions.

| 4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN | 5. COMMISSION COUNSEL |
|---|---|
| Aaron Jamison or Faye Chen Barnouw<br>Federal Trade Commission<br>Western Region Los Angeles<br>10990 Wilshire Boulevard, Suite 400<br>Los Angeles, CA 90024<br>(202) 251-6824 | Carla Cheung<br>Federal Trade Commission<br>Western Region Los Angeles<br>10990 Wilshire Boulevard, Suite 400<br>Los Angeles, CA 90024<br>(202) 644-6785 |

| DATE ISSUED | COMMISSIONER'S SIGNATURE |
|---|---|
| 01/25/2024 | Lina Khan |

## INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

## PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

## YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

## TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

A copy of the Commission's Rules of Practice is available online at http://bit.ly/FTCSRulesofPractice. Paper copies are available upon request.

**FEDERAL TRADE COMMISSION ("FTC")**
**CIVIL INVESTIGATIVE DEMAND ("CID") SCHEDULE**
**FTC File No. 2423028**

**Meet and Confer:** You must contact **FTC counsel, Carla Cheung (202-644-6785; ccheung1@ftc.gov) or David Hankin (202-227-1521; dhankin@ftc.gov)**, as soon as possible to schedule a telephonic meeting to be held within fourteen (14) days after You receive this CID. At the meeting, You must discuss with FTC counsel any questions You have regarding this CID or any possible CID modifications that could reduce Your cost, burden, or response time yet still provide the FTC with the information it needs to pursue its investigation. The meeting also will address how to assert any claims of protected status (e.g., privilege, work-product, etc.) and the production of electronically stored information. You must make available at the meeting personnel knowledgeable about Your information or records management systems, Your systems for electronically stored information, custodians likely to have information responsive to this CID, and any other issues relevant to compliance with this CID.

**Document Retention**: You must retain all Documents used in preparing responses to this CID. The FTC may require the submission of additional Documents later during this investigation. **Accordingly, You must preserve, and immediately stop any deletion or destruction of, Documents in Your possession, custody, or control** that are in any way relevant to this investigation, even if those Documents are being retained by a third party or You believe those Documents are protected from discovery. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. §§ 1505, 1519. In addition, You must disable auto-delete for, or suspend, restrict, or limit use of, any messaging applications or Collaborative Work Environments that automatically delete messages or information that may be relevant to this investigation.

**Sharing of Information:** The FTC will use information You provide in response to the CID for the purpose of investigating violations of the laws the FTC enforces. We will not disclose such information under the Freedom of Information Act, 5 U.S.C. § 552. We also will not disclose such information, except as allowed under the FTC Act (15 U.S.C. § 57b-2), the Commission's Rules of Practice (16 C.F.R. §§ 4.10 & 4.11), or if required by a legal obligation. Under the FTC Act, we may provide Your information in response to a request from Congress or a proper request from another law enforcement agency. However, we will not publicly disclose such information without giving You prior notice.

**Manner of Production**: Contact **Aaron Jamison (202-251-682; ajamison@ftc.gov)** by email or telephone at least five days before the return date for instructions on how to produce information responsive to this CID.

**Certification of Compliance**: You or any person with knowledge of the facts and circumstances relating to the responses to this CID must certify that such responses are complete by signing the "Certification of Compliance" attached to this CID.

**Certification of Records of Regularly Conducted Activity**: Attached is a Certification of Records of Regularly Conducted Activity. Please execute and return this Certification with Your response. Completing this certification may reduce the need to subpoena You to testify at future proceedings to establish the admissibility of Documents produced in response to this CID.

**Definitions and Instructions**: Please review carefully the Definitions and Instructions that appear after the Specifications and provide important information regarding compliance with this CID.

## I. SUBJECT OF INVESTIGATION

Whether the data security practices of the "Company" as defined herein comply with Section 5 of the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45 *et seq.*), the Standards for Safeguarding Customer Information Rule ("Safeguards Rule") (16 C.F.R. Part 314, issued pursuant to Title I of the Gramm-Leach-Bliley ("GLB") Act, 15 U.S.C. § 6801 *et seq.*), and/or the Duties Regarding the Detection, Prevention, and Mitigation of Identity Theft ("Red Flags Rule") (16 C.F.R. Part 681, issued pursuant to Section 615(e) of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681m(e)), and whether Commission action to obtain monetary relief would be in the public interest. See also attached resolution(s).

## II. SPECIFICATIONS

**Applicable Time Period:** Unless otherwise directed, the applicable time period for the requests set forth below is from **January 1, 2021 until the date of full and complete compliance with this CID.**

### A. Interrogatory Specifications

Corporate Information

1. State the complete legal name of the Company and all other names under which it does or has done business, its principal place of business, its corporate mailing address and telephone number, and the date and state of its incorporation.

2. Describe the Company's corporate structure and state the names of all parents, subsidiaries, divisions, affiliates, branches, joint ventures, franchises, operations under assumed names, websites, and entities over which the Company exercises supervision or control. For each such entity, describe the nature of its relationship to the Company.

3. State the Company's total number of employees.

4. For 2021, 2022, and 2023, state the Company's annual gross and net revenues in dollars.

5. List each Product or Service the Company offers for sale, including any related membership, loyalty, reward and/or incentive program, and for each describe:

    a. The number of current customers for each; and

    b. Your total sales and net revenues by year.

6. For each Product or Service, list the types of Personal Information that the Company collects or maintains in connection with its Products or Services, including the formats in

which the Company maintains the information and the approximate number of individuals for whom the Company maintains each type of Personal Information.

7. Describe what parts of the Company are involved in the development, implementation, and execution of the Company's data security practices, policies, and procedures, Identify the individuals responsible therefor, and state the number of employees assigned to each described part.

Security Practices

8. Describe, including through graphic representation, the network architecture of the Company's web portals, data centers, servers, databases, and applications where Personal Information is collected, processed, transmitted, or stored. Your response should also include the names and locations of all web portals, data centers, servers, databases, and applications where Personal Information is collected, processed, transmitted, or stored. Explain any changes in Your collection, processing, transmission, or storage of Personal Information during the applicable time period, if any such changes have occurred.

9. 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

10. Describe in detail the Company's processes for identifying risks of unauthorized access to its Administrative Tools and assessing the sufficiency of any safeguards in place to control those risks, and state the date upon which each described process was implemented and, if applicable, terminated.

11. Describe in detail, including the applicable time period for each, the Company's practices, policies, and procedures for safeguarding all systems that collect, process, transmit, or store Personal Information, including:

    a. Authentication and access management for the Company's Administrative Tools. For each Administrative Tool, state the date upon which each described control was implemented and, if applicable, terminated. In particular, describe:

        i. How authentication is managed;

        ii. The categories of employee access, and the privileges or extent of access corresponding to each;

        iii. For each employee access level described in response to (ii), the reasons or job responsibilities that warrant that access level;

        iv. The use of multi-factor authentication for each category of employee access, including the type(s) of multi-factor authentication, and why multi-

factor authentication was or was not required for each over the Applicable Time Period; and

v. The steps the Company takes to audit or monitor employee access and review the records of such monitoring.

b. Cryptography or security protocols applicable to the collection, transfer, or storage of Personal Information in any of the Company's databases or systems, including:

i. Practices, policies, and procedures with respect to encrypting data in transit;

ii. Each location where Personal Information was or is collected, used, stored, or transferred in encrypted format;

iii. How and where encryption or decryption keys are or were generated or stored, including whether and how such keys were segregated from Personal Information and how access to the keys was restricted;

iv. The manner in which encryption or decryption keys are or were stored, such as in clear text, and what, if anything, the Company has done to prevent and detect clear text storage of user credentials or encryption keys; and

v. What practices, policies, procedures, and tools are or were used to recognize and delete stored Personal Information that is no longer necessary to providing the Company's Products or Services.

c. Categories of employees who are authorized to access, modify, or download customer accounts or Personal Information, and what controls are in place restricting such privileges.

d. Password and secret management, including all practices, policies, and procedures for storing credentials, such as usernames, passwords, API keys, secure access tokens, or asymmetric private keys; and

e. Network segmentation, firewalls, and any other mechanisms to limit or prevent access among or between the Company's systems or networks.

12. Describe in detail the steps the Company has taken to detect unauthorized access to its Administrative Tools, and state the date upon which each described step was implemented and, if applicable, terminated.

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.

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.

15. Describe in detail the Company's logging and log monitoring 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.

16. Describe in detail the Company's practices, policies, and procedures for granting, modifying, or revoking an employee's authorization, and for modifying or resetting an employee's means of authentication, to access the Company's Administrative Tools, including:

    a. The categories of employees who are permitted to grant, modify, or revoke another employee's authorization to access the Company's Administrative Tools, any limitations on each category's permissions to do so, and the reasons for any such limitations;

    b. The categories of employees who are permitted to modify or reset another employee's means of authentication to access the Company's Administrative Tools, any limitations on each category's permissions to do so, and the reasons for any such limitations;

    c. Methods of verifying the identity of an employee requesting a reset or modification to their own means of authentication or authorization;

    d. Any differences between the practices, policies, and procedures for resetting passwords and multi-factor authentication methods;

    e. The design elements incorporated into the Company's data managements systems, including the implementation of any Technical Controls, to enforce or encourage compliance with the practices, policies, and procedures described in Specification 16; and

    f. Any trainings provided to employees listed in (a) and (b) specific to the practices, policies, and procedures described in Specification 16.

17. 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.

18. Describe in detail the Company's efforts to align its cybersecurity risk management with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

19. State the level of Payment Card Industry Data Security Standard (PCI DSS) that the Company considers itself subject to, and describe in detail all practices, policies, and procedures the Company has in place to maintain compliance, including:

    a. Any practices, policies, and procedures regarding the Company's Administrative Tools not described in response to another Specification;

    b. Any practices, policies, and procedures for handling PCI DSS-covered data outside of the Company's digital systems, including the use of manual or paper record keeping;

    c. Any practices, policies, and procedures the Company has in place for handling PCI DSS-covered data in the event that access to Company's Administrative Tools are unavailable; and

    d. Any PCI DSS-related training that Your employees have received.

20. Describe in detail the steps the Company has taken to evaluate, test, and monitor the effectiveness of the practices, policies, and procedures described in Your Response to Specifications 8-19, and state the date upon which each described step was implemented and, if applicable, terminated.

21. List each representation or other information provided about the data security of the Company, including the data security of the Administrative Tools or the Company's Products or Services, made in applying for, obtaining, or submitting a claim for, cybersecurity insurance and state the date on which You made the representation or provided the information.

Security Incidents

22. 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, as referenced in Exhibit 1, attached. In addition:

    a. Describe how and when the Company became aware of the events referenced therein;

b. Describe what occurred and the timeline of all events, including a description of all phishing attacks involved and, if implemented, an explanation of how multi-factor authentication was circumvented;

c. State the number of customers whose Personal Information is known or reasonably suspected to have been accessed without authorization in the security incident(s);

d. State the location, type(s), and amount(s) of Personal Information that unauthorized person(s) could have accessed or viewed, and did copy, download, remove, or exfiltrate;

e. Identify each person who performed any post-security incident investigations or assessments, including forensic or cybersecurity investigators, analysts, consultants, or vendors, and Identify each Company employee or manager responsible for providing information to any such persons;

f. State all findings or conclusions from any internal or external investigation or assessment of the security incident(s).

g. State each information security standard, practice, policy, or procedure the Company implemented or changed in response to the security incident(s), and when each standard, practice, policy, or procedure was implemented or changed;

h. List any instances of reported identity theft, fraud, misuse of Personal Information, or other unauthorized access to the Company's systems or networks attributable to the security incident(s).

i. Describe whether and what alerts or log entries were triggered by the actions of the unauthorized individual(s), when You became aware of these alerts, and what steps You took in response;

j. Describe the resources the unauthorized individual(s) was able to access, and how the unauthorized individual(s) was able to do so;

k. Describe the scope and purposes of the compromised environment(s);

l. Describe whether the Company's security controls prevented the unauthorized individual(s) from further access or actions, and if so, how;

m. Referencing Your response to Specification 11, state what levels of access were held by employee accounts for which authentication credentials were compromised, and how many accounts were affected for each level of access;

n. State how many authentication credentials were used by the unauthorized individual(s), what type(s) of credentials, and how they were used;

o. State whether any compromised authentication credentials were used to obtain other or additional credentials, and if so, describe in detail how;

p. Describe the Company's containment of the unauthorized access, including whether and how You are certain You have identified all impacted customer accounts and eliminated the unauthorized individual(s)'s access;

q. Describe all the resources or locations in the Administrative Tools the unauthorized individual(s) accessed, for example, particular customer accounts, and how You determined that other resources were not accessed;

r. State the earliest time the Company believes the unauthorized individual(s) accessed any Company resource or location, what was likely accessed at that time, and how You came to this conclusion;

s. Describe the software patch status of the entry point of the unauthorized individual(s) into the Administrative Tools as of the security incident(s) occurring during September 2023 as referenced in Exhibit 1, attached;

t. Describe the full scope of the unauthorized individual(s)'s reconnaissance of the Administrative Tools or other Company resources, and any alerts or other logs or records created by that activity; and

u. Describe any notice You have provided to a governmental entity or Your customers, including the date(s), content, and recipients of such notice.

23. List any Administrative Tools or other Company resources that were offline or inaccessible to the Company, consumers, or any third party during or immediately following the security incident(s) identified in Specification 22, state the reason any Administrative Tools or other Company resources were offline or inaccessible, and state the time period during which the Administrative Tools or other Company resources were offline or inaccessible.

24. Describe in detail any manual or contingency practices or procedures used to continue operations affected by the Administrative Tools or other Company resources that were offline or inaccessible during or immediately following the security incident(s) identified in Specification 22. State the date upon which any manual or contingency practices or procedures were implemented and, if applicable, terminated.

25. List any types of Personal Information that the Company collected or maintained in connection with manual or contingency practices or procedures identified in Specification 22, and for each describe in detail:

    a. The approximate number of individuals for whom the Company collected or maintained each type of Personal Information;

b. The time period during which the Personal Information was collected, and if applicable, disposed of; and

c. The Company's processes for preventing unauthorized access to each type of Personal Information collected.

26. Describe in detail all incidents of unauthorized access to the Company's Administrative Tools, customer accounts, or Personal Information during the Applicable Time Period.

27. List any governmental or private investigations or litigation related to the security incident(s) described in Your responses to Specifications 22 and 26, and describe the status of each investigation or litigation.

28. Identify each customer account that You found or learned, in Your investigation of the events described in Your response to Specifications 22 and 26, to have been compromised.

29. List each different Advertisement, website, or other statement (e.g., privacy policy, terms of service, blog postings, press releases, etc.), including the URL(s), on which You have described, discussed, promoted, advertised, or otherwise provided any information about the security of the Company, including the security of the Administrative Tools or the Company's Products or Services, and state the date range during which You made the statement available.

Identity Theft Detection, Prevention, and Mitigation

30. State whether the Company regularly and in the ordinary course of business:

a. Obtains or uses Consumer Reports, directly or indirectly, in connection with a credit transaction;

b. Furnishes information to Consumer Reporting Agencies ("CRAs"), as described in Section 623 of the FCRA, 25 U.S.C. 1681s-2, in connection with a credit transaction; or

c. 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, unless such funds are for expenses incidental to a service the Company provides to that person.

31. Describe in detail the Company's practices, policies, and procedures to comply with 16 C.F.R. Part 681 (the "Red Flags Rule") and for each practice, policy, and procedure, state the dates on which it was initially implemented, and if applicable, materially modified or terminated.

32. Describe in detail the Company's employee training related to the practices, policies, and procedures described in Your response to Interrogatory No. 31, and state the date upon which each type of training occurred during the Applicable Time Period.

Employees and Management

33. 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.

34. Identify the personnel responsible for preventing unauthorized access to computer systems or Personal Information related to the Company's Products or Services over the Applicable Time Period, including title or job description.

35. Identify all persons who have been responsible for creating, developing, approving, implementing, overseeing, or ensuring compliance with the practices, policies, procedures described in Your responses to Specifications 8-19 and 31-32. For each person, state the dates of the person's employment or affiliation with the Company, all title(s) or position(s) held at the Company, and whether the person is currently employed by the Company.

36. Identify all individuals who have the ability to control or participate in the drafting of the Company's representations listed in Your response to Specification 29. For each person, state the dates of the person's employment or affiliation with the Company, all title(s) or position(s) held at the Company, and whether the person is currently employed by the Company.

37. Describe in detail (e.g., through graphic representation) how authority and responsibility have been distributed to employees, officer, directors, principals, and owners within the Company over the Applicable Time Period. Your response should address the individuals Identified and personnel described in Your responses to Specifications 33-35.

38. Identify all persons at the Company who participated in the preparation of responses to these Interrogatories and Document Requests.

## B. Document Request Specifications

39. Produce every written policy or procedure memorializing the processes described in Your responses to Specifications 8-19 and 31-32 that have been in effect during the Applicable Time Period.

40. Produce Documents sufficient to show the Company's execution of the training, practices, policies, processes, and steps described in Your responses to Specifications 9-10, 11(a)(v), 12-15, 17-18, 20, and 31-32.

41. Produce all Documents created as part of Your implementation of the processes described in Your response to Specification 10.

42. Produce a copy of each materially different written identity theft prevention program described in Your response to Interrogatory 31.

43. To the extent not already provided, produce all Documents representing the results of first-party and third-party compromise assessments or threat hunts related to the Administrative Tools during the Applicable Time Period.

44. To the extent not already provided, produce all Documents created as part of internal or external audits or assessments of the security of the Company's computer systems related to the Company's Products or Services with respect to unauthorized access during the Applicable Time Period, including without limitation any Service Organization Control Type 2 (SOC 2), Statements on Standards for Attestation Engagements 16 (SSAE 16), or PCI DSS audits.

45. To the extent not already provided, produce all Documents constituting or relating to the results of such any audit or assessment referenced in Your response to Specification 44 and relating to the Company's efforts to change or remediate issues identified in such an audit or assessment.

46. Produce all Documents related to the security incident(s) affecting the Administrative Tools that the Company identified in September 2023, and which is referenced in Exhibit 1, attached.

47. Produce a copy of each representation or other information listed in Your responses to Specification 21.

48. Produce a copy of each Advertisement, website, or other statement listed in Your responses to Specification 29.

49. Produce a sample of each materially different terms of service for Your Products or Services that was made available to customers during the Applicable Time Period.

50. Produce all organizational charts that were in effect during the Applicable Time Period that list, or illustrate the roles of, any individuals identified or personnel described in Your responses to Specifications 33-36.

51. Produce Customer Correspondence that You maintain for Your own business purposes (excluding all non-content information such as email header information) relating to the security of the Company's Products or Services or related to any of Your responses to Specifications 22-29. For purposes of this Specification, "Customer Correspondence" means Documents, such as complaints and Your responses to such complaints, that You directly or indirectly received from or sent to a customer, including any complaints or

inquiries to or by Better Business Bureaus or government agencies, and Your responses to those complaints or inquiries.

52. Produce the Company's balance sheets, profit and loss statements, and income statements for the Company's two most recent accounting periods.

53. Produce all Documents discussed or described in Your responses to Specifications that have not otherwise been produced.

**NOTICE: This CID does not seek any information that is prohibited from disclosure under the Cable Communications Policy Act of 1984 ("Cable Act"), 47 U.S.C. §§ 551 et seq., the Satellite Television Extension and Location Act ("STELA"), 47 U.S.C. § 338(i), or the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2701 et seq. To the extent that You are, for purposes of ECPA, a provider of Electronic Communications Service or Remote Computing Service to a customer or subscriber about whom this CID seeks information, do not divulge a record or information pertaining to such customer or subscriber or the content of such customer's or subscriber's communications, other than the content, records, and information specifically requested in this CID. If You have any questions, please contact FTC counsel before providing responsive information.**

**RFPA AND SARS NOTICE: This CID does not seek any financial records for which prior customer notice is required under the Right to Financial Privacy Act ("RFPA"), 12 U.S.C. §§ 3401 et seq. If the Company believes it is a financial institution or an agent of a financial institution under RFPA, 12 U.S.C. §§ 3401(1) & 3403(a), You should not produce any information contained in the financial records of any individual or partnership of five or fewer individuals, and You should contact FTC counsel prior to responding to this CID to discuss what information contained in financial records is subject to production under RFPA. This CID does not seek any Suspicious Activity Reports (SARs). Do not produce any SARs. If You have any questions, please contact FTC counsel before providing responsive information.**

## III. DEFINITIONS

The following definitions apply to this CID:

D-1. "**Administrative Tools**" means the systems, services, or applications that the Company uses to store, process, and administer the Company customer accounts or Personal Information.

D-2. "**Advertisement**" or "**Advertising**" or "**Ad**" means any written or verbal statement, illustration, or depiction that promotes the sale, use, or acquisition of a good or service or is designed to increase consumer interest in a brand, good, or service. Advertising media includes but is not limited to: packaging and labeling; promotional materials; print; television; radio; and Internet, social media, and other digital content.

D-3. "**Company**," "**You**," or "**Your**" means **MGM Resorts International**, its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed

names, and affiliates, whether in real properties or online, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

D-4. "**Consumer Report**" means any consumer report as that term. is defined in Section 603(d)(l) of the Fair Credit Reporting Act, 15 U.S.C. § 1681 a(d)(l ).

D-5. "**Consumer Reporting Agency**" or "**CRA**" means an entity as defined in Section 603(t) of the Fair Credit Reporting Act.

D-6. "**Collaborative Work Environment**" means any platform, application, product, or system used to communicate, or to create, edit, review, approve, store, organize, share, and access Documents, communications, and information by and among users, including Microsoft SharePoint sites, cloud storage systems (e.g., Google Drive, OneDrive, Dropbox), eRooms, document management systems (*e.g.*, iManage), intranets, chat (e.g., Slack), web content management systems (*e.g.*, Drupal), wikis (*e.g.*, Confluence), work tracking software (*e.g.*, Jira), version control systems (e.g., Github), and blogs.

D-7. "**Document**" means the complete original, including all attachments and copies of all hyperlinked materials (other than hyperlinks to publicly accessible websites), all drafts or prior versions, and any non-identical copy, whether different from the original because of notations on the copy, different metadata, or otherwise, of any item covered by 15 U.S.C. § 57b-1(a)(5), 16 C.F.R. § 2.7(a)(2), or Federal Rule of Civil Procedure 34(a)(1)(A), including chats, instant messages, text messages, direct messages, information stored on or sent through social media accounts or messaging or other applications (e.g., Microsoft Teams, Slack), information contained in, hyperlinked to, or sent through Collaborative Work Environments, and information on all devices (including employee-owned devices) used for Company-related activity.

D-8. "**Fair Credit Reporting Act**" or "**FCRA**" means the statute found at 15 U .S.C. § 1681 et. seq.

D-9. "**Identify**" or "**the Identity of**" requires identification of (a) natural persons by name, title, present business affiliation, present business address, telephone number, email address, and username, screen name, handle, or any other identifiers used in communications; or, if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, and the identities of Your contact persons at the business or organization.

D-10. "**Personal Information**" means individually identifiable information from or about an individual, including but not limited to: (a) a first and last name; (b) a home or physical address, including street name and name of city or town; (c) geolocation information sufficient to determine street name and name of a city or town; (d) an email address or other online contact information; (e) a mobile or other telephone number; (f) a date of birth; (g) a government-issued identification number, such as a driver's license, military identification, passport number, or Social Security number; (h) user account credentials, such as a login name and password; (i) credit card or other financial information, including account numbers or domestic routing numbers; or (j) persistent identifiers such as an IP address or device identifier.

D-11. "**Product or Service**" or "**Products or Services**" means any product or service offered by the Company.

D-9. "**Technical Controls**" means security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

## IV. INSTRUCTIONS

I-1. **Petitions to Limit or Quash**: You must file any petition to limit or quash this CID with the Secretary of the FTC no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition must set forth all assertions of protected status or other factual and legal objections to the CID and comply with the requirements set forth in 16 C.F.R. § 2.10(a)(1) – (2). **The FTC will not consider petitions to quash or limit if You have not previously met and conferred with FTC staff and, absent extraordinary circumstances, will consider only issues raised during the meet and confer process.** 16 C.F.R. § 2.7(k); *see also* § 2.11(b). **If You file a petition to limit or quash, You must still timely respond to all requests that You do not seek to modify or set aside in Your petition.** 15 U.S.C. § 57b-1(f); 16 C.F.R. § 2.10(b).

I-2. **Withholding Requested Material / Privilege Claims**: For specifications requesting production of Documents or answers to written interrogatories, if You withhold from production any material responsive to this CID based on a claim of privilege, work product protection, statutory exemption, or any similar claim, You must assert the claim no later than the return date of this CID, and You must submit a detailed log, in a searchable electronic format, of the items withheld that identifies the basis for withholding the material and meets all the requirements set forth in 16 C.F.R. § 2.11(a) – (c). The information in the log must be of sufficient detail to enable FTC staff to assess the validity of the claim for each Document, including attachments, without disclosing the protected information. If only some portion of any responsive material is privileged, You must submit all non-privileged portions of the material. Otherwise, produce all responsive information and material without redaction. 16 C.F.R. § 2.11(c). The failure to provide information sufficient to support a claim of protected status may result in denial of the claim. 16 C.F.R. § 2.11(a)(1).

I-3. **Modification of Specifications**: The Bureau Director, a Deputy Bureau Director, Associate Director, Regional Director, or Assistant Regional Director must agree in writing to any modifications of this CID. 16 C.F.R. § 2.7(l).

I-4. **Scope of Search**: This CID covers Documents and information in Your possession or under Your actual or constructive custody or control, including Documents and information in the possession, custody, or control of Your attorneys, accountants, directors, officers, employees, service providers, and other agents and consultants, whether or not such Documents or information were received from or disseminated to any person or entity.

I-5. **Identification of Responsive Documents**: For specifications requesting production of Documents, You must identify in writing the Documents that are responsive to the specification.

Documents that may be responsive to more than one specification of this CID need not be produced more than once. If any Documents responsive to this CID have been previously supplied to the FTC, You may identify the Documents previously provided and the date of submission.

I-6. **Maintain Document Order**: For specifications requesting production of Documents, You must produce Documents in the order in which they appear in Your files or as electronically stored. If Documents are removed from their original folders, binders, covers, containers, or electronic source, You must specify the folder, binder, cover, container, or electronic media or file paths from which such Documents came.

I-7. **Numbering of Documents**: For specifications requesting production of Documents, You must number all Documents in Your submission with a unique identifier such as a Bates number or a Document ID.

I-8. **Production of Copies**: For specifications requesting production of Documents, unless otherwise stated, You may submit copies in lieu of original Documents if they are true, correct, and complete copies of the originals and You preserve and retain the originals in their same state as of the time You received this CID. Submission of copies constitutes a waiver of any claim as to the authenticity of the copies should the FTC introduce such copies as evidence in any legal proceeding.

I-9. **Production in Color**: For specifications requesting production of Documents, You must produce copies of Advertisements in color, and You must produce copies of other materials in color if necessary to interpret them or render them intelligible.

I-10. **Electronically Stored Information**: For specifications requesting production of Documents, see the attached FTC Bureau of Consumer Protection Production Requirements ("Production Requirements"), which detail all requirements for the production of electronically stored information to the FTC. You must discuss issues relating to the production of electronically stored information with FTC staff **prior to** production.

I-11. **Sensitive Personally Identifiable Information ("Sensitive PII") or Sensitive Health Information ("SHI")**: For specifications requesting production of Documents or answers to written interrogatories, if any responsive materials contain Sensitive PII or SHI, please contact FTC counsel before producing those materials to discuss whether there are steps You can take to minimize the amount of Sensitive PII or SHI You produce, and how to securely transmit such information to the FTC.

Sensitive PII includes an individual's Social Security number; an individual's biometric data; and an individual's name, address, or phone number in combination with one or more of the following: date of birth, driver's license or state identification number (or foreign country equivalent), military identification number, passport number, financial account number, credit card number, or debit card number. Biometric data includes biometric identifiers, such as fingerprints or retina scans, but does not include photographs (with the exception of photographs and corresponding analyses used or maintained in connection with facial recognition software) or voice recordings and signatures (with the exception of those stored in a database and used to

verify a person's identity). SHI includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

I-12. **Interrogatory Responses**: For specifications requesting answers to written interrogatories: (a) answer each interrogatory and each interrogatory subpart separately, fully, and in writing; and (b) verify that Your answers are true and correct by signing Your answers under the following statement: "I verify under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)." The verification must be submitted contemporaneously with Your interrogatory responses.

# EXHIBIT 1

# Notice of Data Breach

October 5, 2023

We recently learned of a cybersecurity issue affecting our company.

**What Happened?**

MGM Resorts International recently disclosed that the company identified a cybersecurity issue affecting certain of our systems and that our investigation into the issue was ongoing. On or around September 29, 2023, we determined that an unauthorized third party obtained personal information of some of our customers on September 11, 2023.

**What Information Was Involved?**

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

We do not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

**What We Are Doing**

Promptly after learning of this issue, we took steps to protect our systems and data, including shutting down certain systems. We also quickly launched an investigation with the assistance of leading cybersecurity experts and are coordinating with law enforcement. We take the security of our systems and data very seriously and have put in place additional safeguards to further protect our systems.

MGM Resorts is notifying relevant customers by email as required by law and has arranged to provide those customers with credit monitoring and identity protection services at no cost to them. Individuals who receive an email from MGM Resorts about this issue should refer to that email for additional information and instructions for enrolling in these services.

**What You Can Do**

If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228. The U.S. Reference Guide below provides recommendations by the U.S. Federal Trade Commission on the protection of personal information.

We regret any inconvenience this issue may have caused. If you have any questions regarding this matter, please refer to the Frequently Asked Questions below or contact 1-800-621-9437 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference engagement number B105892 when calling.

For additional information, please review the U.S. Reference Guide.

U.S. REFERENCE GUIDE

## Frequently Asked Questions

To help answer questions you may have related to this matter, please refer to the FAQs below.

**1. What happened?**

MGM Resorts International recently disclosed that the company identified a cybersecurity issue affecting certain of our systems and that our investigation into the issue was ongoing. On or around September 29, 2023, we determined that an unauthorized third party obtained personal information of some of our customers on September 11, 2023.

**2. What did MGM Resorts do when it discovered the issue?**

Promptly after learning of this issue, we took steps to protect our systems and data, including shutting down certain systems. We also quickly launched an investigation with the assistance of leading cybersecurity experts and are

MGM Resorts is notifying relevant customers by email as required by applicable law and has arranged to provide those customers with credit monitoring and identity protection services at no cost to them. Individuals who receive an email from MGM Resorts about this issue should refer to that email for additional information and instructions for enrolling in these services.

**3. What information has been compromised?**

The affected information included name, contact information (such as phone number, email address, and postal address), gender, date of birth, and driver's license number. For a limited number of customers, Social Security number and/or passport number was also affected. The types of impacted information varied by individual.

We do not believe customer passwords, bank account numbers, or payment card information was affected by this issue.

For individuals who became MGM Resorts customers after February 2019, we do not believe sensitive personal information (such as driver's license number, passport number or Social Security number) was affected by this issue.

This issue did not affect personal information that customers provided in connection with their visit to The Cosmopolitan of Las Vegas.

**4. What should I do to help protect my information?**

We recommend that you:

- Remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports.
- Remain alert for unsolicited communications involving your personal information.
- Order a credit report. If you are in the U.S. and would like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. U.S. residents can order a free credit report by visiting www.annualcreditreport.com or calling toll-free at 1-877-322-8228.

**5. Where can I get more information?**

If you have additional questions regarding this matter, please contact us at 800-621-9437 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Please reference engagement number B105892 when calling.

**6. What if I am in Canada?**

Affected Canadian customers should review the information in the notice that they receive. For outstanding questions you may contact 1-855-984-2828. The call centre is available Monday to Friday, from 8:00 am ET to 8:00 pm ET.

**CERTIFICATION OF COMPLIANCE**
**Pursuant to 28 U.S.C. § 1746**

I, _____, certify the following with respect to the Federal Trade Commission's ("FTC") Civil Investigative Demand directed to MGM Resorts International (the "Company") (FTC File No. 2423028) (the "CID"):

1. The Company identified all documents, information, and/or tangible things ("responsive information") in the Company's possession, custody, or control responsive to the CID and either:

   (a) provided such responsive information to the FTC; or

   (b) for any responsive information not provided, given the FTC written objections setting forth the basis for withholding the responsive information.

2. I verify that the responses to the CID are complete and true and correct to my knowledge.

I certify under penalty of perjury that the foregoing is true and correct.

Date: _____

_____
Signature

_____
Printed Name

_____
Title

**CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY**
**Pursuant to 28 U.S.C. § 1746**

1. I, _____, have personal knowledge of the facts set forth below and am competent to testify as follows:

2. I have authority to certify the authenticity of the records produced by MGM Resorts International (the "Company") and attached hereto.

3. The documents produced and attached hereto by the Company are originals or true copies of records of regularly conducted activity that:

   a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

   b) Were kept in the course of the regularly conducted activity of the Company; and

   c) Were made by the regularly conducted activity as a regular practice of the Company.

I certify under penalty of perjury that the foregoing is true and correct.

Date: _____ _____
Signature

**Federal Trade Commission - Bureau of Consumer Protection**

**Production Requirements**

Revised July 2020

In producing information to the FTC, comply with the following requirements, unless the FTC agrees otherwise. If you have questions about these requirements, please contact FTC counsel before production.

## Production Format

1. **General Format**: Provide load-ready electronic productions with:

    a. A delimited data load file (.DAT) containing a line for every document, unique id number for every document (DocID), metadata fields, and native file links where applicable; and

    b. A document level text file, named for the DocID, containing the text of each produced document.

    Do not produce corresponding image renderings (e.g., TIFF or JPEG) for files in native format unless the FTC requests them. If the FTC requests corresponding image renderings, provide an Opticon image load file (.OPT) containing a line for every image file.

2. **Electronically Stored Information (ESI)**: Documents stored in electronic format in the ordinary course of business must be produced in the following format:

    a. For ESI other than the categories below, submit in native format with all metadata and either document level extracted text or Optical Character Recognition (OCR). Do not produce corresponding image renderings (e.g., TIFF or JPEG) for files in native format unless the FTC requests them. If the FTC requests corresponding image renderings, they should be converted to Group IV, 300 DPI, single-page TIFF (or color JPEG images when necessary to interpret the contents or render them intelligible.)

    b. For Microsoft Excel, Access, or PowerPoint files, submit in native format with extracted text and metadata. Data compilations in Excel spreadsheets or delimited text formats must contain all underlying data, formulas, and algorithms without redaction.

    c. For other spreadsheet, database, presentation, or multimedia formats; instant messages; or proprietary applications, discuss the production format with FTC counsel.

3. **Hard Copy Documents**: Documents stored in hard copy in the ordinary course of business must be scanned and submitted as either one multi-page pdf per document or as 300 DPI single page TIFFs (or color JPEGs when necessary to interpret the contents or render them intelligible), with corresponding document-level OCR text and logical document determination in an accompanying load file.

4. **Document Identification**: Provide a unique DocID for each hard copy or electronic document, consisting of a prefix and a consistent number of numerals using leading zeros. Do not use a space to separate the prefix from numbers.

5. **Attachments**: Preserve the parent/child relationship by producing attachments as separate documents, numbering them consecutively to the parent email, and including a reference to all attachments.

6. **Metadata Production**: For each document submitted electronically, include the standard metadata fields listed below in a standard delimited data load file. The first line of the data load file shall include the field names. Submit date and time data in separate fields. Use these standard Concordance delimiters in delimited data load files:

| Description | Symbol | ASCII Character |
|---|---|---|
| Field Separator | ¶ | 20 |
| Quote Character | Þ | 254 |
| Multi Entry delimiter | ® | 174 |
| <Return> Value in data | ~ | 126 |

7. **De-duplication**: Do not use de-duplication or email threading software without FTC approval.

8. **Password-Protected Files**: Remove passwords prior to production. If password removal is not possible, provide the original and production filenames and the passwords, under separate cover.

**Producing Data to the FTC**

1. Prior to production, scan all data and media for viruses and confirm they are virus-free.

2. For productions smaller than 50 GB, submit data electronically using the FTC's secure file transfer protocol. Contact FTC counsel for instructions. **The FTC cannot accept files via Dropbox, Google Drive, OneDrive, or other third-party file transfer sites**.

3. If you submit data using physical media:

    a. Use only CDs, DVDs, flash drives, or hard drives. Format the media for use with Windows 7;

    b. Use data encryption to protect any Sensitive Personally Identifiable Information or Sensitive Health Information (as defined in the instructions), and provide passwords in advance of delivery, under separate cover; and

    c. Use a courier service (e.g., Federal Express, UPS) because heightened security measures delay postal delivery.

4. Provide a transmittal letter with each production that includes:

    a. Production volume name (e.g., Volume 1) and date of production;

    b. Numeric DocID range of all documents in the production, and any gaps in the DocID range; and

    c. List of custodians and the DocID range for each custodian.

**Standard Metadata Fields**

| DAT FILE FIELDS | DEFINITIONS | POPULATE FIELD FOR: |
|---|---|---|
| DocID | Unique ID number for each document | All Documents |
| FamilyID | Unique ID for all documents in a family including parent and all child documents | All Documents |
| ParentID | Document ID of the parent document. This field will only be populated on child items | All Documents |
| File Path | Path to produced native file | All Documents |
| TextPath | Path to document level text or OCR file | All Documents |
| Custodian | Name of the record owner/holder | All Documents |
| AllCustodians | Names of all custodians that had copy of this record (populate if data was deduplicated or email threading was used) | All Documents |
| Source | Source of documents: CID, Subpoena, Third Party Data, etc. | All Documents |
| Filename | Original file name | All Documents |
| File Size | Size of documents | All Documents |
| File Extensions | Extension of file type | All Documents |
| MD5 Hash | Unique identifier for electronic data used in de-duplication | All Documents |
| PRODUCTION_VOLUME | Production Volume | All Documents |
| HASREDACTIONS | Redacted document | All Documents |
| Exception Reason | Reason for exception encountered during processing (e.g., empty file, source file, password-protected file, virus) | All Documents |
| PRODBEG | Beginning production bates number | Documents with Produced Images |
| PRODEND | Ending production bates number | Documents with Produced Images |
| PRODBEG_ATTACH | Beginning production family bates number | Documents with Produced Images |
| PRODEND_ATTACH | Ending production family bates number | Documents with Produced Images |
| Page Count | The number of pages the document contains | Documents with Produced Images |
| From | Names retrieved from the FROM field in a message | Emails |
| To | Names retrieved from the TO field in a message; the recipient(s) | Emails |
| CC | Names retrieved from the CC field in a message; the copied recipient(s) | Emails |
| BCC | Names retrieved from the BCC field in a message; the blind copied recipient(s) | Emails |
| EmailSubject | Email subject line | Emails |
| Date Sent | The date an email message was sent | Emails |
| Time Sent | The time an email message was sent | Emails |
| Date Received | The date an email message was received | Emails |
| Time Received | The time an email message was received | Emails |
| Author | File Author | Loose Native Files and Email Attachments |
| Title | File Title | Loose Native Files and Email Attachments |
| Subject | File Subject | Loose Native Files and Email Attachments |
| Date Created | Date a document was created by the file system | Loose Native Files and Email Attachments |
| Time Created | Time a document was created by the file system | Loose Native Files and Email Attachments |
| Date Modified | Last date a document was modified and recorded by the file system | Loose Native Files and Email Attachments |
| Time Modified | Last time a document was modified and recorded by the file system | Loose Native Files and Email Attachments |
| Date Printed | Last date a document was printed and recorded by the file system | Loose Native Files and Email Attachments |
| Time Printed | Last time a document was printed and recorded by the file system | Loose Native Files and Email Attachments |

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

# RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION OF ACTS AND PRACTICES RELATED TO CONSUMER PRIVACY AND/OR DATA SECURITY

File No. 1823036

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others are engaged in, or may have engaged in, deceptive or unfair acts or practices related to consumer privacy and/or data security, including but not limited to the collection, acquisition, use, disclosure, security, storage, retention, or disposition of consumer information, in or affecting commerce, in violation of Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain monetary relief would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; FTC Procedures and Rules of Practice, 16 C.F.R. § 1.1 *et seq.* and supplements thereto.

By direction of the Commission.

April J. Tabor
Acting Secretary

**Issued: March 14, 2019**

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:** Joseph J. Simons, Chairman
Noah Joshua Phillips
Rohit Chopra
Rebecca Kelly Slaughter
Christine S. Wilson

**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**

File No. 0023284

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others have engaged or are engaging in acts or practices in violation of Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827, the Privacy of Consumer Financial Information Rule (16 C.F.R. pt. 313), the CFPB's Regulation P (12 C.F.R. pt. 1016), the Safeguards Rule (16 C.F.R. pt. 314), or whether any financial institution or its affiliates have engaged or are engaging in deceptive or unfair acts or practices in or affecting commerce with respect to the privacy or security of consumer information in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, as amended. The investigation is also to determine whether Commission action to obtain monetary relief would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory process available to it be used in connection with this investigation for a period not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five-year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five-year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five-year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; and FTC Procedures and Rules of Practice, 16 C.F.R § 1.1 *et seq.*, and supplements thereto.

By direction of the Commission.

April J. Tabor
Acting Secretary

**Issued: July 16, 2019**

**UNITED STATES OF AMERICA**
**BEFORE FEDERAL TRADE COMMISSION**

**COMMISSIONERS:**

Robert Pitofsky, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle

**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**

File No. 992-3120

Nature and Scope of Investigation:

An investigation to determine whether persons, partnerships or corporations may be engaging in, or may have engaged in, acts or practices in violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended, relating to information furnished to consumer reporting agencies, maintained in the files of consumer reporting agencies, or obtained as a consumer report from a consumer reporting agency. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. § § 46, 49, 50 and 57b-1, as amended; FTC Procedures and Rules of Practices 16 C.F.R. 1.1 et seq. and supplements thereto.

Title VI of the Consumer Credit Protection Act, Section 621, 15 USCA § 1681s.

By direction of the Commission.

Donald S. Clark
Secretary

Dated: April 15, 1999

# EXHIBIT 2

**DLA Piper LLP (US)**
One Liberty Place
1650 Market Street
Suite 5000
Philadelphia, Pennsylvania 19103-7300
www.dlapiper.com

Brian J. Boyle
Brian.Boyle@us.dlapiper.com
T 215.656.2450
F 215.606.2150

February 13, 2024

Carla Cheung
Federal Trade Commission
Western Region Los Angeles
10990 Wilshire Boulevard, Suite 400
Los Angeles, CA 90024
(202) 644-6785

**Re: Civil Investigative Demand to MGM Resorts International, No. 2423028**

Dear Carla:

As discussed on our last call, we have concerns with a number of the Specifications in the CID. This letter is to outline those concerns, in the hopes of reaching agreement on modifying the CID.

I note at the outset that because you have declined to grant any extension of the initial deadline to file a petition to quash, you have left us very little time to discuss these complex issues. Nonetheless, my hope is that the detail included in this letter will allow us to expeditiously resolve the many serious issues posed by the CID.

Our concerns fall into the following general categories: requests premised on inapplicable rules; requests for information about a criminal investigation; improper "catch all" questions; requests calling for privileged information; vague and ambiguous requests; requests calling for speculation; requests of little or no relevance; and excessively burdensome requests.

*Requests Premised on Inapplicable Rules*

The CID is explicitly premised on two rules – the Red Flags Rule, 16 C.F.R Part 1681, and the Safeguard Rule, 16 C.F.R Part 314 (the "Rules"). This problem infects the totality of the CID, including each Specification. Indeed, many of the Specifications appear tailored to elicit information with no conceivable relevance to anything other than the Rules, including Requests 30 through 35.

The Rules do not apply to MGM, however. They apply to financial institutions, or entities "significantly" engaged in financial activities. See e.g.16 C.F.R. § 314.2(h)(1). The Rules have never been extended to the gaming industry, and efforts by the Commission to apply the Rules beyond the financial services industry have been rejected. *American Bar Ass'n v. FTC*, 671 F. Supp. 2d 64 (D. D.C. 2009) ("*ABA*"), *vacated on other grounds American Bar Ass'n v. FTC*, 636 F.3d 641 (D.C. Cir. 2011).

Enforcing the CID against MGM would be subject to challenge as beyond the Rules, and beyond the FTC's rulemaking authority.

DLA PIPER



*Criminal Investigation*

Several of the Specifications, including for example 22 and 46, potentially call for information related to investigations by federal law enforcement. Furthermore, during our meet and confer on February 6, 2024, you requested that MGM prioritize producing documents previously produced to law enforcement agencies, and expressly mentioned the Federal Bureau of Investigation ("FBI"). This raises at least three serious issues. First, requiring a victim of crime to produce such information has the effect of punishing crime victims for assisting law enforcement and sets a dangerous precedent. Plainly, your request disincentivizes cooperation with law enforcement.

Second, the fact that any particular information was provided to law enforcement—particularly by a crime victim—in no way entitles the FTC to that information. Nothing in the FTC Act, or in any other relevant legislation, enlarges the FTC's authority in such circumstances. In this case, it certainly does not supersede the numerous problems with the CID outlined in this letter.

Third, this request creates a dangerous practical problem. Although MGM has cooperated with federal law enforcement in connection with the cybercrimes that MGM was a victim of, MGM has neither control over nor visibility into the details of any investigations by the FBI or other agencies. Therefore, MGM has no way of knowing what information may adversely affect criminal investigations or prosecutions if disclosed. It is dangerous and highly prejudicial to put MGM in the position of potentially jeopardizing such proceedings.

*Improper "Catch All" Questions*

In a recent Order granting in part a Motion to Quash a CID, the Commission indicated that "catch all questions," such as "provide all other information [on a subject] not otherwise provided in Your responses," are disfavored, and struck a number of catch all questions from the CID at issue. Amazon ROSCA, File No. 212 3050, September 21, 2022. We believe that a number of the requests in the instant CID are improper "catch all" questions, including Requests 19(a) (describe administrative tool policies "not described in response to another Specification"), 46 (Produce "all documents related to the incident(s)"), and 53 (produce documents "that have not otherwise been produced"). Like the improper requests in *Amazon ROSCA,* these catch all questions are not "sufficiently definite to provide guidance as to what is to be produced by standards or criteria that make clear the duty of the person subpoenaed." *Amazon Rosca*, Order at 13, quoting *Resolution Trust Corp. v. Greif*, 906 F. Supp. 1446, 1452 & n.2 (D. Kan. 1995) (citing *In re Grand Jury Proceedings*, 601 F.2d 162 (5th Cir.1979))

*Requests for Privileged Information*

Several of the requests seek information protected by privilege. These include audits and assessments covered by the attorney work product privilege sought in Requests 20, 21, 22 (e) and 22 (f).

*Vague and Ambiguous Requests*

A number of the requests are rendered impermissibly vague and ambiguous through their use of undefined, unexplained, and unclear terms and phrases. These include: "design elements" that "enforce or encourage compliance," Request 16(e); "efforts to align … cybersecurity risk management with the

DLA PIPER



NIST," 18; data "outside of … digital systems," 19(b); "software update practices," 14; "incident response practices," 13; "unauthorized person(s) among other things," 22; timeline "of all events," 22(b); "how You are certain You have identified" certain accounts, 22 (p); "individuals who have or had the ability to control or participate in the Company's practices, policies and procedures,"33; and "individuals who have the ability to control or participate in the drafting" of certain representations, 36.

*Requests Calling for Speculation*

Many of the requests call for data and information beyond MGM's knowledge and control. For example, Request 22, through its subparts (a) through (u), asks 23 different questions seeking extensive and precise detail as to whether, when, and how the threat actor obtained access to customer personal information. As you know, the FBI is currently undertaking a criminal investigation on precisely these issues. At least until the FBI and other investigators reach their conclusions, any response by MGM to these questions would be premised on speculation.

*Requests of Little or No Relevance*

A fundamental problem with the CID is the requested time frame, dating back to 2021. This problem infects Specification Nos. 8-9, 11(a), 26, 32-34, 37, 39, 43-44, and 49-50, each of which expressly incorporate the "Applicable Time Period," as well as Specification Nos. 1-7, 10, 12-21, 29-31, 35-36, 40-42, and 45-48, which implicitly incorporate the CID's definition by failing to identify any time period more specific. This incident occurred in late 2023, and the outcome of this investigation will turn on MGM's security practices in effect at the time of the incident, and whether MGM acted reasonably in late 2023 in response to the incident. MGM's practices in 2021 and 2022 have no bearing on the reasonableness of its security practices in 2023, nor on the efficacy of MGM's response to the incident in question. Responding to these broad requests for a three-year period would impose a significant burden on MGM, while yielding information that would be entirely irrelevant to this investigation.

In addition, the CID appears to assume, incorrectly, that the incident in question was the result of "phishing" and "spearfishing," Requests 9, 22(b), seeks information on remedial measures that would not be admissible, Request 22 (g), requests extensive detail on cybersecurity technology that the company did *not* employ, Request 17, and throughout requests information regarding MGM's non-US customers, see e.g. request 5(a), 22 (c), 22 (d), 22 (u), 25, and 28. These requests are not reasonably calculated to lead to relevant evidence.

*Excessively Burdensome Requests*

Responding to these requests as drafted would impose an excessive burden on MGM. Counting subparts, the request contains 92 interrogatories, almost all of which will require significant investigation and analysis in order to properly respond, and 15 exceptionally broad document requests, including a massive "catch all" request for "all Documents related to the incident(s)," Request 46, and a request that would require MGM to search every advertisement, web page, press release, and every other public communication for any representations regarding cybersecurity (which are highly unlikely to exist except for in MGM's Privacy Policy.) The sheer volume of these requests – especially given the three-year time frame – is excessively burdensome on its face. Responding to this CID in its current form is certain to disrupt and hinder MGM's operations.

DLA PIPER



The CID is also overbroad in several ways. For example, the CID purports to require MGM to produce information about MGM's organizational structure, *see* Specification Nos. 33-37, including "how authority and responsibility have been distributed to employees, officer[s], directors, principals, and owners with the Company" without *any* limitation, *see* Specification No. 37. Plainly, the manner in which authority is delegated across all of MGM—a global hospitality and entertainment company, with myriad operations distributed across various properties—is not relevant to this investigation into its cyber security practices. Similarly, Specification Nos. 5 and 6 call for information regarding sales and net revenues for every product or service offered by MGM, as well as the types of customer information collected in connection with those offerings. Neither request contains *any* substantive limitation of *any kind*, and therefore would purport to require production of information far afield of the issues in this investigation.

* * *

I look forward to speaking again on our upcoming call. If you would like to speak in the meantime, please do not hesitate to contact me.

Sincerely,

Brian J. Boyle

Brian J. Boyle

BJB:ma

# Exhibit 3

[Confidential – Redacted]

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

| | | |
|---|---|---|
| *In re* Civil Investigative Demand to MGM Resorts International | ) | FTC File No. 2423028 |

DECLARATION OF AMY WONG

1. I am a Vice President at MGM Resorts International ("MGM"). My responsibilities include oversight of MGM's marker limit ("marker") operations for Las Vegas properties. This Declaration is based on my personal knowledge.

2. MGM provides markers to select high-volume customers for their use while gaming at MGM properties. Markers are provided solely for the convenience of our high-volume customers, incidental to the casino services we provide. They have no value to customers other than for use at an MGM casino.

3. When applying for a marker, customers must identify a financial account with sufficient funds to cover the amount of the marker and execute a document that, once accepted by MGM, constitutes a negotiable instrument.

4. The online application to receive a marker includes the following language, to which customers must agree in order to receive a marker:

> I REPRESENT THAT AT THE TIME I SIGN ANY MARKER, I HAVE ON DEPOSIT IN ACCOUNTS ON WHICH I AM AN AUTHORIZED SIGNATORY FOR ALL PURPOSES, WITHOUT RESTRICTION, FUNDS SUFFICIENT TO PAY SUCH MARKER UPON DEMAND OR PRESENTMENT....
>
> Warning: for the purposes of Nevada law, a credit instrument is identical to a personal check and may be deposited in or presented for payment to a bank or other financial institution on which the credit instrument is drawn.

5. Attachment 1 to this Declaration is a copy of the instrument customers must execute when drawing for a marker. It is in the same form as a personal check, and indicates that markers are "identical to a personal check."



DW

6. CONFIDENTIAL

7. CONFIDENTIAL

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: February 19, 2024

2/19/2024

Amy Wong



AW

# ATTACHMENT 1

Check Number: 773490193

Player ID: 64149765

Pay to Order Of: Bellagio $5,000.00

Five Thousand and No/100 USD

I acknowledge receiving the above amount and I represent that I have funds on deposit in accounts on which I am an authorized signatory for all purposes without restriction, sufficient to pay this credit instrument upon demand. I authorize Bellagio Hotel and Casino to obtain my financial information from any source and complete this credit instrument as is necessary for the credit instrument to be presented for payment as a negotiable instrument. I agree (1) to pay all costs of collection, including attorney's fees, (2) to waive any requirements of presentment (3) that the debt for which this credit instrument is issued was incurred in the State of Nevada (4) that Nevada law exclusively applies to this credit instrument and the enforcement thereof and (5) to submit to the exclusive jurisdiction of any court, state or federal, in the State of Nevada. A credit instrument in Nevada is identical to a personal check. Willfully drawing or passing a credit instrument knowing there are insufficient funds in an account upon which it may be drawn, or with the intent to defraud, is a crime in the State of Nevada which may result in criminal prosecution. I also acknowledge that an independent agent collecting front money deposits or payments on any of my debts is my agent and not an agent of Bellagio Hotel and Casino.

Signature: _____
MICKEY MOUSE

## *PAYMENT STUB*

Bellagio

MICKEY MOUSE

Player ID: 64149765

Document #: 773490193

Ref #:

Issued: 02/15/2024 18:08

Location: Cage Supv 4

Acct. Date: 15 Feb 2024

Shift: Swing

Amount: $5,000.00 USD

Date: _____ Amt Paid Cash: _____

Location: _____ Amt Paid Chips: _____

Time: _____ Amt Paid Other: _____

New Marker #: _____

_____
Supervisor Signature-ID #

_____
Dealer/Cashier Signature-ID #

## *ISSUE STUB*

Bellagio

MICKEY MOUSE

Player ID: 64149765

Document #: 773490193

Ref #:

Issued: 02/15/2024 18:08

Location: Cage Supv 4

Acct. Date: 15 Feb 2024

Shift: Swing

Amount: $5,000.00 USD

Issued By: Jacob Margulies

_____
Supervisor Signature-ID #

_____
Dealer/Cashier Signature-ID #

MICKEY MOUSE

Player ID: 64149765

Check Number: 773490193

Issued: 02/15/2024 18:08

Location: Cage Supv 4

Shift: Swing

Pay to Order Of: Bellagio $5,000.00

Five Thousand and No/100 USD

**NON-NEGOTIABLE**

ABA #: Acct #:

Signature: _____
MICKEY MOUSE

# EXHIBIT 4

**UNITED STATES OF AMERICA**
**BEFORE THE FEDERAL TRADE COMMISSION**

| | | |
|---|---|---|
| *In re* Civil Investigative Demand to MGM Resorts International | ) | FTC File No. 2423028 |

DECLARATION OF JOHN BRANDEN NEWMAN

1. I am the Chief Information Security Officer of MGM Resorts International ("MGM"). This Declaration is based on my personal knowledge.

2. I have reviewed the Federal Trade Commission's Civil Investigative Demand ("CID") to MGM in the above-captioned matter.

3. The CID requests more than 100 different categories of ambiguously defined documents and information.

4. Obtaining this information, if possible at all, and to the extent it exists, would be an extremely difficult process. It would involve substantial work on my part, as well as from other employees in multiple functional roles within the company. The process would take a very substantial amount of time—likely months—and would distract me and others from our ordinary duties at MGM.

5. This comes at a time when there are already particularly high demands on MGM staff, including as a result of the September 2023 cyberattack of which MGM was a victim.

6. This is likely to significantly adversely affect MGM and interfere with the responsibilities of the individual employees involved.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: February 15, 2024

John Branden Newman

# EXHIBIT 5

UNITED STATES OF AMERICA
**FEDERAL TRADE COMMISSION**
WESTERN REGION LOS ANGELES

10990 Wilshire Blvd., Suite 400
Los Angeles, CA 90024
Phone: (310) 824-4300

February 15, 2024

Via E-Mail
Brian J. Boyle
DLA Piper LLP
One Liberty Place
1650 Market Street, Suite 5000
Philadelphia, PA 19103-7300
brian.boyle@us.dlapiper.com

Re: Civil Investigation Demand issued to MGM Resorts International
FTC Matter No. 2423028

Dear Mr. Boyle:

On January 25, 2024, the Federal Trade Commission ("FTC") issued a Civil Investigative Demand ("CID") to MGM Resorts International ("MGMRI") for specified documents and information. The deadline for responding to the CID is February 26, 2024.

On February 29, 2024, MGMRI acknowledged receipt of the CID. On February 6, 2024, MGMRI and the FTC telephonically met and conferred regarding the CID pursuant to 16 CFR § 2.7(k). On February 14, 2024, during a telephone meet and confer, MGMRI requested the modifications to certain specifications in the CID. The FTC agrees to modify the specifications listed below as follows:

- **Specification 16(e):** Describe in detail the Company's practices, policies, and procedures for granting, modifying, or revoking an employee's authorization, and for modifying or resetting an employee's means of authentication, to access the Company's Administrative Tools, including: (e) The design elements incorporated into the Company's data managements systems, including the implementation of any Technical Controls, to enforce or encourage compliance with the practices, policies, and procedures described in Specification 16.

  Will be modified to the following:

  **Amended Specification 16(e):** Describe in detail the Company's practices, policies, and procedures for granting, modifying, or revoking an employee's authorization, and for modifying or resetting an employee's means of authentication, to access the Company's Administrative Tools, including: (e) Technical Controls incorporated into the Company's data managements systems intended to enforce or encourage compliance with the practices, policies, and procedures described in Specification 16.

- **Specification 18:** Describe in detail the Company's efforts to align its cybersecurity risk management with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

  Will be modified to the following:

  **Amended Specification 18:** Explain in detail the Company's efforts to align its cybersecurity risk management with the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including but not limited to efforts as referenced in regulatory filings in a May 2023 shareholder proxy statement filed with the Securities and Exchange Commission.

- **Specification 19(a):** State the level of Payment Card Industry Data Security Standard (PCI DSS) that the Company considers itself subject to, and describe in detail all practices, policies, and procedures the Company has in place to maintain compliance, including: (a) Any practices, policies, and procedures regarding the Company's Administrative Tools not described in response to another Specification;

  MGMRI requests that this specification be deleted in its entirety. The FTC does not agree to delete this specification but will modify it to the following:

  **Amended Specification 19(a):** State the level of Payment Card Industry Data Security Standard (PCI DSS) that the Company considers itself subject to, and describe in detail all practices, policies, and procedures the Company has in place to maintain compliance, including: (a) Any practices, policies, and procedures regarding the Company's Administrative Tools.

- **Specification 19(b):** State the level of Payment Card Industry Data Security Standard (PCI DSS) that the Company considers itself subject to, and describe in detail all practices, policies, and procedures the Company has in place to maintain compliance, including: (b) Any practices, policies, and procedures for handling PCI DSS-covered data outside of the Company's digital systems, including the use of manual or paper record keeping.

  Will be modified to the following:

  **Amended Specification 19(b):** State the level of Payment Card Industry Data Security Standard (PCI DSS) that the Company considers itself subject to, and describe in detail all practices, policies, and procedures the Company has in place to maintain compliance, including: (b) Any practices, policies, and procedures for handling non-digital PCI DSS-covered data, including the use of manual or paper record keeping.

- **Specification 22(b):** 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, as referenced in Exhibit 1, attached. In addition: (b) Describe what occurred and the timeline of

all events, including a description of all phishing attacks involved and, if implemented, an explanation of how multifactor authentication was circumvented.

Will be modified to the following:

**Amended Specification 22(b):** 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, as referenced in Exhibit 1, attached. In addition: (b) Describe what occurred and the timeline of all events from the time unauthorized persons(s) initiated contact with the Company for the purpose of gaining access to its information systems until January 25, 2024, including a description of all phishing attacks involved and, if implemented, an explanation of how multifactor authentication was circumvented.

- **Specification 22(p):** 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, as referenced in Exhibit 1, attached. In addition: (p) Describe the Company's containment of the unauthorized access, including whether and how You are certain You have identified all impacted customer accounts and eliminated the unauthorized individual(s)'s access.

  Will be modified to the following:

  **Amended Specification 22(p):** 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, as referenced in Exhibit 1, attached. In addition: (p) Describe the Company's containment of the unauthorized access, including whether and how you contend you have identified all impacted customer accounts and eliminated the unauthorized individual(s)'s access.

- **Specification 36:** Identify all individuals who have the ability to control or participate in the drafting of the Company's representations listed in Your response to Specification 29. For each person, state the dates of the person's employment or affiliation with the Company, all title(s) or position(s) held at the Company, and whether the person is currently employed by the Company.

  Will be modified to the following:

  **Amended Specification 36:** Identify all individuals who drafted and/or approved the Company's representations listed in Your response to Specification 29. For each person, state the dates of the person's employment or affiliation with the Company, all title(s) or position(s) held at the Company, and whether the person is currently employed by the Company.

- **Specification 46:** Produce all Documents related to the security incident(s) affecting the Administrative Tools that the Company identified in September 2023, and which is referenced in Exhibit 1, attached.

  MGMRI requests that this specification be deleted in its entirety. The FTC does not agree to delete this specification but will modify it to the following:

  **Amended Specification 46.** 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, and which is referenced in Exhibit 1, attached.

- **Specification 53:** Produce all Documents discussed or described in Your responses to Specifications that have not otherwise been produced.

  Will be modified to the following:

  **Amended Specification 53:** Produce all Documents referenced in Your responses to Specifications.

**Specifications 5(a), 22(c), 22(d), 22(u), 25, and 28**, will be modified to limit the scope of information sought to customers located within the United States.

The FTC reserves all rights provided by the CID and applicable laws and regulations. If MGMRI has any questions, please contact Carla Cheung (ccheung1@ftc.gov; 202-644-6785) or David Hankin (dhankin@ftc.gov; 202-227-1521) as soon as possible. Thank you for your courtesy and cooperation.

Sincerely,

MARICELA SEGURA Digitally signed by MARICELA SEGURA
Date: 2024.02.15 10:51:49 -08'00'

Maricela Segura
Regional Director
Western Region Los Angeles