LABOR RELATIONS

UNITED STATES POSTAL SERVICE

August 31, 2022

Mr. Ivan D. Butts
President
National Association of Postal Supervisors
1727 King Street, Suite 400
Alexandria, VA 22314-2753

Dear Ivan:

As a matter of general interest, the Postal Service's Corporate Information Security Office (CISO) was notified that MGM Resorts experienced an information breach in 2019. Postal employees who made hotel reservations at MGM Resorts prior to 2017 may have had personal information, which they used to make their reservation, compromised.

CISO has been notified of employees with @usps.gov, @uspis.gov, or @uspsoig.gov email address who have had information disclosed on the internet. The identified employees will receive an email directly from CISO informing them of the MGM Resorts information breach and tips to remain vigilant as a result of the increased possibility of being targeted by phishing campaigns at their Postal email address.

We have enclosed a final copy of the email CISO will send to the identified impacted Postal employees.

Please contact Bruce Nicholson at extension 7773 if you have questions concerning this matter.

Sincerely,

James Lloyd
Director (A)
Labor Relations Policies and Programs

Enclosure

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-4101
WWW.USPS.COM

From: Cybersafe
To: Cybersafe
BCC: <USPS, USPIS, OIG active users impacted by leak>
Subject: CyberSafe Notification of potential impact of MGM Resorts guest records leak

Message:
The U.S. Postal Service's Corporate Information Security Office (CISO) has been notified that your @usps.gov, @uspis.gov, or @uspsoig.gov email address and other personal information has been disclosed on the internet. The personal information and the email address may include your full name, address, phone number, and date of birth. This information is believed to be related to a 2019 theft of more than 10 million guest records from MGM Resorts for guests who registered before December 2017.[1] The Postal Service was not breached; this was an incident at MGM Resorts. The compromised information would have consisted of whatever information individuals used to make hotel reservations, including work or personal phone numbers and addresses. MGM Resorts has stated that the compromise did not extend to financial information or credit card data.

This information had previously been disclosed online by hackers following the theft. No new breach has occurred, but certain information has recently reappeared on additional internet forums. As a result, we are providing you with this notice for your information and helping you remain vigilant for cyber threats and phishing attacks.

CISO cautions you to be aware of the possibility of being targeted by phishing campaigns at your USPS or USPIS email address, or through smishing campaigns targeting the phone number you provided at the time of your reservation. If you receive a suspicious email, click the "Report to CyberSafe" button in your Outlook toolbar. If you don't see the "Report to CyberSafe" button in your Outlook toolbar, you can install the add-on by following the instructions on the USPS ServiceNow website. Should you receive a suspicious text message, delete the message.

Additional tips for dealing with smishing or phishing attacks include:

- **Don't click:** Do not open any link or attachment from a phone number you do not have saved in your contacts list or cannot verify. A best practice is not to click any links on your mobile devices.
- **Don't answer:** For vishing, according to Norton, do not answer calls from unknown numbers – let them go to voice mail. The IRS, Social Security, or Medicare will not initiate contact with you over the phone. Do not allow yourself to be panicked into responding with false urgency. Hand up on scam callers.
- **Filter messages:** Filtering unknown senders will block notifications from unsaved phone numbers, decreasing the likelihood of falling for a smishing scam. To filter unknown numbers on your USPS device, follow these steps:
    - Apple users: Go to Settings > Messages and toggle on the "Filter Unknown Senders" option. This will create a new tab in your Messages app called "Unknown Senders."
    - Android users: Go to Settings > Spam Message Settings and select the "Block Unknown Senders" option.

If you are interested in learning more about phishing, smishing, vishing, or other cyber threats, CISO encourages you to visit Cybersafe at https://blue.usps.gov/cyber/. You can learn more about protecting

[1] They also advised that they notified affected customers in accordance with state laws.

your personal information by visiting the Federal Trade Commission's Consumer Advice website or contacting them at 1-877-438-4338 (TTY: 1-866-653-4261).

Additional information regarding the MGM reservation breach and the current exposure is reported on the Norton and TechRadar sites. CISO cannot vouch for the accuracy of this information.

Sincerely,

USPS CISO CSOC

CyberSafe: 1-866-877-7247

International CyberSafe: 001-919-674-1450

Email: CyberSafe@usps.gov

Phone: 1-866-877-7247

For information security tips visit the CyberSafe at USPS Blue page.
Report information security incidents or suspicious activities to the CyberSecurity Operations Center at cybersafe@usps.gov or 866-877-7247.