Exhibit 11

INFORMATION SECURITY REQUIREMENTS

The following security controls were reviewed and tested in 2023 by the Marriott Global Information Security (GIS) Risk and Compliance team. Toast, Inc. (herein "Vendor" or "Provider") agrees to resolve any non-compliant issues within any specified time frames identified herein and agrees to remain in compliance with all other controls as tested. Vendor shall notify Marriott (herein "MI" or "Marriott") of any changes in the system as set forth herein that could impact the system security such as major modifications or changes to the hosting/data center location.

Vendor has agreed to perform actions as set forth below to address controls identified during the review as Non-Compliant with MI security requirements.

For example: Integrate with MI SSO, Provide SOC reports, Resolve scan findings, etc.

Compliance

1. Application or service being provided to MI has been reviewed by an independent third party and a compliance report or certification letter can be provided. (ex. SOC2 Type 1 or PCI Attestation of Compliance or equivalent).
2. Data Center or Co-location facility used to host the service or application has been reviewed by an independent third party and a compliance report or certification letter can be provided, subject to any additional requirements, including a non-disclosure agreement, of such third party. (ex. Service Organization Controls (SOC) 1 Type 2 report, SOC 2 Type 2 report, an ISO 27002 review or equivalent).
3. At Vendor's election, Vendor allows MI or authorized MI partner/sub-contractor to remotely run non-invasive, credentialed web application/vulnerability scans using industry vendor accepted tools to test the security of the service or application, or Vendor will provide a web application scan report performed by an independent third-party at least annually. Any Critical, High or Medium security issues discovered by these scans will be remediated within time frames agreed to in coordination with MI. (Typically, Critical & High level risks within 30 days and Medium level risks within 60 days). "Critical", "High", and "Medium" severity are each defined by the scoring method set forth in the NIST CVSS 3.0 standard as they are calculated based on the Toast platform.
4. 2Vendor must validate on an annual basis to Marriott that the service that Marriott has engaged in with the service provider is covered by a PCI compliance review (AOC, ROC or SAQ) as may be mutually agreed upon by both parties.

Network Security

5. A firewall or security group exists at each Internet connection and the internal network zone.
6. For web applications, an automated solution (such as a web-application firewall) that continually checks traffic to detect and prevent web-based attacks against externally facing web applications is in place.

7. A formal process is in place for approving and testing all external network connections and changes to firewall configurations.
8. Documentation and business justifications exist for the use of insecure services, protocols or ports and includes documentation of security features implemented to mitigate the risks of using insecure services.
9. Firewall (Security/Network Group) and router rule sets are reviewed at least every six months.
10. Marriott data is not stored on any system components connected directly to the Internet (i.e. on the web servers or in the DMZ).
11. A Network Intrusion Detection or Prevention System (NIDS/NIPS) will be in place to detect, alert on, block or initiate response to potentially malicious activity by July 2023.
12. For communications via HTTPS (web applications, web services, etc.) only non-vulnerable protocols & ciphers are enabled (i.e. TLS 1.2 or higher).
13. Reserved.
14. Network access (non-console) to systems hosting Marriott Data for administrative purposes use encryption technologies such as SSH, VPN or TLS for web-based management.

Configuration Management

15. All patches and system and software configuration changes are tested before deployment.
16. Separate development, test, and production environments exist for developing and/or testing changes to systems or software.
17. Users access each environment (dev, test, QA, Prod, etc.) through segmented access with defined and documented separation of duties between the personnel or functions within each environment.
18. Production Marriott Data is not being used within development environments. Any copies of data used in QA, user acceptance or staging environments for testing purposes has been properly anonymized (masked) or pseudonymized (transformed) using security industry-recognized methods.
19. Material change control procedures are followed and include at least the following steps:
    a. Documentation of impact for all material changes
    b. Sign-off by appropriate parties
    c. Testing of operational functionality
    d. Back-out procedures for all material changes
20. All system components (operating systems, databases, appliances, etc.) have configuration standards that assure all known security vulnerabilities are addressed and the systems are secured/hardened using industry-accepted standards.
21. For any custom developed code, source code repositories are secured, strict access control policies are implemented in accordance with industry standard and all changes or access to code is logged.
22. All system hardware and software are current supported versions by the manufacturer. No hardware or software components which have become “end of life” or have known issues that impact the performance or security of the system.

Identity & Access Management

23. For web applications that will allow MI associates to login, the system supports SAML 2.0 to integrate with Marriott's Single Sign-On (SSO) solution. If SSO cannot be implemented the alternative authentication & authorization system provided must be approved by MI and should support MFA for end user access.
24. An access control system has been established that permits MI to restrict access based on a user's need to know and is set to "deny all" unless specifically allowed by MI.
25. Written procedures are in place to describe how user access to systems is granted, updated and removed. Procedures include how permissions (authorizations) are granted and the recurring review process to ensure only valid users have access.
26. Vendor passwords require a minimum length of 12 characters for all passwords and complexity (alphanumeric, unrelated to user ID, contain at least one number (or special character) and one alpha character, and not all numbers or all characters).
27. Reserved.
28. Accounts with administrative access that have been inactive (not used) in over 90 days are automatically or manually removed/disabled.
29. Passwords do not appear or are masked on the screen when entered.
30. Idle sessions for more than 15 minutes require the user to enter a second factor to enter the point of sale system. Reserved.
    Reserved
31. Reserved.
32. Reserved.
33. The application validates the user identifier and user authenticator as a pair and rejects the logon attempt if the pair is invalid. The system does not inform the user on which of the two is wrong.
34. All passwords are stored in a cryptographic hash format that is generated by a one-way key derivation function (KDF), salted hash or encryption. Fully suitable methods (in order of preference): Argon2, PBKDF2, scrypt and bcrypt.
35. All users are assigned a unique ID before allowing them to access system components. (No shared or group accounts are used.)
36. Vendor-supplied defaults accounts & passwords are changed, and unnecessary services are removed before the system is used in a production environment.
37. Remote access to the network or systems that host Marriott Data by employees, administrators or third parties (contractors) requires multi-factor authentication.
38. All access to web consoles used to manage cloud services are configured to require multi-factor authentication for access.

System and Application Security

39. Anti-virus software has been deployed on all systems commonly affected by malicious software and is updated at least weekly with the proper updates or definitions.
40. An Endpoint Detection and Response (EDR), file-integrity monitoring (FIM), or Host-based Intrusion Detection Solution (IDS) has been implemented to detect, alert on, block or initiate

responses to unauthorized changes, additions, or deletions to critical system files, configuration files, or audit logs.

41. Marriott production data is stored on a backend file or database server which is separate from the web server.
42. All system components and software have the latest vendor-supplied security patches installed and critical security patches are installed within 30 days of release. If the 30 day requirement cannot be met due to potentially unforeseen circumstances (ie: testing or compatibility issues) and those issues put the operational service or security of the Vendor system at risk, the parties shall work together in good faith to address any (limited) additional time needed to install c and/or design (mutually agreed) compensating controls.
43. Vendor will install container security software such as Prisma on all systems where Marriott Personal persists for longer than 1 hour and all PCI in-scope systems.
44. Applications are routinely tested, to include manual or automated inspection of source code to ensure no critical, high or medium vulnerabilities exist within the system. External penetration tests are conducted at least annually, and internal vulnerability scans of the infrastructure are conducted at least quarterly. Code scans are conducted prior to major releases at a minimum (if applicable).

Data Protection & Retention

45. Only the minimum amount of Marriott Data is stored by the system.
46. Reserved.
47. Reserved.
48. All employees and contractors that will have access to Marriott Data receive information security awareness training at least annually.
49. Reserved.

Encryption and Key Management

50. NIST approved cryptography is used to protect all Marriott Data during transmission over open, public networks.
51. Reserved.
52. Strict access control measures are used to protect encryption keys and access is restricted to the fewest number of custodians necessary.
53. Cryptographic keys are securely stored in the fewest possible locations and forms.
54. Key management processes and procedures are documented and implemented to include:
    a. How keys are generated
    b. How keys are stored and distributed for use within the system
    c. How and when keys are changed/rotated
    d. How expiring or possibly compromised keys are changed
    e. How dual control / split knowledge is implemented to limit access to keys

Physical, Media & Peripherals Security

55. Reserved.
56. Reserved.
57. Reserved.
58. Reserved.
59. Reserved.
60. Reserved.
61. Reserved.
62. Reserved.
63. Reserved.

Security Logging & Monitoring

64. Automated audit trails/logging is enabled for system components (servers, applications, etc.) to audit the following events:
    a. Administrative access to Marriott Data or systems hosting/processing Marriott Data
    b. Any access to central logging
    c. Invalid or denied access attempts
    d. The creation or deletion of system objects/software

65. For each event, the following items are captured by the audit trails/logs to identify what occurred on the system:
    a. User ID
    b. Type of event
    c. Date and Time of event
    d. Success or failure of the event
    e. Name of the affected data, component or resource
66. All audit trails are protected from unauthorized modifications or deletion.
67. Audit trails / logs for all system components are reviewed as needed. Reviews can be accomplished either through automated or manual means to identify issues that could affect the confidentiality, integrity or availability of the Marriott Data stored, processed or transmitted by the system.
68. Events from applications or appliances providing security services (Firewalls, IDS's, etc.) are automatically sent to the appropriate personnel in real time to address and respond to potential incidents.

Property-Centric Device Requirements

POS machines/servers deployed to the field, must be manageable by Vendor ("not be orphans").

Marriott GIS Risk and Compliance team has noted areas of non-compliance listed below and Vendor has agreed to the following Remediation Plan (where applicable):

Table 1: Non-Compliant Controls

Control Reference Line Number	Non-Compliance Issue	Remediation/Resolution	Due Date*

NOTE: Changes to the due date timelines above must be coordinated with the Marriott GIS team in writing.

Marriott GIS has determined that certain security controls are not applicable to the Vendor's System and/or Services and as such has agreed that Vendor is not required to comply with the following controls until notified otherwise by Marriott as part of a security review in accordance with Section 7.1:

Control Reference Line Number	Non-Applicability Statement