SCHEDULE 1

This schedule sets out some of the technical and organisational security measures adopted by dunnhumby and its third party cloud hosting providers. dunnhumby may update and modify the Security Measures in this Schedule from time to time, (including if needed as a result of changes made by its cloud hosting providers), however such updates and modifications will be intended to maintain or improve the overall security of the Products and Services.

For the purposes of this Schedule "dunnhumby" shall mean dunnhumby and dunnhumby Group Members.

1. Cyber Security Governance

dunnhumby has an established cyber security risk management strategy which is communicated to relevant stakeholders and monitored.

(a) Risk Management

dunnhumby has an established Information Security Risk Management Framework in place. Information security risks are logged and monitored through various reporting structures to ensure that the board has visibility of, and can monitor, cyber risk.

(b) Roles and responsibilities

dunnhumby has an established Global Information Security Team overseen by the Chief Information Security Officer who is accountable for information security risk within dunnhumby.

(c) Information Security Policies

An Information Security Policy Framework is in place which is maintained and updated as appropriate. This is overseen by the Governance, Risk and Compliance Director.

(c) Third Party / Supplier Risk Management

dunnhumby operates a policy that requires all suppliers or third parties (including, authorised sub-processors, where applicable):

- to be logged and categorised according to the inherent risk associated with the third party's access to dunnhumby (or our clients') data and/or systems;
- to have appropriate security controls in place relative to the inherent risk associated with the engagement; and
- where categorised as high risk, undergo a security assessment by our Third Party Assurance Team at the point of onboarding and periodically thereafter.

2. Identifying Vulnerabilities

(a) Vulnerability Assessments and Remediation

Application and network scanning is conducted regularly to detect vulnerabilities. Patching is applied in accordance with our Vulnerability Management Standard.

Penetration testing is conducted by an external company on dunnhumby applications and network, periodically. Findings are logged and remediation activities are tracked and monitored.

3. Protection of Assets

(a) Identity and Access Management

dunnhumby's internal data access processes and policies are designed to prevent unauthorised persons and/or systems from gaining access to systems used to Process Personal Data. dunnhumby

requires the use of unique user IDs, strong passwords and multi-factor authentication for remote access to dunnhumby systems.

User accounts are reviewed periodically to ensure access is still appropriate. Review cycles are aligned to the level of access, with higher access accounts being reviewed more frequently.

(b) Physical Security

Appropriate physical protective security measures are in place to prevent unauthorised access to dunnhumby's places of work, and damage or interference to dunnhumby's physical assets and any occupants of dunnhumby-owned premises. The sensitivity level of the information and assets hosted within a facility determines the level of security required to be implemented for that facility.

(c) Personnel Security

dunnhumby's Personnel are required to conduct themselves in a manner consistent with dunnhumby's policies regarding confidentiality, business ethics, acceptable use, and professional standards. dunnhumby conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local employment law and statutory regulations. All employee contracts include a confidentiality clause, as well as a clause which requires compliance with dunnhumby policies. These policies include information security; privacy; and acceptable use of data and technology, which must be acknowledged.

dunnhumby mandates training, which includes a variety of compliance related topics, including information security and data privacy. This training is tracked and needs to be completed by all employees, contractors, and temporary staff when joining dunnhumby and annually thereafter. dunnhumby also runs additional campaigns encouraging awareness to malicious emails; awareness of policies, standards, and procedures.

(d) Data Encryption

Encryption at rest: dunnhumby employs encryption where necessary on our platforms. This includes, but is not limited to cloud native encryption, database encryption, and disk and storage encryption. Data is encrypted using current leading encryption ciphers such as AES-256.

Encryption in transit: dunnhumby ensures that sensitive data is transmitted over encrypted channels by using technologies such as HTTPS/TLS or by using encrypted tunnels between network endpoints such as GRE and VPN.

(e) Backups of data

Backups are performed according to defined schedules, where appropriate, using a mix of dedicated media, and public cloud replication services. Backup media and public cloud storage is encrypted and secured to prevent unauthorised access.

(f) Infrastructure

dunnhumby uses a mix of public cloud providers (Google Cloud Platform and Microsoft Azure) and private co-located data centres to host most of its client services. These are offered from both multi- and single- tenancy environments, in line with product offering and/or in agreement with client.

(g) Software Development

dunnhumby has a secure coding standard based on leading industry standards such as OWASP and STRIDE. Developers are required to follow these standards and the application security team engages with developers and architects throughout the development lifecycle.

A range of checks and tests are performed throughout the SDLC, to ensure that security is embedded in the development lifecycle and to minimise vulnerabilities from being introduced into our products. These include:

- manual and automated code reviews
- security design reviews
- architecture reviews

4. Detection and monitoring

(a) Data Loss Prevention (DLP)

Data loss prevention tooling is in place which monitors and alerts on the transmission of predefined data types, and in accordance with applicable laws the on:

- Data in motion — controls installed at the network edge (e.g., One Drive, SharePoint, Teams) and email (Outlook 365) that analyse traffic to detect specific data transmitted in violation of requirements.
- Data at rest (via endpoints) – endpoint-based agents (within laptops) monitor and control information transfer between dunnhumby employees and external parties.
- Data in use — monitor and flag unauthorised activities that users may intentionally or unintentionally perform in their interactions with data.

An escalation and consequence management process is in place to manage violations and, where appropriate, repeat violations.

(b) Anti-Malware and DDoS Protection

dunnhumby takes several measures to protect, detect and prevent malware and other external attacks on dunnhumby's environment. These include a variety of technologies such as antivirus; firewalls; Web / DNS Filtering; and Remote Access VPNs.

(c) Logging & Monitoring

dunnhumby operates Security Incident and Event Management (SIEM) tool which captures logs in near realtime. A 24x7 Security Operations Centre is in place to monitor, investigate and respond to incidents.

5. Incident Response

(a) Incident Response Team

A dunnhumby incident response team which includes representatives from Security, Information Technology, Legal, Human Resources and various other business functions will define escalation paths and manage the incident.

(b) Incident Response Plan

dunnhumby has an established incident response plan, which covers the end-to-end stages of an incident, this is tested periodically to ensure the Incident Response Team is trained and prepared.

- Preparation – ensuring that appropriate teams, policies and procedures are in place, including Runbooks covering a broad range of scenarios are documented to increase the efficiency and consistency of managing incidents.
- Identification – a number of reporting channels exist to capture potential incidents and suspicious behaviour. Incidents are analysed to identify nature, sources, cause, scope and impact.
- Containment – actions are taken to limit and/or prevent any further damage from occurring

- Eradication – corrective actions are taken by addressing symptoms and root causes of the incident. This includes mitigating exploited vulnerabilities and implementing countermeasures.
- Recovery – systems are restored back to acceptable normal levels of operation.
- Lessons Learned – post-mortem reviews are conducted to assess the response activities and improve processes where necessary.

(c) Incident Severity

Incidents are categorised and managed in accordance with their severity level.

(d) Incident Communication

Where an incident involves client and/or personal data, the Legal and/or Client teams will ensure that the affected client and regulatory bodies are notified, if necessary.

6. Recovery & Resilience

(a) Business Continuity Policy

dunnhumby has a documented and approved Business Continuity Policy. This is underpinned by a number of documented plans to enable dunnhumby to continue to operate and recover from disruptions to normal business operations.

(b) Business Impact Assessments (BIAs)

dunnhumby conducts BIAs on critical business services and systems to identify dependencies and support decisions on recovery plans. These include, where appropriate, backup and recovery requirements and plans.

(c) Restore Testing

Where applicable, restore testing is conducted according to the Back-up and Restore Policy and Schedule.

(d) Multi-Availability Zones (Multi-AZ)

dunnhumby leverages the use of Multi-AZ to reduce the number of singe-points of failure and ensure high availability and resilience of our systems.