DATA PROTECTION ACT 1998

UNDERTAKING

Data Controller: Lush Cosmetics Ltd

29 High Street
Poole
Dorset
BH15 1AB

I, Mark Constantine, Chief Executive, of Lush Cosmetics Ltd, for and on behalf of Lush Cosmetics hereby acknowledge the details set out below and undertake to comply with the terms of the following Undertaking:

1. Lush Cosmetics Ltd is the data controller as defined in section 1(1) of the Data Protection Act 1998 (the 'Act'), in respect of the processing of personal data carried out by Lush Cosmetics Ltd and is referred to in this Undertaking as the 'data controller'. Section 4(4) of the Act provides that, subject to section 27(1) of the Act, it is the duty of a data controller to comply with the data protection principles in relation to all personal data in respect of which it is a data controller.

2. The Information Commissioner (the 'Commissioner') was provided with a report by the data controller that their website had been subject to a malicious intrusion, potentially compromising approximately 5000 customer credit card records.

3. Whilst the data controller did have a number of security measures in place, these were not sufficient to prevent a determined attack on the systems. The systems in use at the time also failed to fully log system activity, rendering the precise nature of the attack difficult to assess. It has been noted that the data controller has since taken prompt and substantial remedial action, re-establishing an appropriate standard of security to the systems and minimising the opportunity for a repeat of such an incident.

4. The Commissioner has considered the data controller's compliance with the provisions of the Act in the light of this matter. The relevant provision of the Act is the seventh Data Protection Principle. This Principle is set out in Schedule 1 Part

5. Following consideration of the remedial action that has been taken by the data controller, it is agreed that in consideration of the Commissioner not exercising his powers to serve an Enforcement Notice under section 40 of the Act, the data controller undertakes as follows:

The data controller shall, as from the date of this Undertaking and for so long as similar standards are required by the Act or other successor legislation, ensure that personal data are processed in accordance with the Seventh Data Protection Principle in Part I of Schedule 1 to the Act, and in particular that:

1) **Appropriate technical and organisational measures are employed, and maintained, to prevent the unlawful processing of customer data, particularly within web based systems;**

2) **Only the minimum amount of customer personal data is stored and that this is retained only for as long as a relevant business need exists;**

3) **Computer systems storing customer personal data must be subject of regular penetration testing , with activity logs retained for an appropriate period of time and frequently interrogated for evidence of malicious attack;**

4) **The processing of customer credit card data is conducted by a PCI compliant external service provider;**

5) **The data controller shall implement such other security measures as it deems appropriate to ensure that personal data is protected against unauthorised and unlawful processing, accidental loss, destruction, and/or damage.**

Dated: …….

Signed: ……

Mark Constantine
Chief Executive
Lush

Signed: ……

Sally-Anne Poole
Head of Enforcement
For and on behalf of the Information Commissioner