Digital Security **Breach Checklist**

The following checklist may be used to help organize information in connection with responding to a digital security breach where customer personal information has been accessed (or potentially accessed) by an unauthorized third party.

☐ Identify the individual/team with responsibility for coordinating security breach responses

_____ Even before a breach occurs, identify those with responsibility for response

_____ Provide those individuals with a security breach process policy

_____ Upon learning of a breach, assign one of those individuals to take responsibility for the investigation and response

☐ Identify the breach

_____ Examine logs and other information to confirm a breach of personal information has occurred

_____ Do not assume all security incidents amount to breaches

☐ Determine how the breach occurred

_____ Identify the method of disclosure

_____ Identify the nature of the breach – accidental or malicious attack

_____ If criminal activity is suspected, consider whether notifying law enforcement is appropriate and/or necessary

☐ Confirm the specific vulnerability has been eliminated

_____ Identify all potentially affected data, machines, and devices

_____ Interview personnel

_____ Preserve hardware and backups if necessary as evidence

☐ Confirm the potential for similar breaches on the system has been eliminated

LLP Cobalt
Lawyers in Advertising, Promotions & Intellectual Property
cobaltlaw.com
918 Parker Street, Bldg A21
Berkeley, CA 94710
P.510.841.9800
F.510.295.2401

☐ **Determine exactly what data was potentially exposed (and what could not have been exposed)**

☐ **Determine exactly which accounts were potentially exposed**

☐ **Determine whether notification of the affected data owners is appropriate**

☐ **Notify the data owners**

_____ Make the breach notice self-contained; i.e., it should not beg additional questions, or be emotionally charged - it should only provide notice

_____ Do not discuss the maliciousness of, label as a hacker or the like, or otherwise comment on the individual/entity behind the breach in the notice

_____ Determine the method for communicating the notice – e.g., site post, email, etc.

_____ Send the notice ONLY after all information about the breach, the plugging of the breach, the universe of users at risk, and the specific information potentially exposed has been determined

_____ Send the notice only to the universe of people who were potentially affected

_____ Consider translating the notice into additional languages where appropriate and necessary