DATA DRIVEN SAFETY, LLC (“Company”)

Data Breach Response Policy and Protocol

The **Incident Response Team** shall be comprised of the following individuals, each bearing primary responsibility for the roles specified below:

A. Information Technology
B. Legal Compliance
C. Operational Response
D. Client Support

Upon the discovery of an unauthorized access or disclosure of non-public information, the following actions shall be taken in chronological order (the process owner is indicated in bold for each):

- Notify each representative of the Incident Response Team.
- **A** - Determine whether the breach is ongoing (e.g., unauthorized access is ongoing) and, if so, have the information systems group shut it down;
- **B** - Determine whether DDS owns the affected data, or is a licensee. If DDS is a licensee, (i) immediately inform the owner of the affected data about the breach; (ii) identify any obligations DDS has under its contract with the owner; and (iii) discharge those obligations;
- **B** - Ascertain whether to inform any law enforcement agency or governmental data source (e.g., DPPA-regulated information) and, if so, which one(s);
- **A** - If DDS owns the data, determine the data that has been affected and the affected data subjects (this may require sophisticated forensics, and may take weeks);
- **C** - Determine the jurisdictions in which each affected data subject resides;
- **A** - Identify the "trigger" thresholds (e.g., unauthorized access) in each such jurisdiction;
- **C** - Figure out which thresholds (if any) were met;
- **B** - Determine whether to limit the individuals notified to those required by law;
- **B** - Analyze obligations in each affected jurisdiction (e.g., manner and content of notification; whether the state attorney general must be notified, whether the three credit bureaus must be notified and time limits);
- **B** - Determine whether to offer "extras" (e.g., free credit monitoring, toll-free information line) and, if so, which ones;

- **D** - Decide whether to have in-house personnel send the notifications, or to engage a third party to send them;
- **D** - Choose the mode of communication to be used for the notifications;
- **A** - Determine the content of the notifications;
- **D** - Send the notifications (or have them sent by the pre-selected third party); and
- **C -** Arrange for remediation of the problem.